sipri

THE CHALLENGE OF SOFTWARE AND TECHNOLOGY TRANSFERS TO NON-PROLIFERATION EFFORTS

Implementing and Complying with Export Controls

MARK BROMLEY AND GIOVANNA MALETTA

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The Governing Board is not responsible for the views expressed in the publications of the Institute.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Signalistgatan 9
SE-169 70 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

THE CHALLENGE OF SOFTWARE AND TECHNOLOGY TRANSFERS TO NON-PROLIFERATION EFFORTS

Implementing and Complying with Export Controls

MARK BROMLEY AND GIOVANNA MALETTA

April 2018

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

Contents

Acknowledgements

The information contained in this SIPRI Research Paper builds on past research by the authors on dual-use and arms trade controls, and on information collected through interviews and communications with representatives of national licensing authorities and export control officers from companies, universities and research institutes. The respondents and interviewees were asked to outline how controls on tangible and intangible transfers of software and technology are implemented at the national level and how they are applied in their internal compliance programmes (ICPs).

In putting together this research paper the authors' work was greatly assisted and informed by a background technical briefing paper produced by Joachim Wahren. A draft version of the paper was discussed at a two-day workshop in Stockholm hosted by SIPRI in February 2018. The paper was further revised on the basis of the feedback provided by participants from companies, licensing and enforcement authorities, and technical experts.

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 paper to be produced. They would also like to thank all those who agreed to share their expertise and particularly those who attended the SIPRI workshop in February 2018. The authors would also like to thank SIPRI colleagues Sibylle Bauer and Kolja Brockmann and the two external reviewers for their detailed comments on the paper. The authors are also grateful to the SIPRI Editorial Department for its work. All errors are entirely the responsibility of the authors.

Abbreviations

AG	Australia Group
AM	Additive manufacturing
ANSSI	Agence Nationale de la Sécurité des Systèmes d' Information (National Agency for Information Systems Security)
ATAS	Academic Technology Approval Scheme
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle (Federal Office for Economic Affairs and Export Control)
CBW	Chemical and Biological Weapons
CCL	Commerce Control List
COCOM	Coordinating Committee on Multilateral Export Controls
DPRK	Democratic People's Republic of Korea
EU	European Union
EUGEA	EU General Export Authorization
ICP	Internal compliance programme
ICT	Information and Communications Technology
ITAR	International Traffic in Arms Regulations
ITT	Intangible transfers of technology
JCPOA	Joint Comprehensive Plan of Action
LEA	Law Enforcement Agencies
MTCR	Missile Technology Control Regime
NASA	National Aeronautics and Space Agency
NGEA	National General Export Authorization
OGEL	Open General Export Licence
NSG	Nuclear Suppliers Group
OSCE	Organization for Security and Co-operation in Europe
R&D	Research and development
TRL	Technology Readiness Level
URENCO	Uranium Enrichment Centrifuge Corporation
WMD	Weapons of mass destruction
XAE	Xian Aero-Engine (Co.)
3D printing	Three-dimensional printing

Executive summary

Dual-use and arms export controls cover different types of software and technology—defined as including both 'technical data' and 'knowledge and technical assistance'—that is 'specially designed' or 'necessary' for the 'development, production or use' of controlled items. Controls on software and technology are generally considered an essential aspect of dual-use and arms export controls. However, unlike other controlled items, many types of software and technology can take a non-physical—intangible—form or be transferred through non-physical or intangible means. Transfers of software and technology through intangible means can occur through the electronic transfer of data or the oral transmission of information, and are referred to as intangible transfers of technology (ITT). This SIPRI Research Paper examines: (*a*) the different ways in which tangible and intangible transfers of software and technology can occur; (*b*) the proliferation-related challenges they can generate; (*c*) the way relevant dual-use and arms export controls are structured in the multilateral export control regimes and implemented by EU member states; and (*d*) the particular challenges that implementation and compliance present for the governments of EU member states and EU-based companies and research institutes.

