sipri

CHALLENGES AND GOOD PRACTICES IN THE IMPLEMENTATION OF THE EU'S ARMS AND DUAL-USE EXPORT CONTROLS

A cross-sector analysis

SIBYLLE BAUER, KOLJA BROCKMANN, MARK BROMLEY AND GIOVANNA MALETTA

CHALLENGES AND GOOD PRACTICES IN THE IMPLEMENTATION OF THE EU'S ARMS AND DUAL-USE EXPORT CONTROLS

A cross-sector analysis

SIBYLLE BAUER, KOLJA BROCKMANN,
MARK BROMLEY AND GIOVANNA MALETTA

July 2017

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

Contents

Acknowledgements

The information contained in this report is based on information collected from export compliance officers, experts affiliated with industry associations and representatives of European licensing authorities, working in 14 European Union (EU) member states and one non-EU European state. The people who agreed to participate in the study were asked to outline the main compliance-related challenges companies and other entities face; and to specify whether these are generic challenges or—if not—whether they are sector or actor specific or specific to the size of the entity and/or its location. Finally, the respondents were asked, where possible, to share information about both generic and sector- and actor-specific cases of compliance-related good practices, including examples of good practices developed within companies, or useful guidelines produced by a government, industry association or export control regime. A draft version of this concept paper was discussed at a closed-door seminar, which was held at SIPRI in May 2017, and the paper was further revised on the basis of the feedback provided by participants from companies and industry associations, as well as licensing and enforcement authorities.

The authors would like to thank the US Department of State's Export Control and Related Border Security (EXBS) Program for providing the funding that allowed this concept note to be produced. They would also like to thank all those who kindly responded to the survey and particularly those who attended the SIPRI workshop in May 2017. The authors would also like to thank SIPRI intern Owen LeGrone for carrying out background research to support the drafting of the concept note, and SIPRI Editorial department for its work. All errors are entirely the responsibility of the authors.

Abbreviations

AEO	Authorized Economic Operator
ASD	Aerospace and Defence Association of Europe
BAFA	German Federal Office for Economic Affairs and Export Control
BIS	Bureau of Industry and Security
CECIMO	European Association of the Machine Tool Industries
DG TAXUD	EU Directorate General for Taxation and the Customs Union
ECM	Export Control Manager
EPOC	Export Point of Contact
EU	European Union
EUC	End-user certificate
EUGEA	EU General Export Authorization
FIATA	International Federation of Freight Forwarders Associations
HS	Harmonized system
IAEA	International Atomic Energy Agency
ICP	Internal Compliance Programme
ICT	Information and communications technology
IP	Internet protocol
ISO	International Organization for Standardization
IT	Information technology
ITT	Intangible transfers of technology
LEA	Law enforcement agency
LI	Lawful interception
NSG	Nuclear Suppliers Group
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
R&D	Research and development
SMEs	Small and medium-sized enterprises
WA	Wassenaar Arrangement
WMD	Weapons of mass destruction

Executive summary

Dual-use and arms export controls are the laws and policies that states adopt and implement in order to impose restrictions on the international movement of military goods and dual-use items. An Internal Compliance Programme (ICP) is an arrangement that an entity affected by dual-use and arms export controls puts in place to ensure that it is complying with both these controls and its own internal policies. The European Union (EU) has created a common legal basis for dual-use and, to a certain degree, arms export controls. The EU is also the only regional organisation to do so. In line with global trends in this area, the scope of the EU's controls has widened in recent years to cover a wider range of goods and technologies and—in addition to exports—certain transit, trans-shipment and brokering transactions. Consequently, a wider range of sectors and actors are now affected by these controls. These include brokers, suppliers, transport and distribution service providers and research institutes.

In tandem with this expansion in controls, the EU and national governments have been seeking to reduce the administrative burden associated with the implementation of dual-use and arms export controls, for both themselves and the affected companies, while also placing more responsibility for the implementation of controls on to the companies and other affected stakeholders. A significant aspect of these efforts has been encouraging companies and other stakeholders to adopt ICPs and to allow those that do so to benefit from reduced administrative requirements through the use of facilitated customs controls and licences that allow for multiple shipments to multiple destinations. The EU has created several measures aimed at encouraging the adoption of ICPs and the proposed recast of the Dual-use Regulation—which was published in September 2016—includes further measures in this area.

However, while the requirement to have an ICP is being increasingly mainstreamed, the guidance and tools available to companies and other affected stakeholders on how one should be established and maintained is often patchy and not targeted at those most in need of assistance. For example, at both the EU and the international level the focus of ICP discussions has generally been on companies that produce and export arms and dual-use goods, while research institutes and transport and distribution service providers have featured less in such discussions. Moreover, there has been an explicit or implicit focus on particular sectors—such as nuclear and defence and aerospace—and less on others. However, the need for such targeted guidance and tools is clear. As previous research by SIPRI has shown, the extent and way in which a company or other stakeholder is affected by the EU's dual-use and arms export controls vary significantly. This can depend on a company's size and location, the products it handles and where they are exported to, but also on the sector in which it operates.

This concept paper maps the key challenges faced by many of the sectors and actors most affected by the EU's dual-use and arms export controls, and the steps that have been taken—and could be taken—to help those affected to set up and run an effective ICP. The paper builds on past research by SIPRI in this area as well as information collected from export compliance officers, experts affiliated with industry associations and representatives of European licensing authorities, working in 14 EU member states and one non-EU European state. A draft version of the paper was discussed at a two-day workshop at SIPRI in May 2017.

Following an introductory chapter providing an overview of the above mentioned issues, chapter 2 of the concept paper maps the contours of the range of sectors and actors that are affected by the EU's dual-use and arms export controls, before outlining those that will form the main focus of this study. The section highlights the key challenges that have been faced by past data collection efforts, analysing the limitations of

available licensing, trade and production data. Building on past research in this area, the chapter narrows the focus of the study to a sample of sectors (machine tools manufacturing; defence and aerospace; nuclear; information and communications technology; and biotechnology) and actors (transport or distribution service providers; and academia and research) that have been widely identified to be amongst those that are most affected by dual-use and arms export controls.

Chapter 3 examines each of these sectors and actors in turn through a series of case studies. Each case study presents available data on the size of each sector and detailing how it is affected by the EU's dual-use and arms export controls. It then outlines some of the key sector- and actor-specific compliance-related challenges, including (*a*) compliance with the EU sanctions on Russia (for the machine tools sector); (*b*) the differences in how EU member states classify products (for the defence and aerospace sector); (*c*) the compliance with controls on intra-EU trade (for the nuclear sector); (*d*) an understanding of the limits of controls on cryptography (for the ICT sector); (*e*) the level of awareness among affected stakeholders (for the biotechnology sector); (*f*) an understanding of the responsibilities of different types of companies (for transport or distribution service providers); and (*g*) an understanding of the coverage of the exemption for basic scientific research (for academia and research).

Chapter 3 also includes examples of the good practices and sector- or actor-specific guidance that have been developed to meet such challenges, finding significant variation in the amount of targeted material that is available. For example, there is very little available in terms of targeted guidance for the machine tools and bio-technology sector on how to set up and implement an ICP. On the other hand, several documents have been produced that are focused on the nuclear sector and a growing amount of material has been produced in recent years with a focus on transport and distribution service providers. The chapter also highlights a number of stakeholders—particularly in academia and research—that are making their ICPs publicly available.

Chapter 4 highlights cross-cutting challenges that were found to affect several sectors and actors covered by the study. These were: the particular challenges facing SMEs; differences in the implementation of controls in different EU member states, or location-related challenges; product classification; managing multinational supply chains; controls on intangible transfers of technology (ITT); complexity, multiplicity and vagueness; risk assessments; and securing support from senior management and mobilizing sufficient resources. In each case, the chapter also details examples of good practices and guidance documents that can help to meet those challenges. In almost all cases the range of guidance material available was limited with—for example—very little produced that focuses on the particular needs of SMEs on the specific challenges associated with implementing ITT controls.

The conclusions highlight the lessons learned from the paper and the areas where there is a particular need for new ICP-related guidance. It also examines the potential role that governments, industry associations and in particular the EU could play in the production of this material. The paper recommends that the EU—while moving forward with its recast of the EU Dual-use Regulation—should consider the ways in which it can include language that will assist companies and other affected stakeholders with setting up and implementing ICPs while also putting in place procedures for generating clearer guidance material. These efforts should address, in particular, the specific needs of the ICT sector, academia and research, transport and distribution service providers and the challenges associated with ITT controls. They should also generate tools that can help with product classification and the risk assessments that exporters need to carry out before a transfer takes place.

1. Introduction

Dual-use and arms export controls are the laws and policies that states adopt and implement in order to impose restrictions on the international movement of military goods and dual-use items.[1] For technologically advanced states, export controls represent a key element of their foreign, security and defence policies. They are a primary means of demonstrating and imposing a state's monopoly on the legitimate use of force, while also supporting allies, constraining enemies, and applying and promoting shared normative values in areas such as conflict prevention and human rights, as well as compliance with the international treaties on nuclear, biological, chemical and conventional weapons.

The European Union (EU) is currently the only regional organization with a common legal basis for controls on the export of dual-use goods and, to a certain degree, military items. The Dual-use Regulation covers controls on the export of dual-use goods. It is directly applicable law throughout the EU, and is implemented and enforced by 28 national control systems.[2] The EU dual-use control list—which specifies the dual-use goods that are subject to control—applies to physical goods, software and technology. It incorporates the lists of items agreed in the four multilateral export control regimes: the Australia Group, the Missile Technology Control Regime, the Nuclear Suppliers Group (NSG) and the Wassenaar Arrangement (WA). The 2008 EU Common Position defining common rules governing the export of military equipment (EU Common Position) covers arms export controls. It is complemented by Directive 2009/43/EC, which simplifies the terms and conditions of transfers of defence-related products within the Community (the ICT Directive), the EU Common Position on the control of arms brokering and EU arms embargoes.[3] The EU military list—which specifies the military items that are subject to control—is based on the WA military list.

In line with expanding international commitments and control standards, the scope of dual-use and arms export controls has been widened in recent years to cover not only exports, but also certain transit, trans-shipment and brokering transactions. Consequently, a wider range of sectors and actors are now affected by these controls. These include not only exporting companies, but also brokers, suppliers and the transport sector, as well as academia and research institutes. In addition, the range of items that are subject to export controls has also expanded. For example, the recent expansion of controls on the trade in so-called cyber-surveillance systems created export control obligations for a range of companies that had little or no prior experience in this area. At the same time, austerity measures have reduced the resources available to licensing authorities in a number of countries, while their workload and its complexity have increased—also due to the expanded scope of sanctions. These factors have led governments to pursue a range of trade facilitation measures. As a result, licensing authorities are engaged in various initiatives to reduce the administrative burden associated with the implementation of export controls, for both themselves and the affected companies, while also putting more responsibility on companies but

[1] Dual-use items are goods and technologies that have the potential to be used in both civilian and military products.

[2] Council Regulation 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*, L134, 29 May 2009.

[3] Council of the European Union, 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, 8 Dec. 2008; Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community, *Official Journal of the European Union,* L146, 10 June 2009; Council of the European Union, Council Common Position 2003/468/CFSP of 23 June 2003 on the control of arms brokering, *Official Journal of the European Union,* L159, 25 June 2003; and European Commission, European Union, 'Restrictive measures (sanctions) in force', 7 July 2016, <http://eeas.europa.eu/archives/docs/cfsp/sanctions/docs/measures_en.pdf>.

without diminishing the preventive purpose of export controls. These efforts have included seeking to reduce licensing requirements for less sensitive exports, particularly through the use of 'global licences' and 'general licences'. They have also involved incentivizing the adoption of internal compliance programmes (ICPs) by the companies and institutes affected by dual-use and arms export controls and promoting improved standards in this area.

This concept note focuses on the process of setting up and running an ICP, the particular challenges that the different sectors and actors affected by the EU's dual-use and arms export controls face in this regard, and how these can be overcome. An ICP is an arrangement that an entity affected by dual-use and arms export controls puts in place to ensure that 'it is completing legal transactions, obeying the regulations enacted by the government, and fulfilling company export policies'.[4] This may be an exporting company, a broker, a supplier, a company in the transport or distribution services sector or an actor such as an academic or research institute. While ICP is a commonly used abbreviation, also in non-English language contexts, a number of alternative terms are used such as references to internal compliance 'systems' or 'functions'. Such alternatives avoid the misconception that an ICP can be reduced to an information technology (IT) system. In reality, while an ICP can be—and often should be—IT supported, IT systems do not guarantee compliance. This paper focuses on the role an ICP plays in helping EU-based companies and other affected actors comply with the EU's dual-use and arms export controls. There are also, however, a broader range of 'non-EU' security trade instruments that EU-based companies and institutions are obliged to implement. The most notable of these are the re-export controls imposed by the United States, United Nations sanctions covering trade in listed goods, but also financial sanctions and sanctions on listed persons and the sourcing of conflict minerals, and Organisation for Economic Co-operation and Development (OECD) and UN anti-corruption and human rights standards. Depending on the company or institution concerned—and its products, services, activities and markets—the implementation of many or all of these instruments and obligations may be covered by their ICP.

Developing and managing an ICP incurs costs for the company or institute involved. These costs include training and employing the staff needed to set up and run the ICP—not only the members of the compliance team, but also sales personnel and other employees that need to understand how the ICP works—and often also the purchase of screening software and other support tools. Companies and institutes put them in place because of the benefits they expect to derive from access to simplified export procedures or faster export decisions, the reduced risk of making an illegal export and the increased potential to attract customers and investors. As one representative of an industry association noted, an ICP should be seen as an asset that can increase the value of a company.[5]

Some governments have introduced a formal requirement for companies to have an ICP in place in order to be entitled to receive certain types of licences, and set out the standards that should be applied. In recent years there have also been efforts at the EU-level to incentivize or oblige companies to adopt an ICP. Under the ICT Directive, a company that wishes to receive goods exported under a general transfer licence must

[4] Institute for Science and International Security (ISIS), Key elements of an effective export control system, 2003, <http://exportcontrols.info/key_elements.htm>. For more information, see also the 'Internal Compliance Program' produced by the US State Department's EXBS Program <https://www.state.gov/strategictrade/program/etools/index.htm>.

[5] Representative of industry association, communication with authors, 2 June 2017.

be certified by its national authority—a process that requires it to have an ICP.[6] To achieve Authorized Economic Operator (AEO) status—which gives access to EU-wide customs control-related benefits—companies need to meet common criteria in a range of areas, including having an ICP in place.[7] However, uptake in both areas has been far lower than was initially hoped, largely due to confusion about the benefits of the process. Under the EU Dual-use Regulation, granting a global export authorization to a specific exporter must take account of whether the exporter has 'proportionate and adequate means' to comply with the regulation and the authorization.[8] The proposed recast of the EU Dual-use Regulation—published in September 2016—would take this process a step further by requiring companies that use global licences and the proposed EU General Export Authorizations (EUGEAs) on intra-company transmission of software and technology to have an ICP in place.[9]

However, while the requirement to have an ICP is being increasingly mainstreamed, the guidance available to companies and other affected stakeholders on how it should be established and maintained is often patchy and not targeted at those most in need of assistance. For example, at both the EU and the international level the focus of ICP discussions has generally been on companies that produce and export arms and dual-use goods. To date, even though they are being increasingly affected by export controls, research institutions and transport service providers have been largely absent from such discussions, although—as this paper shows—this is changing in some countries.[10] At the same time, the need for targeted guidance is clear. Previous research conducted by SIPRI has shown that the extent to and the way in which a company or other stakeholder is affected by the EU's dual-use and arms export controls vary significantly. This can depend on a company's size and location, the products it handles and where they are exported to, but also on the sector in which it operates.[11]

The EU has indicated that it is willing to try to help fill this gap, particularly in the context of the revision of the EU Dual-use Regulation. As noted above, the draft recast of the EU Dual-use Regulation would make it obligatory for companies using global licences and a new EUGEA on intra-company transmission of software and technology to have an ICP in place. The draft recast also contains steps that would help provide greater clarity in this area for the sectors and actors affected by the EU's dual-use and arms export controls. In particular, the draft recast would introduce a definition of an ICP into the text of the Regulation. According to the proposal, an ICP would be defined as 'effective, appropriate and proportionate means and procedures, including the development, implementation, and adherence to standardised operational compliance policies, procedures, standards of conduct, and safeguards, developed by exporters to ensure compliance with the provisions and with the terms and conditions of authorisations set out in this Regulation'.[12] Although the language is vague and keeps the focus on exporters—and thereby does not mention the other

[6] Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community, *Official Journal of the European Union*, L146, 10 June 2009.