Section 2 describes the main mechanisms through which transfers of software and technology occur, looking first at software and technical data, and then at knowledge and technical assistance. Transfers of software and technology can occur through the commercial sale of controlled software or technology or of items that contain them. However, they can also be transferred as a result of their inclusion in academic journals and training manuals or the foreign acquisition of companies. The means through which software and technology can be stored and shared have changed significantly in recent years, creating a range of challenges for the effective and consistent application of dual-use and arms export controls. For example, rapid developments in the field of cloud computing are raising difficult questions about whether, how and when controls on transfers of software and technical data should be applied. In addition, the fact that people travel internationally with far greater ease than in the past has increased the range of channels through which in-person transfers of knowledge and technical assistance can occur.

Section 3 examines some of the main proliferation concerns connected with transfers of software and technology. The section focuses on nuclear weapons, biological weapons and conventional arms, and analyses the way in which transfers of technology have played a role in past cases of proliferation. The available evidence indicates that while transfers of software and technical data have played an important role in cases of proliferation, their impact is often limited if they are not accompanied by the transfer of knowledge and technical assistance. However, the impact of both is often constrained further if they are not accompanied by transfers of controlled physical goods. The case studies presented also underline the difficulty of assessing the impact that transfers of technology have had in these cases, not least due to the complex relationship between technical data and technical assistance, the type of weapon systems considered and the historical and geographical contexts.

Section 4 outlines how controls on transfers of software and technology are included in the different export control instruments that are relevant to EU member state governments and EU-based companies and research institutes. UN and EU embargoes, the various export control regimes and EU dual-use and arms export controls all apply to transfers of certain types of software technology. They are also covered by US re-export controls, with which EU-based companies and research institutes are obliged to comply. Although, these controls are structured in broadly similar ways,

key differences exist, particularly between the multilateral regimes and EU controls, and between these and US re-export controls. Controls on transfers of software and technology continue to be a major focus of discussion, particularly in connection with the ongoing review of the EU Dual-use Regulation. Several aspects of the European Commission's proposed 'recast' of the Regulation are focused on facilitating certain transfers of software and technology—such as between different branches of the same company—and creating a better harmonized approach to the application of controls to cloud computing.

Section 5 provides an overview of national practices on the implementation of controls on transfers of software and technology by EU member states. Although the Dual-use Regulation forms part of the EU's 'common commercial policy', member states have substantial leeway in terms of how controls are implemented at the national level and even more so when it comes to implementing controls on exports of military equipment. Key areas of difference include whether a particular software or technology is judged to be subject to control; which transfers are subject to control, as shown in discussions on how export controls should apply to cloud computing; the ways in which controls are applied, either through individual or open licences; and the application of controls to 'deemed' exports and the publication of scientific research. The section also examines some of the key challenges associated with both implementing and complying with controls on transfers of software and technology—particularly ITT. For national authorities, these include interpreting control list language, and detecting and preventing unauthorized transfers. For companies and research institutes, the challenges include complying with the different requirements in EU controls and US export controls, and keeping track of transfers of controlled items and the nationality of employees.

Section 6 presents conclusions and recommendations, focused on the steps that could be taken by the export control regimes, the EU, EU member states, and companies and research institutes to both streamline controls on transfers of software and technology and improve their effectiveness. These suggestions are intended to address some of the challenges and gaps identified by the paper. In particular, the recommendations explore how some of the difficulties associated with interpreting relevant definitions could be addressed through the development and promotion of targeted guidance material. Steps that could be taken to develop a better harmonized approach on certain issues, such as the application of export controls to cloud computing, are discussed along with the challenges of creating truly harmonized approaches in this area. Finally, the conclusions look at the need and potential to complement the application of export controls to software and technology with other governance tools, such as visa screening programmes, the regulation of foreign acquisitions and systems of self-regulation, particularly in the research field and academia.

1. Introduction

International, multilateral and regional instruments require all EU member states to regulate the export, brokering and transit/transshipment of military equipment and dual-use items. These regulations, referred to here as 'dual-use and arms export controls', cover a wide range of physical goods, including conventional arms, weapon of mass destruction (WMD) delivery systems, and conventional arms and WMD-related parts and components. In addition, they cover different types of software and technology—defined as including both 'technical data' and 'knowledge and technical assistance'—that is 'specially designed' or 'required' for the 'development, production or use' of controlled items. Controls on transfers of software and technology are generally considered to be an essential aspect of dual-use and arms export controls. Many of the items that are subject to control—particularly more complex and technically advanced conventional weapons—are less effective if the recipient does not have access to relevant software or technical data to enable or enhance their use. Knowledge and technical assistance can also be crucial to the successful production of certain types of WMD. Furthermore, certain types of software, including those that contain a certain level of encryption and so-called intrusion software, are viewed by states as posing a potential threat to national security. As a result, UN and EU embargoes, the various export control regimes—the Australia Group (AG), the Missile Technology Control Regime (MTCR), the Nuclear Suppliers Group (NSG) and the Wassenaar Arrangement—and EU dual-use and arms export controls all apply to transfers of certain types of software and/or technology.

Transfers of software and technology can occur through numerous channels. These include the commercial sale of controlled software or technology or of products that contain these items. However, controlled software and technology can also be transferred as a result of their inclusion in academic journals, training manuals and university courses, or of the foreign acquisition of companies. Moreover, the means through which different types of software and technology can be stored and shared have changed significantly in recent years, creating a range of challenges for non-proliferation efforts and the effective and consistent application of dual-use and arms export controls. For example, rapid developments in the field of cloud computing are raising difficult questions about whether, how and when controls on transfers of software and technical data should be applied. In addition, the fact that people travel internationally with far greater ease than in the past has increased the range of channels through which in-person transfers of knowledge and technical assistance can occur. Finally, rapid developments in production methods mean that transfers of certain types of software and technology have the potential to be an enabler of proliferation to a greater extent than previously. In particular, additive manufacturing (AM)—also referred to as '3D printing'—has the potential to increase the range and complexity of controlled items that can be produced using software and technical data. [1]

Controls on transfers of software and technology have been the focus of some of the main tensions and controversies concerning the application of dual-use and arms export controls. In the 1970s and 1980s, the application of export controls to software that employed a certain level of encryption led to the so-called crypto-wars in the United States. Computer programmers and others in the information and communications technology (ICT) sector argued that the controls posed a threat to IT security, harmed commercial competitiveness and represented a violation of free speech,

[1] See Brockmann, K. and Kelley, R., *The Challenge of Emerging Technologies to Non-Proliferation Efforts: Controlling Additive Manufacturing and Intangible Transfers of Technology*, SIPRI Research Paper (SIPRI: Stockholm, Apr. 2018).

and pushed for them to be relaxed or abolished.[2] More recently, a key focus of debate in the EU has been on whether a publication that contains detailed explanations on how to produce particular dual-use items should be subject to controls on transfers of technology. The resulting discussion has raised questions about whether export controls pose a threat to academic freedom and could undermine attempts to ensure responsible practices in sensitive areas of academic research. Finally, since the Wassenaar Arrangement introduced controls on 'intrusion software' in 2013 there has been a long-running debate about their potential to generate unintended side-effects for researchers and companies working in IT security. The strength of the response of the ICT sector in the USA led the US Government to delay national implementation of the controls and to press for revisions to the language previously agreed at the Wassenaar Arrangement.

In 2017, controls on transfers of software and technology continued to be a major focus of discussion, particularly within the export control regimes and in connection with the ongoing review of the EU Dual-use Regulation. Within the various export control regimes, states have been discussing whether, and if so how, controls on additive manufacturing and the software, technology and materials they use should be expanded. Meanwhile, several aspects of the European Commission's proposed 'recast' of the EU Dual-use Regulation are focused on how to facilitate certain transfers of software and technology—such as between different branches of the same company—and seeking to establish a more harmonized approach to the issue of how dual-use export controls should apply to cloud computing. At the same time, the review has also provided an avenue for continued debates about how export controls should be applied to encryption and intrusion software. Finally, the review has drawn attention to the application of export controls within research institutes and academia, where controls on transfers of technology are particularly relevant.