[7] Regulation (EC) no. 648/2005 of the European Parliament and of the Council of 13 Apr. 2005 amending Council Regulation (EEC) no. 2913/92 establishing the Community Customs Code, *Official Journal of the European Union*, L117, 4 May 2005, p. 15.

[8] Council Regulation (EC) no. 428/2009 of 5 May 2009 (note 2).

[9] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council: Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (recast)—COM(2016) 616 Final 2016/0295 (COD)' 28 Sep. 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf>.

[10] Bauer, S. and Mark Bromley, M., 'Dual-use and arms trade controls,' *SIPRI Yearbook 2016: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2016), pp. 641–779.

[11] SIPRI and Ecorys, *Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review* (European Commission: Brussels, Nov. 2015).

[12] European Commission (note 9), p. 23.

supply chain actors that would benefit from having ICPs in place—it does pave the way for the generation of sector- and actor-specific guidance in the field of ICPs, stating that '[t]he Commission and the Council shall, where appropriate, make available guidance and/or recommendations for best practices for the subjects referred to in this Regulation to ensure the efficiency of the Union export control regime and the consistency of its implementation'.[13]

This paper highlights the key challenges faced by many of the sectors and actors most affected by the EU's dual-use and arms export controls, and the steps that have been taken—and could be taken—to help those affected to set up and run an effective ICP. Chapter 2 maps the contours of the range of sectors and actors that are affected by the EU's dual-use and arms export controls, before outlining those that will form the main focus of this study. Chapter 3 presents a series of sector and actor-specific case studies, presenting the available data on the size of each sector and detailing how it is affected by the EU's dual-use and arms export controls. Each case study outlines some of the key sector- and actor-specific compliance-related challenges, as well as examples of the good practices and sector- or actor-specific guidance that have been developed to meet such challenges. Chapter 4 highlights a number of 'cross-cutting' challenges that were found to affect several sectors and actors covered by the study and details examples of good practices and guidance documents that can help to meet those challenges. The conclusions highlight the lessons learned from the paper and the areas where there is a particular need for new ICP-related guidance. It also examines the potential role that governments, industry associations and—in particular—the EU could play in the production of this material.

[13] European Commission (note 9), p. 41.

2. Mapping the sectors and actors affected by dual-use and arms export controls

Identifying the sectors and actors affected

There is no single way to map the range of sectors and actors affected by the EU's dual-use and arms export controls. As noted in the introduction, one of the key challenges is to clearly delimit the effect of the EU's controls from other security-related trade controls, such as those imposed by the USA. However, even if that issue is set to one side, several other challenges present themselves. First, there is the difficulty of defining which companies and stakeholders are affected. Recent studies that have sought to measure the impact of the EU's dual-use and arms export controls—and thereby determine which sectors and actors are affected and to what extent—have used one of six definitions:

1. The value of goods exported that are subject to dual-use and arms export controls (including so-called transfers within the EU).
2. The value of goods exported that contain items that are subject to dual-use and arms export controls (including so-called transfers within the EU).
3. The value of goods exported beyond the EU that are subject to dual-use and arms export controls.
4. The value of goods exported beyond the EU that contain items that are subject to dual-use and arms export controls.
5. The value of goods manufactured that are subject to dual-use and arms export controls.
6. The value of goods manufactured that contain items that are subject to dual-use and arms export controls.

Each definition has its own merits and problems, depending on the purpose of the measuring activity. For example, a focus on the value of goods exported that are subject to controls provides a sense of the range of goods that require a licence. However, a focus on the value of goods exported that contain items that are subject to controls gives a better sense of the true impact of controls since—in most cases—the item that is subject to control cannot be removed from the product in question. Moreover, while data on exports gives a sense of the direct impact of controls, data on manufacturing gives a better sense of their potential impact, by providing a picture of the size of the sectors that could be affected by controls. Each definition generates a different image of the overall impact of the EU's dual-use and arms export controls—and hence the range of affected sectors and actors. Moreover, the focus on financial data means that all these measurements will underrepresent the impact of dual-use and arms export controls on the transport sector and research organizations, and focus on those entities which manufacture dual-use items.

Even if it were possible to agree on a definition, it might still be impossible to generate an accurate measurement due to the limitations of the data available. On exports, the two main sources are data on the value of dual-use and arms export licences issued and used, and customs data. However, both sets of data present a number of problems. First, many arms and dual-use goods are not subject to licensing or customs controls when moving from one EU member state to another. This means that intra-community trade is not accurately captured. Second, items may move back and forth between two or more states multiple times during, for example, international production processes,

Table 2.1. Categories of military items and dual-use goods

Categories	Category description
Military items[a]	
ML1 and ML2	Smooth bore weapons
ML3	Ammunition and components for ML1, ML2 and ML12
ML4	Bombs, grenades, rockets, missiles and other devices, components and accessories
ML5	Devices for fire control, components and accessories and their counter measure equipment
ML6	Ground vehicles, containers and components
ML7 and ML8	Explosives and chemicals
ML9	Vessels, special naval equipment, accessories and components
ML10	Aircraft, unmanned airborne vehicles, aeroengines
ML11	Electronic equipment and components
ML12	High velocity kinetic energy weapon systems
ML13	Armour plate and body armour
ML14	Simulators and training equipment
ML15	Imaging equipment
ML16	Forging, castings and unfinished products
ML17	Miscellaneous goods including diving equipment, ferries, containers
ML18	Production equipment
ML19	Directed weapon system
ML20	Cryogenic and 'superconductive' equipment
ML21	Software for listed goods
ML22	Technology for listed goods
Dual-use items	
Category 0	Nuclear materials, facilities and equipment
Category 1	Special materials and related equipment
Category 2	Materials processing
Category 3	Electronics
Category 4	Computers
Category 5	Telecommunications and 'information security'
Category 6	Sensors and lasers
Category 7	Navigation and avionics
Category 8	Marine
Category 9	Aerospace and propulsion

[a] Abbreviated definitions are based on <https://www.nibusinessinfo.co.uk/content/ratings-military-goods-export>.

Source: European Council, 'Common Military List of the European Union', *Official Journal of the European Union*, 28 Mar. 2017, C97; and Council Regulation 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*, L134, 29 May 2009.

resulting in a significant amount of double counting in both licensing and customs data.

The utility of licensing data is also limited by the fact that many EU member states do not collect data on the value of licences used, but only on the licences issued. Data on licences issued does not present an accurate picture of actual exports because not all licenses result in an export, and due to the growing use of global and general licences, which tend to overstate or understate the value of goods that will be exported. Finally, the utility of customs data is also limited by the fact that the Harmonized System (HS) customs codes used to classify goods are not able to meaningfully distinguish between goods that are subject to dual-use export controls and those that contain items that are subject to dual-use export controls. Moreover, the EU Directorate General for Taxation and the Customs Union (DG TAXUD) correlation table identifies the HS customs codes that contain dual-use items but the items captured by these codes are mostly not

dual-use items. A study by the Joint Research Centre (JRC) found that customs data potentially overestimates the value of dual-use exports by a factor of 6.2.[14]

Eurostat's Structural Business Statistics (SBS) database is the main source of data on manufacturing in the EU. However, like the HS customs codes, a large share of the data generated includes production that is not related to dual-use items.

The value of the approved licences issued by EU member states for the export of arms and dual-use goods to both extra-EU and intra-EU destinations was €85 billion in 2013: €48 billion in licences for the export of dual-use goods and €37 billion in licences for arms exports. The value of exports of goods covered by the HS customs codes that contain dual-use items in 2014 was approximately €476 billion to extra-EU destinations and €623 billion to intra-EU destinations.[15] Finally, according to Eurostat data the annual output of the EU's 'dual-use related industries', which produce dual-use items among other things, was over €600 billion in 2013.[16] The large differences between the numbers generated by these datasets illustrate the difficulty of quantitatively assessing the impact of EU dual-use and arms export controls, and thus the range and composition of affected sectors and actors.

Categorizing the sectors and actors affected

Just as there is no agreed way to map the range of sectors and actors affected by dual-use and arms export controls, so too is there no agreed way to break them up into clearly delimited categories. One way to categorize the range of sectors and actors that are affected by arms and dual-use export controls is to use the different categories of products in the EU's control lists for dual-use goods and military items (see table 2.1). However, there are serious limitations to this approach. For example, certain categories affect companies and other stakeholders in a wide variety of sectors, and these can face very different challenges in complying with dual-use and arms export controls. For instance, systems that employ a certain standard of cryptography are controlled under category 5 of the WA and the EU dual-use export control list.[17] These controls cover a vast array of products that are produced in a diverse range of sectors, such as telecommunications, transport and energy.[18]

A second option might be to base the categorization on HS customs codes, which capture goods and items that are subject to dual-use and arms export controls. However, the downsides of this approach are outlined above.

The approach taken in this report is to generate a broad set of categories that capture some of the main sectors and actors affected by the EU's dual-use and arms export controls. Nearly all of the companies involved in the production of military equipment are part of the defence and aerospace sector. However, a wide range of sectors are involved in the production of dual-use items. The European Commission lists the energy, defence and aerospace, telecommunications, life sciences, chemical and pharmaceutical, electronics, semiconductor and computing industries.[19] Aside

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

[15] SIPRI and Ecorys (note 11).

[16] SIPRI and Ecorys (note 11).

[17] Controls on systems that employ a certain level of cryptography have been part of the Wassenaar dual-use list since the 1990s and were introduced on the basis of national security concerns. See Saper, N., 'International cryptography regulation and the global information economy', *Northwestern Journal of Technology and Intellectual Property*, vol. 11, no. 7 (Fall 2013), <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1205&context=njtip>.

[18] European Commission, 'Impact Assessment: Report on the EU Export Control Policy Review Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items, Brussels, SWD(2016) 315 Final', p. 34.

[19] European Commission, 'Review of the EU dual-use export control regime: Regulation 428/2009', Roadmap, Directorate-General Trade F1, 15 July 2014, <http://ec.europa.eu/smart-regulation/impact/planned_ia/

from the companies in different sectors that produce these items, other actors such as transport, and research and academia are also particularly affected by dual-use and arms export controls.[20] However, the lists that have been produced are far from comprehensive and the categories named are often neither mutually exclusive nor widely reflected in the range of established economic categories used in data collection exercises or by industry associations.

Since they are the only indicative lists available, the sectors named in the European Commission documents were taken as a starting point for the analysis below. This information was supplemented by additions and modifications based on interviews, conference attendance and desk research. The sectors that have been selected for attention are: (*a*) machine tools manufacturing; (*b*) defence and aerospace; (*c*) nuclear; (*d*) information and communications technology (ICT); and (*e*) biotechnology.

The actors that have been selected for attention are: (*a*) transport or distribution service providers; and (*b*) academia and research.

There are a number of limitations to this approach. First, the data presented on the size of each sector and how it is affected by dual-use and arms export controls has been generated by industry associations, largely using different methodologies. This means that the figures will probably not be comparable. Second, several sectors overlap. A particular research institute might, for example, be included in the biotechnology, academia and research sectors. It should also be noted that this list is by no means comprehensive. In reality, companies from virtually all sectors are affected by dual-use export controls. For example, some parts of the renewable energy sector, such as those that use high-tech materials like carbon fibre; the agricultural sector, such as those that use chemicals and pesticides; and the oil and gas sector, such as those that use certain kinds of pumps and valves, lubricants or drilling equipment, will be affected by dual-use export controls.[21] Among the actors that are not explicitly covered by the study are resellers, brokers, consultants and wholesalers.

As noted in the introduction, a range of factors affect the way in which different sectors and actors are impacted by the EU's dual-use and arms export controls. Among the most important are the specific policy objectives that states are seeking to achieve through the implementation of controls on the goods and technologies being developed, produced, exported or shipped. There are a number of objectives in play in the field of arms export controls, as reflected in the range of normative criteria that EU member states are obliged to apply under the EU Common Position on Arms Exports. Chief among them are conflict prevention, preventing violations of human rights and international humanitarian law, and protecting the security interests of EU member states. The key objective of dual-use export controls has long been preventing or disrupting the supply of goods and technologies that could contribute to illegal weapons of mass destruction (WMD) programmes or to the military capabilities of states subject to an EU or a UN arms embargo. In addition, the Dual-use Regulation also obliges EU member states to assess all exports of dual-use goods against the eight criteria of the EU Common Position.

However, the expansion in the range of goods covered by dual-use export controls and a continued blurring of the distinction between civilian and military technologies have helped to expand the notion of the contribution to security that can be made by dual-use export controls. Indeed, as part of the review of the EU Dual-use Regulation, the EU has proposed applying a 'human security' approach to the Regulation. This

docs/2014_trade_014_dual_use_en.pdf>, p. 3.

[20] European Commission (note 19), p. 3.

[21] Deloitte, *Export Controls: Oil and Gas* (Deloitte: London, 2010), <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/energy-resources/deloitte-nl-uk-eiu-oilgas.pdf>.

would involve further expansion of the range of goods subject to controls and new guidelines that specifically reference human rights, international humanitarian law and terrorism for use by states when assessing licence applications. The civilian-use or military-use paradigm, which is the basis for the current EU Dual-use Regulation, has already been stretched to encompass systems used by intelligence agencies and law enforcement agencies (LEAs), which do not clearly belong in the civilian or the military sphere.

As the range of policy objectives that states are seeking to pursue through the application of dual-use and arms export controls continues to expand, the need for targeted compliance-related guidance to assist the affected sectors becomes ever more acute. This expansion means that companies and other actors not previously subject to control are being affected by dual-use and arms trade controls. In addition, the expansion looks like it will be accompanied by a further deepening of the trend for putting greater responsibility in the hands of companies and other affected actors, including through requirements on the development and implementation of ICPs. This makes the need to accurately map the particular challenges faced by the different sectors affected by the EU's dual-use and arms export controls, identify areas of good practice and highlight gaps in the available guidance documents both real and acute.

3. Sector and actor specific compliance-related challenges

This chapter describes the key characteristics of each of the sectors and actors that have been selected for closer attention in this study. Each section details how the sector or actor is affected by the EU's dual-use and arms export controls before describing the key challenges its companies and institutes face when complying with such controls. Each section then provides examples of good practices that have been developed in order to meet these challenges and a summary of the publicly available targeted guidance that has been created to help affected companies and institutes set up and implement an effective ICP.

Machine tools manufacturing

Impact of dual-use and arms export controls

Machine tools enable the production of other industrial equipment and machinery. The industry is dominated by small and medium-sized enterprises (SMEs) and concentrated on customized and small-scale production of high-precision machines. Part of this sector is metalworking machine tools, which encompasses a wide variety of machines designed to manufacture usually, but not exclusively, metallic products or parts. These often produce high-value machines that cost between €100 000 and €10 million to make. The three most common technologies are cutting machines, drilling and milling machines, and forming machines.[22] The European Association of the Machine Tool Industries (CECIMO) represents companies in the EU, as well as Switzerland and Turkey, that in total employ nearly 150 000 people. CECIMO estimates that machine tool production in CECIMO countries in 2016 was worth €24.2 billion, which represents a global market share of 40.5 per cent, and that exports were worth €18.7 billion.[23]

Because the European machine tools industry is increasingly focused on top-end and high-precision machines, nearly all the European producers must comply with dual-use trade controls. According to CECIMO, more than 80 per cent of European cutting machine tools are classified as dual-use.[24] Of the forming machine tools, only certain hot-isostatic or isostatic presses and some highly advanced forming technologies are controlled. The share of dual-use exports differs widely by company, depending on both its product portfolio and its customers. According to those who work in the machine tools sector, the proportion of a company's products that is subject to dual-use controls can vary from 15 per cent to almost 100 per cent.[25]

Sector-related compliance challenges

Representatives of the machine tools sector identified a range of compliance-related challenges. Many of these were linked to the location and size of the company but others were sector-specific. For example, company representatives from Germany and Italy highlighted the fact that in the machine tools sector there are often cases where an exported product is not subject to controls but some of the components—when

[22] SIPRI and Ecorys (note 11).

[23] CECIMO, *Economic and Statistical Toolbox* (CECIMO: Brussels, 2017), <http://www.cecimo.eu/site/fileadmin/documents/STATISTICS%20and%20MARKETING/Statistics/CECIMO%20Statistical%20Toolbox/CECIMO_Statistical_Toolbox_01_2017.pdf>.

[24] European Commission (note 18), p. 15.