Controls on transfers of software and technology are considered to be among the most challenging issues for national authorities seeking to implement dual-use and arms export controls, and companies and research institutes seeking to comply with them. One of the most frequently cited challenges is that—unlike other items that are subject to dual-use and arms export controls—many types of software technology can take a non-physical/intangible form or be transferred through non-physical/intangible means. Hence, while software and technical data are generally viewed as 'tangible' goods, knowledge and technical assistance are viewed as intangible, in that they relate to the type of expertise that people may carry in their heads. Transfers of software and technology through intangible means can occur through the electronic transfer of data or the oral transmission of information and are referred to as an intangible transfer of technology (ITT). Hence, the export of a computer or CD-ROM that contains controlled software would be viewed as a tangible transfer of tangible goods. However, sending controlled technical data by email from one country to another would be an intangible transfer of tangible goods and an example of an ITT. Finally, an individual travelling abroad to give or take part in a training workshop where controlled knowledge is discussed would be an intangible transfer of intangible goods and would also be an example of an ITT.

For national authorities, controls on ITT are frequently cited as particularly problematic.[3] However, many of the challenges that are often highlighted are relevant to software and technology—or dual-use and arms export controls—in general and are

[2] Grimmett, J. J., *Encryption Export Controls*, Congressional Research Service (CRS) Report for Congress RL30273 (US Congress, CRS: Washington, DC, 11 Jan. 2001).

[3] Wassenaar Arrangement, 'Best Practices for Implementing Intangible Transfer of Technology Controls (Agreed at the 2006 Plenary)'.

not specific to ITT. For example, determining whether a particular manual or guidance document contains information that is necessary for the 'development, production or use' of controlled items can be a difficult process but is not specific to ITT. That said, ITT can occur in ways that do not leave a clear physical footprint, which does present a particular set of difficulties. In particular, it makes it more difficult to prevent unauthorized transfers from taking place and to generate the evidence needed to demonstrate that controls have been violated. As a result, the effective implementation and enforcement of controls on transfers of software and technology—and particularly ITT—are reliant on a high level of awareness and self-regulation among the companies and research sectors affected. At the same time, controls on transfers of certain types of technology can also benefit from their integration into other areas of government regulation, such as systems for vetting which students can take part in academic courses where proliferation-relevant knowledge is taught and determining whether a company can be the subject of foreign acquisitions.

For companies and research institutes seeking to comply with dual-use and arms export controls, determining whether a particular piece of software or technology is subject to control is also a challenge. This is particularly true for those working in rapidly evolving fields or that have limited resources or a lack of prior experience with export controls. In addition, companies and research institutes often have to contend with differences in the way key aspects of controls are applied in EU member states and the contrasting requirements of EU regulations and US re-export controls. Again, controls on ITT are frequently highlighted as being particularly problematic. Complying with controls on ITT can involve keeping records on every instance in which controlled software or technology is included in an email or downloaded from—or uploaded to—a computer server. It can also mean checking which controlled technology is included in a presentation and the nationalities of the people in the audience. Effective compliance, therefore, is particularly reliant on investing time and money in ensuring that relevant personnel understand their export control-related obligations.

This SIPRI Research Paper focuses on the different ways in which transfers of software and technology occur, the proliferation-related challenges they can generate, the way relevant dual-use and arms export controls are structured in the regimes and implemented by EU member states, and the particular challenges that implementation and compliance present for governments, companies and research institutes. Of the issues raised, some relate only to ITT, while others relate to transfers of software and technology more generally, or dual-use and arms export controls as a whole. This is the first of two papers that SIPRI is producing on the issue of controls on transfers of technology. The second examines the particular issues around AM, the state of the art in AM technology, its ability to produce certain conventional arms and dual-use items, the application of export controls to AM, their implementation at the national level, and the challenges that implementation and compliance present for governments, companies and research institutes.[4]

Section 2 of this paper describes the main mechanisms through which transfers of software and technology occur, looking first at transfers of software and technical data and then at transfers of knowledge and technical assistance. The section also looks at recent trends and innovations in this area, particularly in relation to cloud computing. Section 3 examines some of the main proliferation concerns connected with transfers of software and technology. The section focuses on nuclear weapons, biological weapons and conventional arms, and analyses the way in which transfers of technology have played a role in past cases of proliferation. Section 4 outlines how controls on transfers of software and technology are included in the different export

[4] See Brockmann and Kelley (note 1).

control regimes. The section also looks at recent discussions on how to modernize controls on transfers of software and technology, particularly in connection with the recast of the EU Dual-use Regulation. Section 5 provides an overview of national practices on the implementation of controls on transfers of software and technology by EU member states. The section also examines some of the key challenges associated with both implementing and complying with controls. Section 6 presents conclusions and recommendations, focused on the steps that could be taken by the export control regimes, the EU, EU member states, and companies and research institutes to both streamline controls on transfers of software and technology, and improve their effectiveness.

2. Means of transferring software and technology

Within the various export control regimes, 'software' is defined as 'a collection of one or more "programs", or "microprograms", fixed in any tangible medium of expression'.[5] Meanwhile, technology is defined as including both 'technical data', such as 'blueprints, plans and diagrams and models', and 'knowledge and technical assistance', such as 'instruction, skills, training, working knowledge, consulting services'.[6] This section discusses the means through which transfers can occur of first software and technical data, and then knowledge and technical assistance, distinguishing between tangible transfers on the one hand and ITT on the other. The section also summarizes the various means through which transfers of software and technology can occur in the course of research cooperation activities with both the private sector and academia (see box 2.1).

Software and technical data

Software and technical data are forms of what can be defined as 'explicit knowledge', that is 'knowledge that can be expressed in words, numbers and symbols, and stored in books or computers'.[7] As such, software and technical data are stored using tangible means through their inclusion in books, articles or manuals or by being saved on CD-ROMs, memory sticks, computers or servers. These storage mechanisms also allow software and technical data to be transferred through tangible means. This would be the case if a CD-ROM containing controlled software or a hard copy of a journal article were taken from one country to another. However, it is becoming increasingly common for software and technical data to be shared and transferred through intangible means, such as through email attachments, server downloads and uploads, and cloud computing services. The use of these systems to share software and technical data among different branches of the same company or with supply chain partners or customers has expanded significantly in recent years. In 2000, most companies—even those with a large global presence—found it hard to communicate electronically across borders, even with parts of their own business located overseas.[8] However, by 2003 export licensing authorities were finding that the volume of controlled software and technical data that was being transferred via intangible means was increasing significantly, driven by the globalization of businesses and organizations, and advances in telecommunications and the internet.[9]

One of the main changes to the way in which software and technical data are stored and shared has been the expansion of cloud computing. Cloud computing emerged in the early 2000s and can be broadly defined as 'using shared rather than private local computing resources to store software or technology and handle applications'.[10] These shared resources can be both geographically distant from the user and spread across a number of locations. At least one cloud service provider has announced plans to launch a network of satellites that will be used to store data in space.[11] Moreover, the precise location of the software or technology can shift rapidly between locations depending on use and need. Drawing a precise boundary between cloud computing and more

[5] See e.g. Missile Technology Control Regime, 'Equipment, software and technology annex', 19 Oct. 2017.

[6] See e.g. Wassenaar Arrangement, 'List of dual-use goods and technologies and munitions list', WA-LIST (16) 1 Corr. 1, 17 Feb. 2017.

[7] Cambridge Dictionary, 'Explicit knowledge'.

[8] Chilvers, S., *Electronic Transfers of Technology* (ESARDA: Ispra, Nov. 2014).

[9] Chilvers (note 8).