[25] SIPRI and Ecorys (note 11).

delivered as spare parts—are considered dual-use and require an authorization.[26] These exports generally require an individual—rather than a general—licence, which represents more of an administrative burden. On a related point, more than one respondent highlighted the difficulty of complying with dual-use export controls when exporting non-dual use goods that contain dual-use components.[27] In addition, the high level of 'personalization' and 'innovation' in machine tools production can make product classification difficult and increase the likelihood that an individual licence will be required.[28]

One of the companies interviewed highlighted challenges related to complying with the EU sanctions on Russia, which bar exports of dual-use goods to military end-users.[29] Certain companies in Russia that wish to purchase machine tools are listed as producing equipment for both civil and military end-users (e.g. 'civil railway, cars and tanks'). In this case, the licensing authority must be notified in order to clarify whether it is possible to ship and how, which complicates the export process.

Good practices and guidance documents

Representatives of companies from the machine tools sector generally saw having an ICP—and having AEO status—as an advantage when applying for an export licence.[30] One representative from a German company described how it had decided to put in place a more systematic ICP, starting by recruiting export control experts to assist with its development and establish a clear set of procedures to be followed, after a customs audit.[31] Since then, a set of procedures within the company and within its Enterprise Resource Planning (ERP) system has ensured that products are handled properly when they are exported. The procedures also involve informing any customers in Germany that the products they are purchasing may be subject to dual-use export controls.[32] There do not appear to have been any ICP-related guidance documents produced by governments, export regimes or other sources that are specifically tailored to the machine tools sector.

Defence and aerospace

Impact of dual-use and arms export controls

According to the Aerospace and Defence Association of Europe (ASD), the EU defence and aerospace sector has a turnover of €222.2 billion, invests €20 billion in Research & Development (R&D) and has annual exports valued at €115 billion.[33] The sector comprises over 3000 companies and 80 000 suppliers, which provide direct employment to 847 000 people in Europe.[34] The EU defence and aerospace sector has a large number of SMEs but also a high level of concentration. About three-quarters of the

[26] Managing Director, Technologies, Machine tool company, Germany, Correspondence with author, 14 Mar. 2017; Technical expert, Industry association, Italy, Correspondence with author, 17 Mar. 2017.

[27] Technical expert (note 26); Managing Director (note 26).

[28] Technical expert (note 26).

[29] Managing Director (note 26).

[30] Technical expert (note 26).

[31] Director, Purchasing and Order Processing, Machine tool company, Germany, Correspondence with author, 28 Mar. 2017.

[32] Director, Purchasing and Order Processing (note 31).

[33] European Commission (note 18), pp. 15–16.

[34] AeroSpace and Defence Industries Association of Europe (ASD), *Key Facts & Figures, 2015* (ASD: Brussels, Nov. 2016), <http://www.asd-europe.org/fileadmin/user_upload/ASD_F_F2015_web_spreads_Nov.pdf>.

EU-based companies in the sector have fewer than 10 employees.[35] At the same time, larger enterprises account for 6 per cent of firms but nearly 80 per cent of turnover.[36]

According to the ASD, most of the defence and aerospace sector's activity is affected by dual-use and arms trade controls.[37] However, the way in which such controls affect companies in the defence and aerospace sector varies from sub-sector to sub-sector. For example, the space sector is mainly affected by dual-use export controls.[38] Companies in the defence and aerospace sector are also more likely to be impacted by US controls on re-exports, in addition to EU dual-use and arms export controls.[39] Even if the material being controlled is a dual-use item, there may be 'defence services' involved, which has implications for technical data transfers, logging, record keeping and 'deemed exports', such as the release of technology or source code.[40]

Sector-related compliance challenges

One key compliance-related challenge for companies in the defence and aerospace sector is the fact that the same item can be classified as covered by the EU dual-use list in one member state and by the EU military list in another.[41] This is partly due to the use of terms that are open to interpretation, such as 'specially designed or modified for military use', a term which appears throughout the EU military list but which lacks a clear definition at either the WA or the EU level.[42] A related issue is the differences in member states' licensing procedures with regard to dual-use products that are embedded in larger systems.[43] In particular, there appear to be differences as to whether a dual-use item would require a licence even when it is integrated into a larger system and its removal for separate use would be disproportionately expensive and highly unlikely. Another challenge relates to controls on intangible technology transfers (ITT) and the legal requirement to limit employee access to documents containing controlled technology when they travel outside the EU.[44] This can often pose practical and privacy law-related challenges.

Additional administrative burdens are created by the requirement to document each time a controlled technology is accessed. One company representative noted that the rules have become too complex and progressively harder to implement, even for those who are seeking to comply.[45] Another sector specific-challenge is US controls on deemed exports. This is a key factor that distinguishes compliance in the defence and aerospace sector from other sectors 'where the focus may be more on hardware shipments or sometimes software, and less on access to a facility, photo policies and public releases'.[46] Another issue that affects the defence and aerospace sector is the amount of information that companies are required to supply when applying for an export licence for certain types of military equipment. For example, under WA and Organization for Security and Co-operation in Europe (OSCE) guidelines adopted in 2007 and 2008, respectively, states are encouraged to require companies to provide

[35] European Commission (note 18), p. 16.
[36] European Commission (note 18), p. 16.
[37] European Commission (note 18), p. 15.
[38] Director of export controls, Space company, France, Correspondence with author, 16 Mar. 2017.
[39] Chief export compliance officer, Aviation and Aerospace group, Norway, Correspondence with author, 11 Mar. 2017; Export control manager, Aviation company, Correspondence with author, 23 Mar. 2017.
[40] Chief export compliance officer (note 39).
[41] Compliance officer, Defence and aerospace company, meeting with author, Sweden, 5 Apr. 2017.
[42] See Samuel A. W. Evans 'Revising export control lists', Flemish Peace Institute, Mar. 2014, <http://www.vlaamsvredesinstituut.eu/sites/vlaamsvredesinstituut.eu/files/files/reports/revising_export_control_lists_web.pdf>, p. 24.
[43] Compliance officer (note 41).
[44] Compliance officer (note 41).
[45] Compliance officer (note 41).
[46] Chief export compliance officer (note 39).

information when they apply for an export licence for small arms and light weapons that are to be shipped using air transport.[47] Some states have stricter requirements. In Romania, for some shipments of military goods companies are required to provide information on: (*a*) the companies and means of transport that will be employed at all stages of the delivery; and (*b*) the routes taken during the delivery.[48] However, as one company representative noted, it is often not possible to know these details when the licence application is submitted.[49] Another challenge is that it is often difficult to find a company willing to undertake the shipment, since many transport companies are unwilling to transport military goods.[50] Finally, when exporting military goods, companies are required to obtain a Delivery Verification Certificate (DVC) from the consignee, which can be a difficult or time-consuming process.[51]

Good practices and guidance documents

Representatives of companies from the defence and aerospace sector generally viewed ICPs as 'indispensable' and a guarantee of the company's 'reliability and competence'.[52] Representatives also highlighted a number of good practices on trade compliance, such as standardization, clear policies and implementation tools that flow down; the 'involvement of the Chief Compliance Officer in every aspect of the business'; 'tailored training';[53] record keeping and early identification and classification of products;[54] and maintaining 'contacts with all relevant authorities' when applying for a licence.[55]

There are only a few targeted compliance-related guidance documents aimed at the defence and aerospace industry sector. The British Government has a guide on its website, which stresses the importance of the application of export regulations in the UK and of any import regulations in the destination country.[56] The guide provides information on the different types of licences that may be used, the trade facilitations that are available and the restrictions that apply on trading certain types of goods produced by the defence and aerospace sector. One key factor identified in the British guidance is the need for proper research on the export destination. The ICP Guidelines published by the US Department of Commerce—which require companies in the USA to implement an 'Export Management and Compliance Program Manual'—can also be of assistance to companies affected by US re-export controls.[57] Leonardo is one of the few European companies in the defence and aerospace sector to make its compliance programme publicly available. The programme contains an overview of national, European and US legislation, as well as a description of the respective elements of the company's ICP. Notable among these are a risk analysis process for defence goods

[47] Wassenaar Arrangement, 'Best Practices to Prevent Destabilising Transfers of Small Arms and Light Weapons (SALW) through Air Transport', Dec. 2007; and OSCE Decision 11/08 'Introducing Best Practices to Prevent Destabilizing transfers of Small Arms and Light Weapons Through Air Transport and on an Associated Questionnaire', FSC.DEC/11/08, 5 Nov. 2008.

[48] External Relations Expert, Export Department, Defence Company, Romania, communication with the authors, 6 June 2017.

[49] External Relations Expert (note 48).

[50] External Relations Expert (note 48). This challenge may not be confined to the defence and aerospace sector. Since 2009 a number of transport companies have decided not to carry certain types of dual-use goods because of the administrative burden involved. See SIPRI and Ecorys (note 11), p. 232.

[51] External Relations Expert (note 48).

[52] Chief export compliance officer (note 39); and Export control manager (note 39).

[53] Chief export compliance officer (note 39).

[54] Director of export controls (note 38).

[55] Export control manager (note 39).

[56] British Government, Department for International Trade, Export Control Organization, 'Aerospace and Defence Sector: International Trade Regulations', 7 Aug. 2012, <https://www.gov.uk/guidance/aerospace-and-defence-import-and-export-regulations>.

[57] US Department of Commerce, Bureau of Industry and Security, Export compliance guidelines, 2017, <https://www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance>.

and technology transactions, screening and verification at three different phases of a transaction, and a 'preventive notice' and 'regular reporting system' for politically sensitive exports.[58]

Nuclear

Impact of dual-use and arms export controls

The nuclear sector covers both the companies that build and operate nuclear power plants and those involved in all associated manufacturing and trading activities. According to the World Nuclear Association there are 128 nuclear power reactors operating in 14 EU member states. These account for more than a quarter of the electricity generated across the whole of the EU.[59] According to FORATOM, the annual turnover of the European nuclear industry is €70 billion, 240 000 people are employed in operating nuclear reactors and there are 460 000 direct and indirect jobs connected to the European nuclear energy sector.[60] Almost all aspects of the nuclear sector are subject to dual-use controls, and nearly all the principal items and components concerned are included on the EU dual-use list.[61]

Sector-related challenges

One industry organization representative argued that the main compliance-related challenge for the nuclear sector is that it is treated differently compared to sectors such as the chemical, and defence and aerospace sectors.[62] This is specifically related to the regulations that apply and the number of authorizations that are needed before exports can take place, even to other EU member states. One company representative commented on the number of export licences that are required even 'to bid for a project' in another EU member state, something that is not required in other sectors, where intra-EU transfers do not require specific authorization.[63] There is also a requirement to provide an end-user certificate (EUC) even when exporting to a nuclear facility that is subject to International Atomic Energy Agency (IAEA) safeguards. Thus, 'developing a supply chain' in the nuclear sector can prove challenging due to export controls. In this regard one of the companies consulted argued that 'while initial identification of potential suppliers can be achieved without recourse to licensing', it eventually becomes necessary 'to share with them controlled technology' in order to receive a 'realistic quote for the job'. Therefore, a licence will be required if the potential supplier is located inside the EU, while a government-to-government assurance will also be necessary for a licence to be issued if the supplier is located outside the EU.[64]

In addition, the nuclear sector and the markets involved are relatively small. As a result, export control authorities receive fewer licence applications for nuclear exports and are therefore less familiar with the topic. In some cases, this requires them to consult officials with the necessary expertise, which delays the application process.[65]

[58] Leonardo, 'Controls on exports and sensitive countries', 2017, <http://www.leonardocompany.com/en/chisiamo-aboutus/etica-compliance/controlli-sulle-esportazioni-e-paesi-sensibili>.

[59] World Nuclear Association, 'Nuclear Power in the European Union', April 2017, <http://www.world-nuclear.org/information-library/country-profiles/others/european-union.aspx>.

[60] FORATOM, Pocket guides, Jan. 2017, <https://www.foratom.org/facts-figures/#>.

[61] European Commission (note 18), pp. 15–16.

[62] Senior Project Manager, Industry Association, Interview with author, 29 Mar. 2017.

[63] Head of Export Control Policy, Nuclear energy sector company, the UK, Correspondence with author, 21 Apr. 2017.

[64] Head of Export Control Policy (note 63).

[65] Senior Project Manager (note 62).

Companies also find that administrative arrangements vary from country to country, and that their effectiveness partly depends on the degree of familiarity the competent authorities have with the nuclear sector. In addition, doing business in some countries—especially extra-EU countries, even if they are NSG members—can prove prohibitive due to the time it takes to obtain export authorizations. For example, providing spare parts to China is very difficult. This is linked not to the issuance of export licence denials, but to the time it takes to obtain an approval. Some argued that the above-mentioned challenges make it difficult or economically unsustainable for smaller companies to compete in this sector. At the same time, a compliance-related challenge for larger companies is the lack of expertise and knowledge among smaller suppliers or subsidiaries, where employees are often unaware of the fact that they are supplying controlled information and technologies.[66]

Good practices and guidance documents

One company representative highlighted the importance of getting export controls into a positive rather than negative perspective. This allows staff to see the 'bigger picture' and to understand the purposes of the controls rather than perceive them as something imposed by the government or the EU to make their lives difficult.[67] With reference to good practices, the same company representative mentioned the instructions staff must follow in cases of exports of equipment, material and technology. In such cases, if the export classification is not already known, it must be determined by a specialist, signed by a Senior Engineer and sent to the Export Control Manager (ECM) or local Export Point of Contact (EPOC) for approval. The ECM or EPOC should also be contacted for advice where any concerns arise that non-controlled items might be used in a nuclear weapons programme.[68]

The British Government has produced targeted compliance-related guidance for exporters of nuclear equipment, materials and technology. The guidance outlines the process of submitting an application for an export licence and the subsequent assessment of applications by the appropriate authorities. It also lists the most important factors that exporters must be aware of when submitting an application.[69] In addition, a small number of documents have been published by associations in the nuclear sector, which outline generic principles on how to ensure compliance with strategic trade controls. These usually refer to internationally agreed provisions (the NSG Guidelines, IAEA safeguards) and—as in the case of Carnegie's Principles of Conduct—contain a commitment by the adherents to abide by national and international regulations.[70] A report produced by the World Nuclear Association on 'Good Practice in the Compliance and Licensing of Nuclear Exports' contains some useful suggestions on the basic principles of an internal compliance programme, as well as as fostering coordination and communication between the nuclear industry and the competent export control authorities; and streamlining the export control regime.[71]

[66] Head of Export Control Policy (note 63).

[67] Head of Export Control Policy (note 63).

[68] Head of Export Control Policy (note 63).

[69] UK Department for International Trade and UK Department of Energy and Climate Change and Export Control Organization, Guidance, 'Export of Nuclear Equipment, Material and Technology: "Trigger List" Requirements', 12 Dec. 2012, <https://www.gov.uk/guidance/export-of-nuclear-equipment-material-and-technology-trigger-list-requirements>.

[70] Nuclearprinciples.org and Carnegie Endowment for International Peace, 'Nuclear Power Plant and Reactor Exporters' Principles of Conduct', 1 Jan. 2015, <http://nuclearprinciples.org/wp-content/uploads/2015/02/PrinciplesofConduct_January20153.pdf>.

[71] World Nuclear Association, 'Good Practice in the Compliance and Licensing of Nuclear Exports', Aug. 2015, <http://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/REPORT_Good_Practice_in_Nuclear_Exports(1).pdf>.

One sector representative noted that there was less need for more targeted guidance documents and more need to encourage governments to streamline their export control regulations in order to reduce the overall burden on the industry.[72] The sector representative also suggested that the NSG should not only undertake outreach to non-member states, but also conduct in-reach activities among its own members. This should be aimed at ensuring that exports to all NSG members are treated equally, something that is not currently the case.[73] On the development of internationally accepted common standards for internal compliance programmes in the nuclear sector, one respondent mentioned the development of a quality management standard for the nuclear sector that also covers export compliance.[74]

Information and communications technology

Impact of dual-use and arms export controls

According to the EU, the 'value added' of the EU ICT sector in 2013 was around €530 billion, or over €580 billion if the wholesale trade and the manufacturing of magnetic and optical media are included.[75] In 2013, 5.6 million people were employed in the ICT sector.[76] According to the OECD, in 2012 the sum of all ICT exports from 21 of the 28 EU member states was US $286 billion.[77]

The ICT sector is significantly affected by dual-use export controls, particularly through the controls on cryptography, which is an integral part of many of the systems produced by the ICT sector. In 2014, dual-use-related exports of telecommunications and 'information security' were worth €32.5 billion.[78]

The impact of dual-use export controls on the ICT sector has also been affected by the expansion in controls on so-called cyber-surveillance technologies. Cyber-surveillance technologies enable the monitoring and exploitation of data or content that is stored, processed or transferred via ICTs, such as computers, mobile phones and telecommunications networks (see box 3.1). Prior to 2011 several cyber-surveillance technologies were covered by dual-use export controls because of the level of cryptography they employed.[79] After the Arab Spring uprisings in 2011, a series of NGO and media reports highlighted the role of EU- and US-based companies in the supply of non-controlled cyber-surveillance technologies to states in the Middle East and North Africa.[80] Citing the security and human rights concerns connected with their use, the WA and subsequently the EU responded by expanding their dual-use export controls to directly capture a wider range of cyber-surveillance technologies. This led to the creation of controls on mobile telecommunications interception equipment, intrusion

[72] Senior Project Manager (note 62).