[10] Tauwhare, R., 'Cloud computing and export controls', Tech UK, 22 Feb. 2016.

[11] See Spacebelt, <http://spacebelt.com>, accessed 20 Mar. 2018.

Box 2.1 Transfers of technology through research cooperation activities

Transfers of technology can also occur through collaborations between research and academic institutes, and between research and academic institutes and the private sector. These activities can take place through 'trade interactions' or 'multilateral cooperation' and in each case the aspects that concern the transfer of controlled knowledge and technical assistance are not easy to distinguish.[a] In the framework of this type of cooperation, research and academic institutes, while they do not possess the means for the 'mass production of marketable products', may be tasked with developing new technologies in the shape of 'model products' or 'prototypes' for commercial purposes.[b] The variety of funding sources, and the increasingly globalized context in which research and academic institutes and their partners operate, also mean that these actors may engage in a range of international collaborations that might involve the exchange of controlled technology with partners located in different countries.[c] Multinational companies in particular contribute to this trend in that their research and development activities are conducted globally.[d] From a proliferation perspective, collaborative research in certain fields, such as aeronautics, nuclear technology and the life sciences, even when driven by peaceful aims, can to varying degrees involve sharing controlled technology.

[a] Rebolledo, V. G., 'Intangible transfers of technology and visa screening in the European Union', EU Non-Proliferation Paper no. 13 (SIPRI: Stockholm, 2012), pp. 5–6.
[b] 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 2017), p. 58.
[c] Starks, B. and Tucker, C., 'Export control compliance and American academia', *Strategic Trade Review*, vol. 3, no. 4 (spring 2017).
[d] Meier, O., 'Dual-use technology transfers and the legitimacy of non-proliferation regimes', ed. O. Meier, *Technology Transfers and Non-proliferation: Between Control and Cooperation* (Routledge: London, 2014), p. 10.

standard methods of storing and accessing data is difficult. One way of defining the distinction is by focusing on the 'essential characteristics' of cloud computing: 'on-demand self-service; broad network access; resource pooling; rapid elasticity; and measured service'.[12] Some of these characteristics are present in more traditional methods of data storage and access, but it is only with cloud computing that they are all present.

There are several different cloud computing models: 'public clouds', which are accessible to all users; 'private clouds', where access is restricted to authorized users; 'community clouds', which are used by a specific group of users with common requirements; and 'hybrid clouds', which involve a mix of public, community and private systems.[13] Some larger companies manage their own in-house cloud computing services but this is rare. It is more common for companies to use cloud computing service providers to meet their needs. Again, there are various different models of service provision, from providing the software that cloud computing uses, to providing the infrastructure it employs or the platform that allows users to access these services.[14] Major providers—such as Amazon Web Services, Google Apps and Microsoft—offer a complete set of these different types of services while other smaller companies tend to specialize in particular areas.[15] Using these externally managed services is widely seen as 'less expensive and more efficient' than using internal resources.[16] Market analysts project that the global market for providing these services will increase from $40.7 billion in 2011 to $240 billion in 2020.[17]

The basic tension between the model employed by cloud computing and the way export controls have traditionally functioned has been widely discussed. In 2012 one analysis noted that 'export-control laws and the cloud have opposing ideologies'.[18] Export controls are built around the notion that it is possible to maintain oversight

[12] Chilvers (note 8).
[13] Rolls-Royce, 'Export control and IT joint policy on the use of cloud IT systems', 2017, Unpublished.
[14] Chilvers (note 8).
[15] Braverman, B. and Wong, B., 'Cloud computing: US export controls reach for the sky', Davis Wright Tremaine LLP, 20 May 2013.
[16] Braverman and Wong (note 15).
[17] Braverman and Wong (note 15).
[18] Knight, G., 'Cloud computing and export laws: Are you exporting illegal data?', Info Boom, 2 Mar. 2012.

of situations in which controlled items cross international borders. Cloud computing—which is increasingly becoming the industry standard for the storage of large volumes of data—is built around the notion that data should be able to move freely between servers based in multiple locations depending on where the need is greatest and the cost is lowest.[19] The growing use of cloud computing services raises a number of questions concerning whether, and if so how, export controls should apply when cloud computing is used to store and share controlled software and technology. Among these are whether the act of uploading or downloading controlled software or technical data should be subject to export controls, whether the location of the server or the entity downloading the data is the main point of concern, and whether it is the user or the provider of the cloud computing services that should be subject to licensing requirements. These issues are explored in more depth in section 5.