[73] Senior Project Manager (note 62).

[74] Senior Project Manager (note 62).

[75] De Panizza, A. and Bogdanowicz, M., *PREDICT 2016: Key Facts*, Joint Research Centre (JRC) Technical Report (European Commission JRC/Publications Office of the EU: Seville and Luxembourg, 2016), <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC102368/jrc102368.pdf>, p. 15.

[76] De Panizza and Bogdanowicz (note 75), p. 16.

[77] OECD, <https://data.oecd.org/ict/ict-goods-exports.htm#indicator-chart>. These states are Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden and the United Kingdom.

[78] European Commission (note 18), p. 15.

[79] In particular, exports of digital forensics, intrusion software and lawful interception (LI) systems have all been made subject to dual-use export controls on these grounds. '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>.

[80] See e.g. Elgin, B., Silver, V. and Katz, A., 'Iranian police seizing dissidents get aid of western companies', Bloomberg Business, 31 Oct. 2011, <http://www.bloomberg.com/news/articles/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies>; and International Federation for Human Rights (FIDH), *Surveillance Technologies 'Made in Europe': Regulation Needed to Prevent Human Rights Abuses*, Position paper (FIDH: Paris, Dec. 2014), <http://fr.scribd.com/doc/251396002/Surveillance-Technologies-Made-in-Europe>.

Box 3.1. Types of cyber-surveillance technologies

1. *Mobile telecommunications interception equipment*—also know as 'IMSI Catchers'—are used to remotely track, identify, intercept and record mobile phones.

2. *Intrusion software* can be inserted into computers and mobile phones without detection and used to remotely monitor and, in certain cases, control them.

3. *Internet Protocol (IP) network surveillance systems* are used to intercept, collect and, in some cases, analyse data as it passes through an IP network.

4. *Data retention systems* are used by network operators to comply with legal requirement to store 'meta data' on their users for potential later use by LEAs or intelligence agencies.

5. *Lawful Interception (LI) systems* are used by network operators to enable them to comply with requests from LEAs and intelligence agencies for the provision of their users' communications data.

6. *Monitoring centres* are used by LEAs and intelligence agencies to collect, store and analyse different forms of communications data from various surveillance sources.

7. *Digital forensics systems* are used by LEAs or intelligence agencies to retrieve and analyse data stored on networks, computers and mobile devices.

Note: A network operator is a company that manages a communications network, such as Vodafone 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, about what is said in a phone call or the content of a text message; or (*c*) location data, information about the movements of a subscriber to a mobile phone network.

Source: Adapted from Bromley, M., Jan Steenhoek, K., Halink, S. and Wijkstra, E., 'ICT surveillance systems: Trade policy and the application of human security concerns', *Strategic Trade Review* (Spring 2016).

software and Internet protocol (IP) network surveillance systems. The proposed recast of the EU Dual-use Regulation would create an EU autonomous control list for certain monitoring centres and data retention systems, while also establishing a targeted end-use control that would—in certain special circumstances—allow authorities to control non-listed cyber-surveillance technologies.

Sector-related challenges

Companies in the ICT sector face a number of challenges when seeking to comply with controls on cryptography, particularly when it comes to determining whether the systems they are exporting are covered by the 'Cryptography Note', which outlines the situations in which items are exempt from controls.[81] The representative of one company that makes IT security tools noted that due to the lack of clear guidance from the national authority, it takes a cautious approach when determining whether items are covered by the note. This means that, for the majority of its products, the company applies for an individual licence for every export to a state not covered by Union General Export Authorization EU001.[82] This can be a time-consuming process, the length of which varies considerably from one EU member state to another.[83] The company had exported from the Netherlands and from Ireland, and had found that the Irish export control system had a greater reliance on end-user statements, which made the process of applying for licences more time-consuming.[84] The company representative also noted the difference between EU controls on cryptography and those in the USA, where the range of systems exempt from licensing requirements is far

[81] Such situations are listed as the sale of items: that are 'generally available to the public by being sold, without restriction, from stock at retail selling points'; where the 'cryptographic functionality cannot easily be changed by the user'; and that are 'designed for installation by the user without further substantial support by the supplier'. In addition, 'when necessary, details of the goods [should be] accessible and will be provided, upon request, to the competent authorities of the Member State in which the exporter is established.' Note 3: Cryptography Note, Council Regulation (EC) no. 428/2009 of 5 May 2009 (note 2).

[82] The states covered by Union General Export Authorization EU001 are Australia, Canada, Japan, New Zealand, Norway, Switzerland and Liechtenstein.

[83] Senior Manager, Trade Compliance, ICT multinational Company, Ireland, communication with the authors, 2 June 2017.

[84] Senior Manager (note 83).

broader. Although the company exports similar systems from both the USA and the EU, in the former it has not had to apply for an export licence in the past three years while in the latter making an application is a weekly occurrence.[85] Operating effective end-use controls is also a challenge, particularly when dealing with software that can be downloaded online or IT security infrastructure that can be re-purposed for surveillance purposes. In the former case, steps can be taken to cut off updates if, for example, the end-user is located in a territory that is subject to an embargo. However, there is nothing to stop the end-user from leaving that territory to obtain the update and then moving back.[86]

Making cyber-surveillance technologies subject to dual-use export controls has presented a challenge for many of the companies affected. Some of the companies that produce these systems—particularly the many SMEs involved—have little experience with dual-use export controls or related requirements concerning the creation and management of ICPs. In addition, depending on the systems they produce and their markets, some companies are more likely than others to be forced to adjust their business models as a result of being made subject to dual-use export controls. Another key determinant of how companies are affected by the expansion of controls on cyber-surveillance technologies is the way they are applied by individual EU member states. In 2014, it was reported that Germany was controlling exports of intrusion software through individual licences for each transfer.[87] By contrast, in 2015 it was reported that Italy was controlling exports of intrusion software through the use of general licences, which means that exporters were being given a single licence for exports of intrusion software that was valid for multiple years and destinations.[88]

The companies involved have responded differently to being made subject to export controls. At least one company that produces intrusion software—Gamma Group—is reported to have moved its work in this area to offices in countries that are outside the WA.[89] Amseys, a French company that makes IP network surveillance systems, is also reported to have moved its operations outside of the EU, but it is unclear whether this is as a result of the application of export controls.[90] However, other companies have not moved. Indeed, one EU-based producer of IP network surveillance systems noted that being subject to export controls has advantages, particularly as it creates the conditions for political and economic support should a contract need to be cancelled due to changing conditions in the recipient state.[91] Nonetheless, many of the companies affected highlighted similar compliance-related challenges, not least the need for clear and timely information from either the EU or the national licensing authority about which destinations and end-users should be viewed as suitable customers.[92]

There has also been a significant amount of confusion about the precise scope of new controls on exports of cyber-surveillance technologies. In particular, companies and researchers in the IT sector have voiced concerns about the unintended impacts and 'chilling effects' of the controls on intrusion software introduced by the WA and at

[85] Senior Manager (note 83).

[86] Senior Manager (note 83).

[87] Page, K., 'Six things we know from the latest FinFisher documents', Privacy International, 15 Aug. 2014, <https://www.privacyinternational.org/?q=node/371>.

[88] Currier, C. and Marquis-Boire, M., '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/>.

[89] Omanovic, E., 'Surveillance companies ditch Switzerland, but further action needed', Privacy International, 5 Mar. 2014, <https://www.privacyinternational.org/?q=node/377>; and Habegger, H., 'Bund Verscheucht Hersteller von Spionagesoftware Aus Der Schweiz [Federation 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/>.

[90] SIPRI and Ecorys (note 11), p. 180.

[91] SIPRI and Ecorys (note 11), p. 181.

[92] SIPRI and Ecorys (note 11), p. 181.

the EU level.[93] A number of companies and researchers have argued that the language used describes both the intrusion software used by LEAs and intelligence agencies and systems and processes that are essential to IT security, particularly systems used for penetration testing and processes of vulnerability disclosure.[94] In the USA, concern about the potential impact of controls on exports of intrusion software on processes of vulnerability disclosure and penetration testing led the US Government to delay the adoption of the controls and to seek to amend the language adopted by the WA.[95]

Good practices and available guidance

A number of compliance-related guidance documents have been targeted at the ICT sector. For example, the European Commission recently produced a set of guidance for exporters with regard to ICT items and the application of the 'Cryptography Note'.[96] However, the guidance is mainly focused on the process through which the note should be applied by EU member states and does not provide concrete information on how the language it contains should be interpreted. A number of corporate social responsibility standards have also been produced that provide guidance for companies affected by controls on exports of cyber-surveillance technologies. The most relevant are the UN Human Rights Council's 'Guiding Principles on Business and Human Rights'; the OECD's set of guidelines for multinational enterprises; the European Commission's 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights'; the Electronic Frontiers Foundation's '"Know Your Customer" Standards for Sales of Surveillance Equipment'; and TechUK's 'Assessing Cyber-Security Export Risks'.[97] However, these guidelines either largely focus on the ICT sector or cyber-surveillance systems in general, without discussing the particular risks associated with each particular type of system, or only cover certain types of systems.

Various efforts have also been made to clarify the precise scope of the controls on intrusion software. In particular, a number of articles have argued that these controls, if properly applied, should not affect processes for vulnerability disclosure or capture penetration testing systems.[98] In 2015 the British Government produced a guidance note aimed at alleviating the concerns of the IT security research community. The

[93] Carty, K., 'Lawmakers assail cybersecurity provisions in international treaty', Morning Consult, 12 Jan 2016, <https://morningconsult.com/alert/lawmakers-assail-cybersecurity-provisions-in-international-treaty/>.

[94] Bratus, S., Capelis, D J, Locasto, M. and Shubina, A., *Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense at Risk, and How to Fix it*, 9 Oct. 2014, <http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf>. 'Penetration testing systems' are used to test the security of a network by simulating attacks against it in order to locate vulnerabilities. Processes of 'vulnerability disclosure' are the means through which software vulnerabilities are identified and reported. Others have argued that, if properly applied, the controls should have no effect in these areas. See Anderson, C., *Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies*, Access Now, 13 Mar. 2015, <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf>.

[95] Cardozo, N. and Galperin, E., 'Victory! State Department will try to fix Wassenaar Arrangement', Electronic Frontiers Foundation, 29 Feb. 2016, <https://www.eff.org/deeplinks/2016/02/victory-state-department-will-try-fix-wassenaar-arrangement>.

[96] European Commission, DG Trade, 'FAQ on controls of "Information Security" items and implementation of the Cryptography Note exemption'.

[97] United Nations, Office of the High Commissioner, Human Rights, *Guiding Principles on Business and Human Rights* (United Nations: New York and Geneva, 2011), <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>; OECD, Guidelines for Multinational Enterprises, [n.d.], <http://www.oecd.org/corporate/mne>; Shift and Institute for Human Rights and Business, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (European Commission: Brussels, June 2013), <https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf>; Cohn, C. and York, J., '"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>; and British Government and TechUK, *Assessing Cyber Security Export Risks*, Cyber Growth Partnership Industry Guidance (TechUK: London, 25 Nov. 2014), <https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf>.

[98] See Anderson (note 94).

note underlined the exemptions that apply under the WA and the intended focus of the controls. However, the note also indicated that certain types of penetration testing software were covered by the controls on intrusion software as well as certain types of vulnerability disclosures.[99] The note has not fully alleviated the concerns raised by companies and researchers in the ICT security sector.

Biotechnology

Impact of dual-use and arms export controls

According to the European Commission, the total value of the production of the European biotechnology industry was €105 billion in 2013 and it provided employment for 236 000 people.[100] In the Horizon 2020 programme, the EU identifies biotechnology as one of the 'key enabling technologies', on account of its widespread applications across industries, the public sector and research.[101]

The number of biological materials and technologies, and the different types of equipment and other related items included in the EU dual-use list clearly indicate the strong impact of the EU Dual-use Regulation on this sector. The resulting export controls however affect not only industrial actors, but also a wide range of public sector actors such as research institutes, hospitals and universities (see research and academia). Research on biotechnology also produces new technologies and knowledge that cannot be readily classified within the existing parameters of export controls. This presents additional challenges for dual-use export controls to stay up to date and prevent unnecessary periods of uncertainty, for both industry and researchers.

Sector-related challenges

Actors engaged in biotechnology and the life sciences face a variety of compliance-related challenges. Pathogens occur naturally, and risk assessments that seek to judge the potential danger associated with a transfer on the basis of the amounts of pathogens involved are often inadequate because a tiny sample can multiply and expand rapidly. In addition, enabling technologies—such as the equipment used to grow and store pathogens or to assemble DNA (DNA synthesizer)—have such a variety of uses, both legitimate and prohibited, that control efforts are largely ineffective.[102] The different interpretations of export control regulations by EU member states and the lack of awareness of many affected stakeholders add to these challenges. Lack of awareness is an issue not only for the growing 'do-it-yourself' and 'biohacking' communities, but also for companies and particularly for research institutes.[103] In 2012 the Government of Hungary (prompted by the licensing authority) issued a decree directing companies and institutes working in the biotechnology sector to register and report on their activities in connection with the items and technologies listed by the Australia Group.[104] The government took this decision because it had not received a single licence application from the sector, even though it had previously carried out a dedicated outreach programme.[105] Where companies and institutes in the biotechnol-

[99] 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/>.

[100] European Commission, DG Research and Innovation, 'Biotechnology: An enabling technology for industry', 2016, <DOI: 10.2777/251095>.

[101] European Commission (note 100).

[102] Representative of German governmental research institution, Correspondence with authors, 21 June 2017.

[103] SIPRI and Ecorys (note 11), pp. 36–41. This information was based on a background paper provided by Peter Clevestig.

[104] Representative of EU member state licensing authority, communication with the authors, 6 June 2017.

[105] Representative of EU member state licensing authority (note 104).

ogy sector are aware of export controls, they often view them with suspicion. Among other reasons, this is partly due to concerns that restrictions on the free movement of knowledge and material in this area will create hindrances to business activities, generate obstacles to global public health efforts and generally infringe on the freedom of scientific research.[106] A related challenge—which is common to research and academia more generally—is that researchers consider it 'absurd' that they should have to apply for a licence in order to discuss their findings at a conference or publish them in an academic journal.[107]

Another key challenge is the constant emergence of new enabling technologies within the biotechnology sector—such as those described above—that are too broad in scope to be effectively controlled.[108] This demands continuing engagement and cooperation among scientists, industry representatives and the authorities in order to address new classification and control challenges. One representative of a research institute argued that one response to these rapid developments should be to narrow the scope of export controls in the biotechnology sector and to apply a 'combination approach': neither pathogens nor enabling equipment alone should trigger export controls, but only certain combinations of the two.[109]

A further challenge in the biotechnology sector is the question of how best to integrate bio-safety initiatives and export control compliance efforts. Bio-safety initiatives are largely focused on vetting particular research projects and ensuring that they are in line with ethical standards. Export control compliance efforts are focused on ensuring that restrictions on the international movement of items are enforced. While the two efforts could be designed to complement each other, there is a danger of over-burdening already stretched institutes. This is true even among the more institutionalized surroundings of universities and research institutes.[110]

Good practices and guidance documents

Actors from the policy community and in industry and academia have identified approaches to strengthen compliance with export controls and limit the risks of diversion and misuse. The 2016 Symposium on Export Control of Emerging Biotechnologies is an example of bringing actors from these different backgrounds together to identify gaps in and issues with the existing regulatory frameworks. In their findings, the participants in the symposium identified 17 emerging biotechnologies of concern and recommended that four of these should be addressed as a priority.[111]

Monitoring developments in and establishing controls over synthetic biology to improve security has been a topic of much discussion, specifically on issues such as gene synthesis and oversight of the trade in DNA segments, genes and whole genomes. The International Gene Synthesis Consortium (IGSC), established in 2009, which currently comprises seven partners responsible for approximately 80 per cent of international commercial gene synthesis, implements screening procedures against potential misuse. The companies involved rely on the 'know your customer' principle and a

[106] Representative of German governmental research institution (note 102)
[107] Representative of German governmental research institution (note 102)
[108] Representative of German governmental research institution (note 102)
[109] Representative of German governmental research institution (note 102)
[110] See also Clevestig, P., *Handbook of Applied Biosecurity for Life Science Laboratories* (SIPRI: Stockholm, 2009), <https://www.sipri.org/publications/2009/handbook-applied-biosecurity-life-science-laboratories>.
[111] Fairchild, S. et al., *Findings from the 2016 Symposium on Export Control of Emerging Biotechnologies*, CNS Occasional Papers no. 26 (James Martin Center for Nonproliferation Studies: Monterey, CA, Apr. 2017).

documentation system that permits questionable cases to be examined individually to confirm end-use.[112]

There are only a limited number of targeted compliance-related guidance documents on the biotechnology sector. The website of Australia's Department of Defence provides a generic guide that introduces export controls and their applicability to the biotechnology sector.[113] The guide is mostly focused on the specific Australian legislation, the goods covered by the controls and the control of both tangible and intangible transfers of technology. The US Bureau of Industry and Security (BIS) provides additional guidance with regard to research in the biotechnology sector, which discusses issues such as deemed exports, fundamental research and licensing exemptions that are specific to goods and technologies in the sector.[114] No sector-specific documents appear to have been published by the EU or any EU member state. However, as part of the Wiesbaden Process, an industry event focused on the bio sector was organized by the UN 1540 Committee together with the German Government.[115]

Transport or distribution service providers

Impact of dual-use and arms export controls

Developments in the ICT sector and 3D printing/additive manufacturing mean that the transfer of technology now increasingly takes place through digital transmission rather than physical transportation using traditional modes of transport (air, sea, rail and road).[116] Nonetheless, the range of transport or distribution service providers continues to grow due to continuing increases in international trade (see figure 3.1). According to the European Commission, the transport sector currently accounts for 3.7 per cent of GDP and 5.1 per cent of employment in the EU.[117] The level of interdependence and overlap of functions provided by transport or distribution service providers is also increasing. Freight forwarders now operate container ships and container shipping companies own freight forwarders. The postal authorities and express parcel services are now also important actors.

Moreover, the number of ancillary and trade-facilitation services that transport and distribution service providers can offer continues to expand, increasing their role in the supply chain. These services range from handling to packaging, customs processing, consolidations, documentation, the sale of insurance and customs clearance.[118] This presents both an opportunity and a challenge. The expansion in the range of services means that the companies involved can potentially provide an additional level of control in the screening process. However, this expansion also increases the responsibilities of the companies and the number of requirements that their export control and compliance divisions must fulfil. The rise of e-commerce retailers is further

[112] SIPRI and Ecorys (note 11), pp. 36-41. This information was based on a background paper provided by Peter Clevestig.

[113] Australian Government, Department of Defence, 'Export controls on materials, equipment and technology used in the biotech industry', n. d., <http://www.defence.gov.au/ExportControls/Biotech.asp>.

[114] US Department of Commerce, Bureau of Industry and Security, Chemical and biological controls: General information, Jan. 2014, <https://www.bis.doc.gov/index.php/policy-guidance/product-guidance/chemical-and-biological-controls>.

[115] 'Risks, Challenges and Responses: Industry's Effective Practices in Responding to Biosecurity Risks', A Conference in Support of Implementing UN Security Council Resolution 1540 (2004) and bilateral discussion at the German Federal Office of Economics and Export Control (BAFA), Information Note, <http://www.un.org/fr/sc/1540/documents/Information%20Note%20Wiesbaden%20Bio%20Security%20Conf%202013-83.pdf>.

[116] See SIPRI and Ecorys (note 11). This information was based on a background paper provided by Martin Palmer.

[117] European Commission, DG Competition, 'Overview: EU competition policy in the transport sector', Dec. 2015, <http://ec.europa.eu/competition/sectors/transport/overview.html>.

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

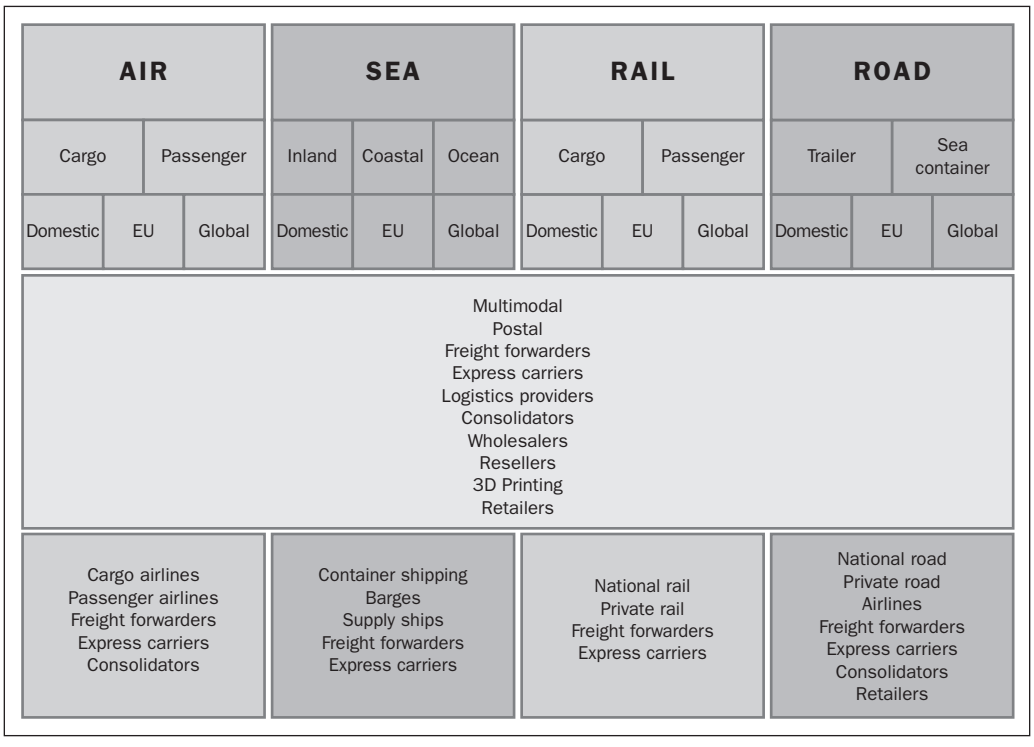

Figure 3.1. Key components of the transportation sector

Source: Palmer, M., Background paper on transport sector for SIPRI and Ecorys, *Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review* (European Commission: Brussels, Nov. 2015).

transforming the transport and distribution service provider landscape. Companies such as Amazon and Alibaba make it possible for smaller producers to deliver products directly to their customers.[119] This has assisted the emergence of an ever-expanding community of smaller 'originators of trade', some of which have no awareness of compliance-related issues or may even be actively seeking to by-pass controls.[120] Some efforts have been made to improve compliance standards among e-commerce retailers but—given their business models—it is hard to see how existing ICP guidelines can be applied.[121]

The extent to which transport service providers are affected by the EU's dual-use and arms export controls is unclear. According to the European Commission, only 48 licences for the transit of dual-use goods, with a combined value of €108 million, were issued by EU member states in 2013. Consolidated data on the number of licenses issued for the transit of military goods is not available. The Netherlands, which is one of the most active states when it comes to imposing controls in this area, issued over 1000 licences for the transit of military goods in in 2016.[122] However, this in no way reflects the impact of ICP requirements on transport and distribution service provider companies, since the relevant regulations go beyond dual-use export controls and include—in particular—the implementation of EU sanctions and US re-export controls. Moreover, screening and preventive measures are not reflected in licence applications, since the current control system in the EU largely applies an end-user control principle based on very few, targeted cases where authorities have information

[119] Representative of industry association (note 5).
[120] Representative of industry association (note 5).
[121] Representative of industry association (note 5).
[122] Government of the Netherlands, 'Maandelijkse rapportage doorvoermeldingen militaire goederen [Monthly reporting on transit reports military goods]', 2 May 2017, <https://www.rijksoverheid.nl/onderwerpen/exportcontrole-strategische-goederen/documenten/rapporten/2016/10/01/overzicht-doorvoer-militaire-goederen>.

about potential misuse. In addition, the customs requirements and controls which apply at the moment the physical items leave the EU, such as the form in which the export authorizations are to be presented and validated, and in some cases returned to the licensing authority, vary in each member state. The result is exceptions to the standard process, and therefore increased costs and risks of non-compliance.[123]

Actor-related challenges

A number of factors can limit the ability of transport and distribution service providers to effectively implement the provisions on transit and trans-shipment control in the EU's arms and dual-use export controls.[124] First, the roles and responsibilities of transport providers are specified not in the EU Common Position or the EU Dual-use Regulation, but in customs law. While there is a requirement to apply for a transit or trans-shipment licence under the EU Common Position and—in a narrower range of cases—under the EU Dual-use Regulation, which actor in the supply chain is required to do so—the exporter overseas, the freight forwarder, the airline or the express carrier—is often unclear.[125] Further confusion might be added by the recast of the Dual-use Regulation, which looks set to expand the range of cases in which a transit or trans-shipment licence would be required for dual-use goods. In particular, the proposed language specifies that the catch-all controls and assessment criteria—including the new language on human rights, international humanitarian law and terrorism—would also apply to transit. A representative of the transport sector expressed concern over the proposed new language, arguing that it would expand the range of cases in which a licence would be required without clarifying where responsibility for obtaining one should lie.[126]

Second, transport and distribution service providers are not the manufacturer of the commodities and have no expertise on their technical characteristics. They are reliant on the information supplied by the shipper from the country of export, the supplier or the manufacturer.[127] Most transportation companies will have some kind of formal or informal alert system in place to try to identify suspicious transactions.[128] However, these 'red flag' systems are largely based on an analysis of the documentation and other information that has been supplied by the exporter. Third, transporters often have thousands, or even millions, of customers that between them ship tens of millions of commodities. A representative of one company noted that since it carried out more than a million shipments per day and operated in more than 200 countries, any obligation with regard to export controls imposed on the carrier would have to be laid out extremely clearly in the regulations in order to be feasible.[129] Fourth, the transporter works in multiple jurisdictions and with multiple regulatory bodies, in a world where classification systems are not harmonized and there is little or no guidance on the relation between them.[130] Furthermore, the transporter seldom acts as either exporter or importer of record or has legal ownership over the commodities transported.[131] In addition, freight forwarders provide services according to shippers'

[123] Legal adviser, Global transport company, the Netherlands, communication with the authors, 2 June 2017.
[124] SIPRI and Ecorys (note 11).
[125] Legal adviser (note 123).
[126] Legal adviser (note 123).
[127] Palmer, M., The transport sector as counterproliferation partner, 'Restricted parties and the transport sector', *SIPRI Good Practice Guide* no. 2 (Sep. 2016), <https://www.sipri.org/publications/2016/restricted-parties-good-practice-guide>, p. 3.
[128] See SIPRI and Ecorys (note 11).
[129] Legal adviser (note 123).
[130] Legal adviser (note 123).
[131] See SIPRI and Ecorys (note 11).

requirements; they act as logistics service providers and are not the originators of trade, as is often the case for shippers. The two functions are different and therefore need differently structured ICPs. Guidance on how the ICPs and compliance tools of the two could interact or complement each other would probably be advantageous for both.[132] At the same time, exporters in all the sectors categorized in the present analysis require transport value-added solutions that can systematically identify, route and monitor their controlled exports.[133] Operators that can meet such a demand will stand out from the crowd in an increasingly competitive industry.[134]

Good practices and guidance documents

Transporters need to be aware of the constraints and opportunities inherent in their position in the supply chain and develop their compliance measures and a portfolio of added value services accordingly. A number of supply chain compliance programmes and standards are in place within the EU, such as the United Nations Office of Drugs and Crime (UNODC) Container Control Programme, the EU AEO scheme, the Transported Asset Protection Association (TAPA) Air Cargo Security Standard, the International Air Transport Association (IATA) Secure Freight programme and the International Organization for Standardization (ISO) standards and programmes.[135] However, these are largely optional and mainly driven by customer demand rather than regulatory requirements. In addition, none of these programmes effectively integrates all the issues pertinent to the enforcement of the EU's dual-use and arms export controls. Moreover, it is difficult for an authority or a business to identify a company that has obtained a particular compliance programme standard, and for company compliance officers to defend the cost of implementing such tailor-made programmes, which are usually in-house efforts.[136] There is therefore significant scope for additional work on integrating export control compliance-related measures into the safety-focused standards that have been developed.[137] The International Federation of Freight Forwarders Associations (FIATA) is updating the entire syllabus of the 'FIATA Minimum Standards' to incorporate safety and security measures and export trade compliance control.[138]

There are a small number of compliance-related guidance documents targeted at transport or distribution service providers. A US Department of Commerce guidance document specifically targeted at freight forwarders proposes a number of measures, such as checklists, export management and compliance programmes, active engagement with the export control authorities and building compliance partnerships with all the parties involved.[139] In addition, SIPRI has published a series of good practice guides for the transport sector.[140] There are guides on restricted parties, red flags, and transit and trans-shipment, as well as a compilation of additional guidance documents from other sources. The series provides specific guidance for freight forwarders on the lessons learned from setting up and implementing an ICP for a company in the

[132] Representative of industry association, communication with the authors, 13 June 2017.
[133] Legal adviser (note 123).
[134] Legal adviser (note 123).
[135] See SIPRI and Ecorys (note 11).
[136] Legal adviser (note 123).
[137] Legal adviser (note 123).
[138] Representative of industry association (note 132).
[139] US Department of Commerce, Bureau of Industry and Security, Office of Exporter Services, Export Management and Compliance Division, 'Freight Forwarder Guidance', Feb. 2012, <https://www.bis.doc.gov/index.php/forms-documents/compliance-training/export-management-compliance/620-new-freight-forwarder-guidance/file>.
[140] The Transport Sector as Counterproliferation Partner SIPRI Good Practice Guide series is available at <https://www.sipri.org/research/conflict-and-peace/transport-and-security/transport-service-providers/recent-pubs>.

transport sector. The document for freight forwarders provides guidance on advance data collection, vetting clients and identifying restricted goods, as well as the elements of 'whole-of-supply-chain compliance'.[141] The document on lessons learned focuses on the ICP aspects of management commitment, responsible officials, risk assessment, export compliance services, relations with governments, record keeping, audits and training.[142]

Academia and research

Impact of dual-use and arms export controls

Developments in technology and scientific practices mean that academia and research institutions often 'export' items that are subject to dual-use controls. For example, in a number of cases scientists have published research online that details the processes through which items subject to dual-use export controls can be produced. These actions can be seen as constituting an export of intangible goods and therefore subject to control. Moreover, in the biological, chemical and nuclear fields, work in academia or research might involve transfers of physical items subject to export controls and create avenues for proliferation to take place. This issue is particularly relevant and challenging in the EU, where academic freedom is enshrined as a core value in article 13 of the EU's Charter of Fundamental Rights.[143] In recent years a number of academics have argued that the freedom to carry out and publish certain types of research has been restricted by dual-use export controls.[144]

Actor-related challenges

Representatives from research and academia highlighted a number of compliance-related challenges. The representative of one research organization producing new technologies for the private sector and government (including a defence ministry) noted that the organization is often developing entirely new products. It can be extremely difficult to determine whether these are subject to dual-use or arms export controls.[145] The representative also noted that since the customer is usually in the private sector or a government, the work is not covered by the exemption for fundamental—also referred to as 'basic', as opposed to 'applied'—research. However, the organization often cooperates with universities that work mostly in the field of fundamental research. Since the outcome of the collaboration will be a product for the private sector, the universities are required to classify the technology and make statements regarding potential dual uses, which they often find hard to do.

One representative of a British University highlighted a range of compliance-related challenges: sourcing higher education-specific guidance from experts; interpreting concepts such as 'goods' and 'exports' in ways that are meaningful to academic researchers; the wide breadth of research that is carried out in most research-intensive

[141] Jones, S., The transport sector as counterproliferation partner: 'Counterproliferation good practice for freight forwarders', *SIPRI Good Practice Guide* no. 4 (Sep. 2016), <https://www.sipri.org/publications/2016/freight-forwarders-good-practice-guide>.

[142] Orzel, R., Pal, D. and Heine, P., The transport sector as counterproliferation partner, 'Export control compliance and the transport sector: lessons for internal compliance programmes', *SIPRI Good Practice Guide* no. 5 (Sep. 2016), <www.sipri.org/publications/2016/internal-compliance-programmes-good- practice-guide>.

[143] Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, C364, 18 Dec. 2000, pp. 1–22.

[144] See Charatsis, C., 'Setting the publication of dual-use research under the export authorisation process: the H5N1 case', *Strategic Trade Review*, vol. 1, no. 1 (autumn 2015), pp. 56–72; and Biercuk, M., 'Science and the slammer: the consequences of Australia's new export control regime', The Conversation, 15 Oct. 2012, <http://theconversation.com/science-and-the-slammer-the-consequences-of-australias-new-export-control-regime-10127>.

[145] Contract Manager, Research Organization, the Netherlands, Interview with author, 5 Apr. 2017.

universities; the wide range of industry sectors with which researchers working at the university might engage; the relatively small volume of research activities that are actually affected by dual-use and arms export controls, which makes it hard to justify establishing a dedicated compliance office; the highly devolved nature of many universities' operations; and the differences between the export control regulations they are subject to and those that their research collaborators in the USA face.[146]

Both national laws protecting academic freedom and the EU Dual-use Regulation contain language that exempts certain types of academic research from the EU's dual-use and arms export controls, but these provisions can be difficult to interpret. The representative of a national academy of sciences argued that it is often extremely difficult to determine whether the work that a scientist is doing is covered by the protection of 'freedom of research' in Germany's Constitution.[147] In basic research in particular, the final results and potential applications are often unpredictable.[148] The Dual-use Regulation states that controls on 'technology' transfers do not apply to information 'in the public domain', to 'basic scientific research' or to the minimum necessary information for patent applications.[149] However, interpreting concepts such as 'basic scientific research' and 'in the public domain' can be difficult, as demonstrated by diverging court rulings on how to apply these concepts in EU member states and the USA.[150]

The representative of a national academy of sciences noted that, especially among younger researchers, there seems to be 'a lack of awareness' of scientists' responsibility to assess the potential risks associated with their research.[151] In addition, in some cases academia has proved fairly unresponsive to outreach initiatives. The representative of a licencing authority of an EU member state gave the example of an outreach event for academia and research institutions, for which it was difficult to find participants.[152] Another noted that academia does not always show great openness to the export control authorities and usually only a few representatives respond positively to invitations to outreach conferences.[153] On the other hand, some research institutes or individuals have been interested in receiving updates about the dual-use legislation. One licensing authority representative argued that those working in research and academia are reluctant to be instructed on additional rules as they believe that they already operate in an over-regulated environment.[154]

Good practices and guidance documents

Representatives from research and academia highlighted several areas of compliance-related good practice. Some referred to the need for awareness raising among scientists by developing codes of conduct.[155] Others suggested developing ICPs based

[146] Director of research service, British University, Correspondence with author, 28 Mar. 2017.

[147] Head of Office of the Committee for the Handling of Security-relevant Research, Germany, Correspondence with author, 7 Apr. 2017.

[148] Head of Office of the Committee for the Handling of Security-relevant Research (note 147).

[149] Council Regulation (EC) no. 428/2009 of 5 May 2009 (note 2).

[150] See Charatsis (note 144)

[151] Head of Office of the Committee for the Handling of Security-relevant Research (note 147).

[152] Representative of EU member state licensing authority, communication with the authors, 2 June 2017.

[153] Representative of an EU member state export control authority, communication with the authors, 6 June 2017

[154] Representative of EU member state licensing authority (note 152).

[155] One respondent from a national academy of science listed as a best practice tool for raising awareness among scientists, German Research Foundation (DFG) and the German National Academy of Sciences, Leopoldina, *Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security-relevant Research* (DFG and German National Academy of Sciences: Bonn and Halle, 28 May 2014), <https://www.leopoldina.org/uploads/tx_leopublication/2014_06_DFG-Leopoldina_Scientific_Freedom_Responsibility_EN.pdf>.

on guidance from the national export licensing authorities.[156] In this regard, the UK's 'Higher Education Guide and Toolkit on Export Controls and the ATAS Student Vetting Scheme', and the higher education-specific training session held in November 2016 by the British Export Control Organization and Project Alpha at King's College, London were both regarded as useful sources of information.[157] Another case of good practice in dealing with export controls has been established by a Belgian university, KU Leuven, where a 'Committee for Ethics in Dual-use Research' has been established.[158] Researchers are encouraged to submit an 'application for advice', specifying the title of the research and whether its potential outcomes could in any way have military or WMD-related applications. If the research raises dual-use concerns, the committee contacts the competent authority to seek advice.

A respondent from a research centre located in Belgium shared the internal good practices adopted by the institute, which had created a flow chart to help researchers understand when they need to apply for a licence. Each department at the institute deals with a different research topic. Department directors were instructed to check whether the technology being developed under a particular programme could be classified as dual use. This process allowed the institute to create a 'Technology Integration Map' that covered all the technologies developed internally. To keep the map up-to-date the process needs to be repeated on a regular basis, given the fact that technology changes rapidly. The Belgian research centre's experience shows that for research institutes which 'develop technology 10 years before industrial application' reliance on the judgement of technical experts during classification is crucial, since dual-use lists compiled by regulators are not composed with frontier technologies in mind.[159]

A number of government guidance documents are available targeted at academia and research institutions. The German export licensing authority, BAFA, publishes an information leaflet that explains export controls on technology transfers and technical assistance for universities and research institutions.[160] It presents a set of examples of critical technical assistance and a guide to detecting possible attempts at procurement. The British Department for Business, Innovation and Skills publishes a guide for academics and researchers in the UK that explains the general exemptions for basic research and information in the public domain, and the conditions under which export controls apply, with case studies and an overview of the legislative background.[161] The Australian Government has also provided brief scenarios to illustrate cases where export controls may apply, including scenarios common to academics and researchers.[162]

[156] Another German research organization elaborated an internal export control system following the guidelines provided by the competent national authority (BAFA).

[157] *Higher Education Guide and Toolkit on Export Controls and the ATAS Student Vetting Scheme*, Drafted in partnership with the Association of University Legal Practitioners and Project Alpha of King's College, London. In partnership with the Export Control Organization and the Foreign and Commonwealth Office, 2 Apr. 2015 <http://projectalpha.eu/wp-content/uploads/sites/21/2015/07/20150407_Guidance_for_Academia_on_Export_Controls_UpdatedCR.pdf>; and Event hosted by the University of Oxford in association with the Association of Research Managers and Administrators (ARMA).

[158] Ethics committee for Dual-use Research, KU Leuven <http://set.kuleuven.be/ethicsatarenberg/dual-use>

[159] Export Compliance Manager, Research Centre, Belgium, Correspondence with author, 8 May 2017.

[160] German Federal Office for Economic Affairs and Export Control (BAFA), *Information Leaflet on Responsibilities and Risks in Case of Know-how Transfer: Control of Technical Cooperation with Individuals, Universities and Research Institutions*, Part 1: Sensitization, 1 Aug. 2005, <http://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/afk_information_leaflet_know-how_transfer.pdf?__blob=publicationFile&v=2>.

[161] Department for Business Innovation and Skills, Export Control Organization, *Guidance on Export Control Legislation for Academics and Researchers in the UK* (Department for Business Innovation and Skills: London, Mar. 2010), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/68680/Guidance_on_Export_Control_Legislation_for_academics_and_researchers_in_the_UK.pdf>.

[162] Australian Government, Department of Defence, Defence Export Controls, 'Defence Trade Controls Act: Scenarios', <http://www.defence.gov.au/ExportControls/Scenarios.asp>.

The 'Toolkit on Export Controls' targeted at British universities provides a comprehensive set of guidelines on potential dual-use concerns relevant to universities in the UK.[163] It contains an overview of the applicable legislation and licencing procedures, an interpretation of key definitions and a discussion on the areas of research potentially affected by export controls and the exemptions that may apply. Other institutes, such as the Royal Netherlands Academy of Arts and Science, the National Academy of Sciences Leopoldina, the German National Research Foundation (DGF) and the Robert Koch Institute, have produced guidance documents that highlight the dual-use potential of life science research and issues of biosecurity.[164] They also provide guidelines on the criteria that should be used to assess dual-use research, the stage at which this assessment should be made and who should be responsible for making it. Nonetheless, while they cover the life sciences in some detail and provide case studies on nuclear and nanotechnology research, they do not provide instructions tailored to other specific fields of research.

[163] Association of University Legal Practitioners and Project Alpha (note 157).

[164] Royal Netherlands Academy of Arts and Science (KNAW), 'Improving bio-security: assessment of dual-use research', Dec. 2013; German Research Foundation (DFG) and the German National Academy of Sciences (note 155); Robert Koch Institute, 'Dual use potential of life sciences research: Code of conduct for risk assessment and risk mitigation', 14 June 2013, <http://www.rki.de/EN/Content/Institute/Dual_Use/code_of_conduct.html>.

4. Cross-sector and actor compliance-related challenges

Chapter 3 identified a number of sector- and actor-specific compliance-related challenges, but many issues affect stakeholders from across the different sectors. This chapter summarizes some of these issues: (*a*) the particular challenges facing SMEs; (*b*) differences in the implementation of controls in different EU member states, or location-related challenges; (*c*) product classification; (*d*) managing multinational supply chains; (*e*) ITT controls; complexity, multiplicity and vagueness; (*f*) risk assessments; and (*g*) securing support from senior management and mobilizing sufficient resources.

Particular challenges for SMEs

Because of their size, it might be possible for SMEs to tailor their compliance programmes better than larger companies. However, they are also less likely to have the expertise and the contacts with government officials that would be found in a multinational entity.[165] The majority of the companies that contributed to the 2015 SIPRI/Ecorys study agreed that trade compliance-related challenges vary according to the size of the firm. This point was confirmed in the European Commission's impact assessment as well as the interviews for this study. This is not surprising given the fact that one of the main differences in terms of trade compliance challenges between large and small or medium-sized companies, identified in the 2015 study and confirmed in the 2017 interviews, is the level of human and financial resources available to work on export control within the company.[166]

Interviewees identified several types of challenges for SMEs:[167]

1. *Technical challenges*: The lists of controlled items produced by the various multilateral regimes are constantly evolving. For a small company it is not easy to stay up to date with these changes. In this regard, the assistance they receive from industry associations is fundamental.
2. *Administrative challenges*: These are mostly related to procedures for obtaining an export authorization, which can be highly complex and require information on end-users that is not always easily available.
3. *Legal challenges*: Legal complexity and lack of clarity/ambiguities in the law.
4. *Logistical challenges*: Most of the companies offering logistics solutions for the strategic trade supply chain are not in a position to offer a product that can systematically identify, monitor and track controlled exports according to their needs across the several jurisdictions the commodities might traverse.[168]

Because of this disparity, compliance requirements and conditions for accessing facilitated/ex-post control procedures might favour larger companies. For example, in order to benefit from EUGEAs, companies often have to register, follow specific record-keeping procedures, carry out self-auditing and prepare for compliance visits. This generates costs for companies. Smaller companies are less likely to have such procedures already in place, or more likely to incur costs that are disproportionate

[165] Representative of a UK industry association, Correspondence with author, 20 Mar. and 24 April 2017.
[166] Technical expert (note 26); and Managing Director (note 26).
[167] Technical expert (note 26); and Sales Manager, Machine Tool company, Italy, Correspondence with author, 24 and 31 Mar. 2017.
[168] Legal adviser (note 123).

to their size. If, as planned, the recast of the Dual-use Regulation makes it obligatory for companies that use EU General Export Authorizations to have an ICP in place, this burden could increase. This could be partly addressed by systematically involving the associations and sectors that primarily represent SMEs in providing support and guidance, which would require them to establish the capacity to do so. In this context, it would be helpful to identify companies that could contribute to the development of export control compliance guidelines and tools suitable for SMEs.[169]

Best practices and available guidance

There are very few guidance documents available that are specifically geared to SMEs. The Australian Department of Defence refers to the 'Australian Best Practice Guide for the Management of Controlled Exports and Technology', which provides specific advice for SMEs on tailoring their compliance systems according to their involvement in the market and the type of products and technologies they trade, and provides concrete examples.[170] The European Commission has produced an SME-specific guide on compliance-related issues. However, the guide is mainly focused on the integration of international standards on Human Rights into ICPs and does not cover dual-use and arms export controls in any substantive detail.[171]

Differences in the implementation of controls

The EU Common Position forms part of the EU's CFSP, one of the areas of 'special' EU competence. Measures adopted in this area are legally binding on member states but they are free to determine their mechanisms for implementation and the EU has no legal powers to sanction non-compliance. Although the Dual-use Regulation forms part of the EU's 'common commercial policy', one of the areas of 'exclusive' EU competence, certain aspects of controls—particularly licensing decisions and enforcement—have been left in the hands of EU member states. As a result, there continue to be substantial differences in terms of how the EU's arms and dual-use export controls are implemented at the national level. This includes determining whether items are controlled through the use of individual, global or general licences (where no EUGEAs are in place) and the way in which applications for licences for similar exports are assessed by different EU member states. However, the extent to which this is the case has always been difficult to establish. The specific areas where concerns have been raised about different national practices are the implementation of 'catch-all' controls and different processing times for licence applications. Several companies have highlighted the negative impacts in terms of the 'distortion of competition' and 'legal uncertainty' produced by the uneven application of the catch-all clause.[172]

Another key variation is whether the licensing authority operates a system of electronic licensing or still relies on hard copy documentation. Companies based in states where electronic licence procedures have been introduced argued that this has not led

[169] Bauer S. and Bromley, M., 'The dual-use export control policy review: balancing security, trade and academic freedom in a changing world', Non-Proliferation Consortium Paper, Mar. 2016.

[170] Australian Government, Department of Defence and Australian Industry Group, *Australian Best Practice Guide for the Management of Controlled Exports and Technology*, May 2014, <http://www.defence.gov.au/exportcontrols/_master/docs/australian-best-practice-guide-for-the-management-of-controlled-exports-and-technology-may14.pdf>.

[171] European Commission, Internal Market, Industry, Entrepreneurship and SMEs, *My Business and Human Rights: A Guide to Human Rights for Small and Medium-sized Enterprises* (European Commission: Brussels, 20 May 2015), <http://ec.europa.eu/DocsRoom/documents/10375/attachments/1/translations/en/renditions/pdf>.

[172] Legal Officer, Chemical company, the Netherlands, Correspondence with author, 8 June 2015; Interview with author, 17 August 2015; Legal Officer, Chemical company, Belgium, Correspondence with author, 19 June 2015; Export Control Officer, Chemical company, Germany, Correspondence with author, 26 June 2015.

to significant improvements since problems remain with their speed and effectiveness. However, companies based in states where electronic licence procedures have not been introduced argued that such systems might make the process faster, since they currently need to send original documents through the regular mail.[173] The administrative burden associated with licensing procedures may also have consequences for the compliance costs associated with staff capacity, screening systems, software and databases, and training.[174] These in turn will differ depending on the frequency with which applications are made by a particular company, the degree of access to fast track procedures, the speed of processing, the responsiveness of licensing authorities to queries and the time/capacity they have to respond, as well as the specific paperwork required, which differs between countries and for different types of licences.

Best practices and available guidance

One of the outcomes of the review of the EU Common Position—completed in 2015—was to introduce some improvements in the mechanisms for sharing information among member states, particularly with regard to approved and denied export licences.[175] As part of its draft recast of the EU Dual-use Regulation, the European Commission has proposed more detailed processes for reporting and information sharing, particularly with regard to the implementation of catch-all controls and processing times for licences. These measures may go some way towards smoothing out the differences between how EU member states implement their dual-use export controls. However, it is not clear that it would ever be possible—or even desirable—to create a truly 'level playing field' as long as key aspects of policy implementation—particularly licensing decision making—remain in the hands of EU member states. In addition, until there are clearly agreed standards in these areas, it is unclear what contribution targeted guidance on ICP implementation could make. However, enhanced information exchange on different practices, which identifies issues that present particular challenges for companies and other stakeholders in one country but have been successfully addressed in another, would go some way towards addressing this issue.

Product classification

Classifying products in order to determine whether and if so, how they are covered by dual-use or arms export controls is a common challenge highlighted by representatives from different sectors in a number of EU member states. Large enterprises can potentially produce or work with thousands of items—including parts and components—that might be on the EU military list or EU dual-use list, or affected by catch-all controls. In addition, product classification is an issue for companies not only when they are exporting items themselves, but also when dealing with customers and suppliers. Suppliers that do not export, or do not export to states outside the EU, face a particular set of challenges when it comes to complying with dual-use and arms export controls. For dual-use goods, this group of companies does not have to apply for licences, but may be asked to classify items and inform those that do export, as part of a system or the item, that this item is listed as a dual-use good. One company representative from the defence and aerospace sector noted that the main compliance-related challenge was responding to the 'overwhelming' volume of product export control classification

[173] SIPRI and Ecorys (note 11), p. 230.

[174] SIPRI and Ecorys (note 11), p. 231.

[175] Council of the European Union, 'Council conclusions relating to the review of Common Position 2008/944/CFSP on arms exports and the implementation of the Arms Trade treaty (ATT)', 20 July 2015, http://data.consilium.europa.eu/doc/document/ST-10900-2015-INIT/en/pdf.

requests from partners, suppliers and customers.[176] At the same time, a wholesaler could be faced with the reverse problem—that it lacks in-depth technical knowledge about the items but needs to export them. Wholesalers thus have to rely on producers to share those classifications.

However, the wide and expanding range of goods and technologies that are subject to dual-use export controls also means that some authorities, particularly those in smaller EU member states, may be unable—because of a lack of resources or expertise—to respond in a timely or accurate way to product classification requests. As a company representative from the defence and aerospace sector noted, product classification issues can become particularly tricky when dealing with highly technical and complex topics such as cryptography.[177] Knowledge or expertise in these areas is extremely scarce, which makes it hard for export licensing officials to make accurate decisions, or to challenge them if it looks like errors have been made.

Good practices and available guidance

In the USA companies can submit a production classification request for dual-use goods to the BIS via the Simplified Network Application Process-Redesign (SNAP-R).[178] Companies can submit up to six classification requests at a time and are encouraged to provide 'sales brochures, catalogues, and other descriptive information' in order to help determine the category that captures the item concerned.[179] Until 1 June 2014, the British Government maintained a Commodity Classification Service that helped companies to understand whether they needed to apply for a licence. However, 'the extreme pressure of workload on the Technical Assessment Unit and the whole of the Export Control Organization arising from the introduction of a new computer system' led to the service being discontinued.[180] There are, however, 'provisional plans for its resurrection' in the future. This revival will probably be linked to the official launch of the new LITE electronic licensing system, which will replace the current SPIRE system 'by the first quarter of 2018'.[181] One representative of a British industry association noted that this decision 'left many firms who are unaware of whether they need licences or not with little alternative but to "self-rate" their products, or to utilize the services of expensive consultants'.[182]

Managing multinational supply chains

When establishing their internal compliance programmes or, more generally, when dealing with export controls, multinational companies in particular must consider multiple regulations.[183] Because they deal with several products and customers, 'more aspects of compliance may be involved'.[184] In addition, the headquarters of multinational companies are responsible for guaranteeing the implementation of export control regulations in multiple locations. This makes it important to 'find a common denominator to apply everywhere in a harmonized way' while avoiding a

[176] Security & Export Control Manager, Aerospace company, France, Correspondence with author, 10 Apr. 2017.
[177] Representative of industry association (note 132).
[178] US Bureau of Industry and Security (BIS), 'Commerce control list classification', accessed 28 June 2017, <https://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification>,.
[179] US Bureau of Industry and Security (BIS), 'Classification request guidelines', accessed 28 June 2017, <https://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/classification-request-guidelines>.
[180] Representative of industry association (note 132).
[181] Representative of industry association (note 132).
[182] Representative of industry association (note 132).
[183] Chief export compliance officer (note 39).
[184] Chief export compliance officer (note 39).

one-size-fits-all approach.[185] The challenges of operating in multiple national jurisdictions are naturally multiplied when different or even contradictory interpretations and rules are being applied (see above). Another trade compliance-related challenge multinational companies have in common is the amount of time and effort that must be spent doing due diligence and risk assessment checks while acquiring or merging businesses covered by a wide variety of laws in multiple jurisdictions.[186] Finally, it is worth highlighting that spreading a compliance culture and embedding compliance procedures in small subsidiaries is a challenge for larger companies, which makes SME challenges also 'big company' challenges.[187]

Good practices and available guidance

One interviewee explained how multinational supply chains are not a problem if they are adequately factored into the compliance process. In this case, compliance positions have been established in all production facilities and sales offices. Export applications are submitted to the licensing authorities where the production facility is located, planning ahead by submitting them well in advance to take account of differing processing times (30 days or 60 days in the two EU member states the company exports from). US extraterritoriality rules can be avoided by procuring special materials from Europe. Classification is based on the materials used, and each item is given a part number and full material description. An array of resources are available for company training for new and current staff, most of which is internal and not acquired from the outside or based on outside guidelines. Resources include regular in-house training with guest speakers, monthly webex presentations on different topics, internal conferences and online training, as well as attendance at external events.[188] Every employee must undergo compliance training, which is arranged through the HR department at least once every two years.[189]

A company from the automotive sector stated that it had established a global role responsible for export control regulatory compliance to reflect the multinational nature of the company's operations.[190] Its establishment has been coupled with regional offices, which regularly communicate with country risk managers since each country has its own laws and regulations governing the import and export of materials, products, information and technology. The procedures at its base are internally developed and periodically revised. The company representative also indicated that an element of good practice is the adoption of an 'International Sanction Matrix', which summarizes the 'legal touch points' of the company's business with export control laws and regulations in the different jurisdictions in which they operate, such as the USA, the EU and Japan.

Intangible technology transfer controls

ITT is a key element of daily life for many global business entities and supply chains. ITT can occur through email attachments, server uploads or downloads, cloud computing or other Internet-sharing platforms. A large multinational company will carry out ITT numerous times every day, involving transfers between different branches

[185] Chief export compliance officer (note 39).

[186] Director of compliance, Defence and Aerospace multinational company, Italy, communication with author, 14 June 2017.

[187] Managing director, Semiconductor company, Italy, communication with author, 14 June 2017; and Director of compliance (note 186).

[188] Compliance officer, the UK, communication with author, 10 April 2017.

[189] Compliance officer (note 188).

[190] Compliance manager, Multinational automotive industry, Interview with author, 23 Mar. 2017.

of the company and transfers between itself and other companies in a supply chain. According to a respondent from an electronics company, implementing effective ITT controls in a multinational company is a 'difficult and time-consuming' activity that requires regular training sessions in order to raise awareness and understanding among staff.[191] This can generate significant compliance costs for companies and other stakeholders. Additive manufacturing or 3D printing in particular is transforming modes of production, transportation and sales in many sectors. Moreover, as noted above, ITT controls are one of the key ways in which academia and research have become subject to dual-use export controls. The fact that ITT is difficult for enforcement authorities to monitor makes industry compliance even more important.[192]

Best practices and available guidance

ITT is a recurring theme in both general and sector-specific compliance-related guidance documents. However, for the most part, references to ITT are confined to brief sentences or paragraphs that highlight the fact that transfers of technology—in the form of knowledge or data—can constitute an export and may therefore be subject to export controls and licensing requirements. There are no compliance-related guidance documents with an exclusive focus on ITT. The Australian Industry Group has produced a guide on the management of controlled exports and technology for the Australian Department of Defence. It engages more thoroughly with technology transfers, and includes Australia's requirement for a 'Technology Control Plan' and a full-length example.[193] The British Government provides guidance on the export of technology that while it does not explicitly refer to intangible transfers, does discuss the implications of a number of types of technology transfer that fit into this category.[194] The German licensing authority BAFA has issued a similar guide in German, which covers both the export of technology and technical assistance, and explicitly mentions ITT and specific issues such as the definition of technology and 'cloud computing'.[195]

Complexity, multiplicity and vagueness

Some of the respondents to the 2015 SIPRI/Ecorys study flagged the need for 'legal clarifications' on 'transit provisions', the difference between 'technical data' and 'technical assistance', and ITT and 'brokering activities'.[196] A key message from that study is that legal uncertainty or a lack of clarity increases compliance costs, since different interpretations have to be prepared for and considered. Companies also frequently mentioned that increasingly complex regulations and sanctions, reinforced by vague legal provisions or legal uncertainty, present a particular challenge. With reference to the EU, more than one respondent stressed the importance of harmonizing

[191] Director Export Control & ECO, Electronics Company, Germany, Correspondence with Author, 16 May 2017

[192] Bauer and Bromley (note 169).

[193] Australian Government, Department of Defence and Australian Industry Group, *Australian Best Practice Guide for the Management of Controlled Exports and Technology*, Part Two, Section B, May 2014, <http://www.defence.gov.au/exportcontrols/_master/docs/australian-best-practice-guide-for-the-management-of-controlled-exports-and-technology-may14.pdf>.

[194] British Department for Business Innovation and Skills, Export Control Organization, *Guidance on Export of Technology* (Department for Business Innovation and Skills: London, Mar. 2010), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/15203/Export_of_technology_Guidance_-_URN_10-660_-_new_logo_-_2012.pdf>.

[195] German Federal Office for Economic Affairs and Export Control, Technologietransfer und Non-Proliferation: Leitfaden für Industrie und Wissenschaft (Federal Office for Economic Affairs and Export Control: Frankfurt, June 2016), <http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_technologietransfer.pdf?__blob=publicationFile&v=4>.

[196] Chemical company, Germany, Interview with author, 16 July 2015; Regulatory Affairs Officer, Chemical company, the Netherlands, Correspondence with author, 18 June 2015.

the definitions of key terms that appear in both export and customs legislation.[197] Harmonization should also apply to the functions of the relevant entities in the field of export controls within the EU. The work of DG TRADE, for example, should be aligned with that of DG TAXAUD.[198] In addition, concerns were raised about the lack of clarity in the language of the recast of the Dual-use Regulation with reference to the definitions of exporters and ITT.[199] The issue of vagueness also applies to the functioning of the 'catch-all' controls, which are difficult to implement in the absence of a clear framework.[200] Linked to this is the requirement to establish and maintain multiple 'compliance' systems (e.g. ISO and AEO) and to identify overlaps and synergies with existing compliance processes.

Good practices and available guidance

The main goal of many of the compliance-related guidance documents highlighted in this study is to create greater clarity for the companies and other actors affected by the EU's dual-use and arms export controls. However, as the study demonstrates, there are many gaps in the guidance material available. There is also scope to further clarify the terms and definitions in the EU Dual-use Regulation, such as 'basic research' and 'technology'. Creating systematic ways for customs authorities to provide input into the legal drafting process for trade control regulations, including sanctions, will also increase coherence between different legal concepts.

Risk assessments

Another cross-sector challenge is how a company or an institute that is subject to the EU's arms and dual-use export controls can obtain a more complete picture of the transaction and any potential risks of diversion or misuse, given the partial or limited information it will have at its disposal. Performing these kinds of risk assessments means keeping up to date with 'red flags' such as prohibited or suspicious parties, end-users, end-uses, illicit trafficking routes and so on, as well as legal changes, and integrating these swiftly into company routines. In addition, linked to the issue of how to structure internal compliance procedures, there is the question of how best to ensure the right person in the company receives the information. There are a number of software tools available to help companies perform risk assessments but most of these appear to focus on denied party screening, rather than the broader range of concerns that should be covered by an effective risk assessment framework.[201] Moreover, they tend to be costly, which poses a challenge in particular for SMEs.

The challenge for companies and institutes affected by the EU's dual-use export controls may become more acute as a result of the recast of the EU Dual-use Regulation. The proposed language would require companies to carry out 'due diligence' to establish whether any unlisted dual-use goods that they are planning to export will be used in any of the situations covered by the catch-all clause. It also expands the coverage of the catch-all—which currently covers the supply of items to a military end-user in an embargoed state, or that will be used in connection with a WMD programme or as spare parts for illegally supplied military items—to include exports of items that are, or may be, intended 'for use by persons complicit in or responsible for directing

[197] Representative of industry association (note 5); Senior Manager (note 83); and Representative of EU member state licensing authority (note 152).
[198] Representative of industry association (note 5).
[199] Senior Manager (note 83).
[200] Representative of industry association (note 5).
[201] Representative of EU member state licensing authority, communication with the authors, 7 June 2017.

or committing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination . . . or for use in connection with acts of terrorism'.[202] The challenge is particularly acute for the wide range of goods and technologies that are subject to dual-use export controls, which have entirely benign or positive (and in some cases essential) applications but also have the potential for misuse in the wrong hands.

Good practices and available guidance

The EU Common Position on the export of military equipment has an accompanying User's Guide, which provides guidance on how the eight criteria should be implemented. This document is publicly available and provides information for companies in the defence and aerospace sector on the kinds of risk assessments they should be carrying out and the different sources of information they can rely on when doing so. However, the User's Guide is exclusively focused on transfers of military items to military end-users and does not provide specific guidance on the risks associated with exports of dual-use goods. There is currently no equivalent document on the EU Dual-use Regulation. A number of companies—particularly in the ICT sector—have developed ICPs that encompass both export control-related issues and a wider range of concerns in the human rights field. These could form the basis for the kind of due diligence processes envisaged under the recast of the Dual-use Regulation. For example, Ericsson's Sales Compliance Board brings together different departments to assess the human rights issues associated with a particular sale.[203] The Board can approve or reject deals or make them subject to conditional approval.[204] A company working in the IT security field has put measures in place to ensure, as far as possible, that end-users are not involved in WMD-related activities or in human rights violations, for the subset of products for which such an end-use is a theoretical possibility.[205] This involves using a screening pyramid to determine which parties are involved in the transaction, what they will do with the product and what else they do.[206]

Securing support from senior management and mobilizing sufficient resources

Developing and managing an ICP incurs costs for the company or institute involved. These costs include training and employing the staff needed to set up and run the ICP—not just the members of the compliance team but also sales personnel and other employees that need to understand how the ICP works—as well as purchasing screening software and other support tools. Companies and institutes put ICPs in place because of the benefits they expect to derive from access to simplified export procedures or faster export decisions, the reduced risk of making an illegal export and the increased potential to attract customers and investors. At the same time, measuring the precise benefits that can be derived from implementing an ICP is an extremely difficult task to perform and attempting to do so can lead to under-resourced policies. Since it is impossible to measure the effectiveness of ICPs in terms of profit and loss, commonly used cost-benefit analyses will be misleading, and companies will need to identify other ways to make the case for the mobilization of appropriate resources.

[202] European Commission (note 9).

[203] Purdon, L., *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>.

[204] Purdon (note 203).

[205] Senior Manager (note 83).

[206] Senior Manager (note 83).

Good practices and available guidance

The German approach of legally requiring a member of senior management as the Export Control Responsible Person (*Ausfuhrverantwortlicher*) to be liable for export control compliance and any offences—including the risk of prison—is one way to ensure buy-in from the top and the mobilization of appropriate resources. Another approach suggested by companies is peer benchmarking through informal or formal exchanges on staffing costs and the costs and components of compliance systems, as well as exchanging information about any penalties incurred. Legal requirements can also help compliance officers mobilize the necessary resources, as can penalty provisions.

5. Conclusions

The main components of an ICP are well established and widely recognized. The key principles established by the USA, the EU and individual EU member states over the past 20 years—and in some cases even earlier—are still broadly applicable today. In particular, an effective ICP should have several specific goals:

1. To develop contacts and relationships of good standing between the company and export agencies;
2. To stay informed of updates to the government's export control laws and regulations;
3. To centralize export-related questions and issues;
4. To standardize procedures;
5. To provide early warning and screening of all enquires and orders;
6. To generate coherent and complete documentation on all sensitive export transactions; and
7. To train all employees engaged, either directly or indirectly, in exports.[207]

It is also widely recognized that the exact parameters of an ICP should be tailored to fit the specific needs of the company or other stakeholder that is putting it in place. In particular, an ICP needs to be adapted to the size and structure of the company and integrated into standard procedures and business practices. The various issues linked to the scope and operation of an ICP are discussed below.[208]

The scope of an ICP (the 'what')

1. The ICP must consider the type of product (classification and potential uses), the type of activity, the country of destination (in particular for the implementation of sanctions), the end-use, the end-user and the entities involved, as well as the resulting licensing requirements and prohibitions.
2. The entities involved in a transaction will include the invoicing entity, the receiving entity, banks, intermediaries and transit/trans-shipment points. Intermediaries during transportation could be freight forwarders, shippers and customs agents. The intermediaries and relevant parties in the recipient country might be agents, distributors, brokers, joint ventures, subcontractors and subsidiaries.
3. Applicable laws might concern multiple jurisdictions, some of which may be contradictory, and comprise regular export, transit, trans-shipment and brokering controls as well as sanctions and other restrictive measures (national, regional and international).

How to establish and operate an ICP (the 'how')

1. Processes and procedures are required to facilitate and enable compliance, to monitor compliance (internal audits) and to act where a compliance breach is detected; some form of infrastructure, such as software and screening tools, specialized staff,

[207] Institute for Science and International Security (ISIS), Key elements of an effective export control system, 2003, <http://exportcontrols.info/key_elements.htm>.

[208] The questions to be considered when establishing and implementing an ICP were developed in the context of a previous SIPRI project. Bauer, S., 'Internal compliance: implementation challenges for government and industry', Background paper, Mar. 2015.

awareness raising and training of other staff, and may also involve support from external lawyers and consultancies.[209]

2. An effective ICP will enable a company to communicate with the licensing authorities and facilitate swift processing of applications and queries, as well as regular contact with the authorities.

3. An explicit company policy or written commitment is generally considered a key element.

At the same time, for the person or team tasked with establishing, maintaining or improving an effective ICP, the challenges are manifold.

1. Incentivizing compliance among company staff and making the case for compliance in the business world, which is often driven by speed, competition and market access.

2. Identifying the relevant staff within the company for the purposes of raising awareness and in-depth training. This may involve purchasing, product development, sales, logistics, contract/legal department, finance, IT and HR staff.

3. Mobilizing resources for staff training, software tools and external advice.

4. Securing support from senior management and colleagues.

5. Ensuring that information flows within the company.

6. Designing the most appropriate (effective and efficient) compliance system for the company for both legal requirements (on licensing, prohibitions, record keeping, notification/reporting, but also in line with relevant privacy and data protection requirements) and company policy/risk assessment, which may go beyond the legal requirements in a given country, especially where headquarters are based in a different jurisdiction or where extraterritoriality applies. This will depend on the company's size, structure, product range and markets.

7. Identifying actual needs, benchmarks and international standards for ICPs. Which model to follow? Should industry set voluntary self-compliance standards or develop codes of conduct?

The need for better guidance and greater clarity

This report demonstrates that the type and extent of the impact that dual-use and arms export controls have on different companies and other stakeholders are determined by a range of factors, such as their size, location, product range and market structure. At the same time, there are a number of challenges linked more specifically to the sector in which the company or stakeholder is operating. Some of these sectors have been better served in terms of the production of effective guidance documents. Companies and stakeholders from all sectors have developed compliance-related good practices that could be of benefit to others both within and beyond their sector. The report also highlights a range of cross-cutting compliance-related issues of concern to most if not all of the sectors covered by the study. Some of these issues affect some sectors and actors more than others. For example, implementing controls on ITT will affect multinational companies and research institutes/universities in particular.[210]

There is a clear need to generate better—and better targeted—guidance, resources and other tools, and in other ways promote greater clarity for the companies and

[209] European Commission, 'Strategic export controls: ensuring security and competiveness in a changing world'. A report on the public consultation launched under the Green Paper COM(2011)393, European Commission Staff Working Document, Brussels, 17 Jan. 2013, SWD(2013) 7 final <http://trade.ec.europa.eu/doclib/docs/2013/february/tradoc_150459.pdf>.

[210] European Commission (note 18), p. 16.

stakeholders affected by the EU's dual-use and arms export controls. Some of the greatest need is not for sector-specific guidelines but for 'functional guidance' on particular aspects of export controls where there is a lack of understanding about the scope of controls or where there are clear differences in the way controls are being interpreted at the EU member state level. There is a clear role for industry associations to play in helping to generate this material and a number of initiatives are under way in this field. Efforts by the United Nations 1540 Committee to engage with industry on issues related to dual-use export controls and non-proliferation through the so-called Wiesbaden process, which was initiated in 2012 with support from the German Government, have resulted in ambitions to develop compliance-related guidance.[211] One outcome of the Wiesbaden process is the creation of the Botticelli project, an industry-led network launched in Belgium in October 2015 that aims to produce 'guidelines to help companies implement internal compliance programs'.[212] However, to date no guidance documents have been produced.

The EU also has a clear role to play in generating useful guidance material, particularly as it moves ahead with its review of the Dual-use Regulation. During the consultation process a number of key areas were identified for attention and highlighted in the draft recast published by the European Commission in September 2016. The EU has recognized the lack of guidance documents to help companies understand how they should implement controls on exports of dual-use goods. The Impact Assessment notes: 'the EU has so far not issued any guidance on the control of emerging technologies, while for example, some competitors like the US and Japan have clarified their approach, for the benefit of their operators, to the control of technology transfers through the cloud'.[213] The draft recast also—for the first time—introduces a definition of an ICP into the Dual-use Regulation and would make having an ICP obligatory for any company wishing to use a global licence or the proposed EUGEA on intra-company transmission of software and technology.[214] However, there is scope for the review process to go considerably further, by laying out in more detail the key components of an effective ICP and tailoring these standards to the different sectors affected by the EU's Dual-use export controls.

As the EU moves forward with this process it will need to improve on—and learn lessons from—previous efforts to promote the adoption of ICPs—particularly under the ICT Directive and in connection with the AEO Programme—which have often been patchy and poorly coordinated and where the outcomes have been uneven. It would also be wise to try to build on the various guidelines highlighted in the course of this concept note as well as recent efforts by the US Government to develop improved ICP-related material. In particular, the US Government has recently launched a new website with both general, sector- and actor-specific guidelines and resources on what an ICP should contain.[215] These tools could be adapted and used by the EU and national governments to fit their specific needs.

[211] Kasprzyk, N., Shadung, M. and Stott, N., *Towards the 2016 Comprehensive Review: Former Experts Assess UNSC Resolution 1540*, Institute for Security Studies (ISS) monograph no. 191 (ISS Africa: Pretoria, Addis Ababa Dakar and Nairobi, 2015); 'First Industry Conference on Security Council Resolution 1540', UNODA website, 25 April 2012 <https://www.un.org/disarmament/update/20120425/>; 'Wiesbaden III: Governance and compliance management conference on Resolution 1540 (2004)', Information note, <http://www.un.org/en/sc/1540/documents/Information%20Note%20Germany%201540%20Industry%20WS%202014-74.pdf>.

[212] Zero, S., 'Towards smarter nuclear export controls', World Nuclear News, 6 Oct. 2015, <http://www.world-nuclear-news.org/V-Towards-smarter-nuclear-export-controls-0610151.html>.

[213] European Commission (note 18), p. 6.

[214] The draft recast states that "'internal compliance programme" shall mean effective, appropriate and proportionate means and procedures, including the development, implementation, and adherence to standardised operational compliance policies, procedures, standards of conduct, and safeguards, developed by exporters to ensure compliance with the provisions and with the terms and conditions of authorisations set out in this Regulation'.

[215] See 'Internal Compliance Programme' Guide, <http://icp.rit.albany.edu/>.

When drafting any guidance documents, regular exchanges with industry will be essential. Here, it will be important that SMEs, not just multinational corporations, are represented in this feedback loop and that a broad range of sectors' and stakeholders' perspectives and particularities are taken into account. It will also be important to widen the range of industry actors that are consulted. The industry associations responsible for certain sectors, such as biotechnology and the transport sector, have to date had only limited discussions about dual-use and arms export controls at the EU level. Finally, it will be essential to build on work already carried out. For example, the Joint Working Group on AEO-ICP Convergence mandated by the Dual-Use Coordination Group and the AEO Network has already gathered industry input into the process, which should be carried forward. The remainder of these conclusions highlights the particular areas on which the EU should focus its attention when drafting targeted compliance-related guidance.

Areas where sector-, actor- and issue-specific standards could be developed

ICT Sector

In relation to the ICT sector, a key gap that the EU needs to fill is to create greater clarity about the intended scope of the controls on intrusion software and to make clear that work in the field of IT security is not covered by controls. At the same time, there is also a need to bring together technologists, legal experts and policymakers to draft a detailed set of good practice guidelines for the companies that are the intended target of the expanded controls on cyber-surveillance technologies. As it stands, there is a significant lack of clarity about the intended focus of the controls and the issues that should be taken into account when deciding whether a particular export is suitable. These guidelines would need to be based on existing legal standards and recommendations relating to the capabilities that cyber-surveillance technologies should have, as well as those detailing when and how cyber-surveillance technologies should be used by national authorities, and how their use should be governed.

Academia and research

The ability of academia and research institutes to comply with dual-use and arms export controls would also be enhanced by greater clarity at the EU level with regard to the coverage of controls. The EU Dual-use Regulation exempts basic or fundamental research from control requirements. However, the term 'basic scientific research' has been interpreted differently in individual EU member states, something that became a central issue in disputes regarding the publication of research on Influenza A.[216] As described above, some guidelines have been drawn up to make applicants and evaluators more aware of their obligations under dual-use export controls, but these efforts could be conducted more broadly and systematically, and in areas of research that have not previously been the focus of attention.[217] There is also a need to raise awareness of issues related to dual-use and arms export controls within academia, and to create forums where representatives of academia and research can meet to discuss

[216] SIPRI and Ecorys (note 11), p. 38; and Enserink, M., 'Dutch appeals court dodges decision on hotly debated H5N1 papers', *Science*, 16 July 2015, <http://www.sciencemag.org/ news/2015/07/ dutch-appeals-court-dodges-decision-hotly-debated- h5n1-papers>.

[217] European Commission, 'Explanatory note on the control of 'export' for 'dual-use goods', 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 goods', <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>.

shared challenges and examples of good practices. Representatives from research and academia noted in particular that there are very few opportunities to discuss experience and good practices in the field of export control compliance at the EU level.[218] As they noted, the challenges they encountered were 'generic across higher education' but also varied depending on the 'university's research profile and activity'.[219]

Transport service providers

The application of dual-use and arms export controls to transport or distribution service providers is also an area that could benefit from greater clarity and actor-specific guidance at the EU level. As it stands, there are no agreed definitions of some of the key terms that apply in this area. For example, the EU Dual-use Regulation and the Union Customs Code have different definitions of the term 'transit'.[220] The draft recast of the EU Dual-use Regulation seeks to bring greater clarity to the definition of transit.[221] However, as noted the recast also implies certain expansions to the scope of transit controls that would widen the range of potentially affected companies. According to the European Commission, changes in this area would be beneficial 'in terms of legal clarity, uniform application throughout the EU and enhanced security—while additional costs for the involved authorities can also be expected to remain very low due to the small number of transit operations concerned'.[222]

Product classification

Providing tools that companies can use to assist them with product classification or that EU member states can use to better respond to industry enquiries is also an area where the EU should focus its attention. The 2014 Commission Communication mentions the possibility of creating an 'EU technological reaction capacity' that could help to draft future control list language and produce guidance on how particular control list entries should be interpreted. If such a capacity were to be established it would need to have access to expertise across the full spectrum of technologies covered by dual-use export controls, and to harness inputs from both industry and academia. The proposed recast does not make specific recommendations on this issue but does note that: 'The Commission and the Council shall, where appropriate, make available guidance and/or recommendations for best practices for the subjects referred to in this Regulation to ensure the efficiency of the Union export control regime and the consistency of its implementation'.[223]

[218] Contract Manager (note 145).

[219] Director of research service (note 146).

[220] The Union Customs Code entered into force in 2013, replacing the 2008 Community Customs Code. Regulation (EU) no. 952/2013 of the European Parliament and of the Council of 9 Oct. 2013 laying down the Union Customs Code, *Official Journal of the European Union*, L69, 10 Oct. 2013, p. 1. Its substantive provisions are applicable from 1 May 2016, once the corresponding Commission acts are in force, see European Commission, 'The Union Customs Code: a recast of the Modernised Customs Code', <http://ec.europa.eu/taxation_customs/ customs/customs_code/unioncustoms_code/index_en.htm>.

[221] The proposed recast specifies that transit controls cover items: '(a) which are placed under the external transit procedure and only pass through the customs territory of the Union; (b) which are trans-shipped within, or directly re-exported from, a free zone; (c) which are in temporary storage and are directly re-exported from a temporary storage facility; (d) which were brought into the customs territory of the Union on the same vessel or aircraft that will take them out of that territory without unloading'. The proposal also specifies that transit controls can apply to: '(a) the declarant within the meaning of Article 5(15) of the Union Customs Code; (b) the carrier within the meaning of Article 5(40) of the Union Customs Code; (c) the natural person carrying the goods to be exported where these goods are contained in the person's personal baggage within the meaning of Article 1(19)(b) of Regulation (EU) 2015/2446'. European Commission (note 9), pp. 21, 26.

[222] European Commission (note 18), pp. 33–34.

[223] European Commission (note 9), p. 41.

Intangible technology transfer controls

Companies from a number of sectors frequently underlined the need for legal clarification of the coverage of ITT controls and practical guidelines to help with compliance. The ability of companies and institutes to comply with ITT controls would potentially be enhanced by greater clarity at the EU level about their exact coverage. The draft recast of the EU Dual-use Regulation attempts to bring greater clarity to the application of ITT controls by specifying that controls would only apply when the technology is made available to 'legal and natural persons and partnerships' outside the EU, rather than a destination as is currently the case.[224] The draft recast also proposes a new EU General Export Authorization for 'Intra-company transmission of software and technology'.[225] The intention of the new language is—in part—to 'facilitate the use of cloud services'.[226] However, Digital Europe has argued that the language needs to be further clarified, particularly by deleting the reference to 'making available' software and technology in electronic form.[227] The concern appears to be that even under the proposed language, a company supplying technologies that allow another company to provide cloud services would be held responsible for who downloads information from the cloud.

Risk assessments

As part of its draft recast of the EU Dual-use Regulation, the European Commission has proposed making 'available guidance and/or recommendations to ensure common risk assessments by the competent authorities of the Member States' for the implementation of licensing criteria.[228] This could take the form of a user's guide to the EU Dual-use Regulation, with detailed sector-, actor and issue-specific guidelines and risk assessment tools for exports of all types of dual-use goods and technologies. The development of such a document would be a useful outcome of the review process, particularly if it were to result in a public document that companies and institutes affected by the EU's Dual-use Regulation could draw on when making their own risk assessments.

[224] European Commission (note 9), p. 19.

[225] European Commission (note 9), p. 8.

[226] European Commission (note 9), p. 7.

[227] Digital Europe, *European Commission Proposed Recast of the European Export Control Regime: Making the Rules Fit for the Digital World* (Digital Europe: Brussels, Feb. 2017), <http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2358&language=en-US&PortalId=0&TabId=353>.

[228] European Commission (note 9), p. 33.

About the authors

Dr Sibylle Bauer (Germany) is Director of Studies, Armament and Disarmament and also Director of SIPRI's Dual-use and Arms Trade Control Programme. Since 2005 she has designed and implemented capacity-building activities in Europe and South East Asia, with a focus on legal and enforcement issues related to the enhancement of transit, brokering and export controls. Before joining SIPRI in 2003, she was a Researcher with the Institute for European Studies (ULB) in Brussels. Her recent publications include 'The dual-use export control policy review: balancing security, trade and academic freedom in a changing world', Non-proliferation Paper no. 48 (Mar. 2016, co-author) and 'Export controls', *Routledge Handbook of Nuclear Proliferation and Policy* (Routledge, 2015).

Kolja Brockmann (Germany) is a Research Assistant in the Dual-use and Arms Trade Control Programme, following an EU Non-proliferation Consortium internship at SIPRI. He finished his Master's degree in Non-Proliferation and International Security at the War Studies Department of King's College London in 2016. Previous to joining SIPRI, he was an intern with the German Federal Office for Economic Affairs and Export Control (BAFA) in Frankfurt, where he worked on licensing of dual-use goods and contributed to a number of EU outreach and assistance projects on arms export controls and Arms Trade Treaty (ATT) implementation.

Mark Bromley (United Kingdom) is the Co-Director of SIPRI's Dual-use and Arms Trade Control Programme, where his work focuses on national, regional and international efforts to regulate the international arms trade. Previously, he was a policy analyst for the British American Security Information Council (BASIC). His recent publications include 'ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns', Strategic Trade Review (Spring 2016, co-author), 'The dual-use export control policy review: balancing security, trade and academic freedom in a changing world', Non-proliferation Paper no. 48 (Mar. 2016, co-author) and 'ATT-related outreach assistance in sub-Saharan Africa: identifying gaps and improving coordination', SIPRI Background Paper (Feb. 2016, co-author).

Giovanna Maletta (Italy) is a Research Assistant in the Dual-use and Arms Trade Control Programme, following an EU Non-proliferation Consortium internship at SIPRI. Previously she was a Blue Book Trainee at the Disarmament, Non-proliferation and Arms Export Control Division of the European External Action Service (EEAS) in Brussels, an Intern in the International Cooperation Branch of the Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague and the Office of the Ambassador of Pakistan in Rome.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org