Knowledge and technical assistance

Knowledge and technical assistance are forms of what can be defined as 'tacit knowledge', that is 'knowledge that you do not get from being taught, or from books' but 'from personal experience'.[20] As such, knowledge and technical assistance are forms of technology that are both stored and shared through intangible means. The term tacit knowledge was introduced by Michael Polanyi to 'describe the fact that "expert scientists know more than they can tell"' and, therefore, to define a type of knowledge that it is not easy to communicate or transfer to another person without years of 'apprenticeship'.[21] This definition can be applied to the type of 'know-how' and information that can possibly be transferred through 'education, training and doing'.[22] More generally, this concept refers to the kind of knowledge that can be transferred in-person. Transfers of knowledge and technical assistance can therefore involve the active movement of people across borders carrying with them specific and sensitive knowledge acquired through their practical experience. This means that efforts to exert control over transfers of knowledge and technical assistance are a cross-cutting issue, and control cannot simply be addressed by export controls, but may need to be complemented with other tools such as visa policies.

Transfers of knowledge and technical assistance can take place through the provision of skills training and consulting services or via academic courses, such as PhD programmes in certain disciplines (e.g. 'nuclear physics or microbiology').[23] These types of transfer can also occur in the context of activities aimed at the promotion of the peaceful application of dual-use technologies, such as capacity building, assistance in integrating international non-proliferation obligations into national systems and training to respond to an attack or an incident involving hazardous chemical, biological, radiological or nuclear materials.[24] Based on the analysis of Meier and Hunger, from a proliferation perspective, the 'risk of misuse' deriving from the transfer of dual-use technologies in the nuclear, biological and chemical fields is highest in the context of cooperation on fuel-cycle nuclear technologies, on biodefence and/

[19] Knight (note 18).

[20] Cambridge Dictionary, 'Tacit knowledge'.

[21] Gorman, M. E., 'Types of knowledge and their role in technology transfer', *Journal of Technology Transfer*, vol. 27, no. 3 (2002), pp. 219–231, 220.

[22] Stewart, I., 'The contribution of intangible technology controls in controlling the spread of strategic technologies', *Strategic Trade Review*, vol.1, no. 1 (Autumn 2015), p. 45.

[23] Rebolledo, V. G., 'Intangible transfers of technology and visa screening in the European Union', EU Non-Proliferation Paper no. 13 (SIPRI: Stockholm, 2012), p. 5.

[24] Hunger, I. and Meier, O., 'Between control and cooperation: Dual-use technology transfers and the non-proliferation of weapons of mass destruction', *Friedensforschung DSF*, no. 37, Deutschen Stiftung Friedensforschung (DSF), 2014, p. 11.

or biosecurity and on military defence against chemical attacks.[25] All these activities may also involve the physical movement of people across borders to provide training, knowledge or technical assistance, or in seeking to acquire these by moving to other countries. For instance, knowledge and technical assistance can be provided in a third country through 'on-site consultation', the engagement of skilled individuals in 'sensitive technology' projects and 'training, scientific cooperation and seminars on sensitive disciplines in the recipient country (where the end-user is based)'.[26]

Although it is a type of technology that is—by definition—not easy to transfer, the role of knowledge and technical assistance in facilitating proliferation is potentially significant. As mentioned above, knowledge and technical assistance could be spread through the distribution and deployment of 'skilled staff' around the world.[27] In addition, technological advances create the potential for knowledge and technical assistance to be transferred between people who are not physically in the same room using internet services such as Skype.[28] That said, it is unclear whether there have been any cases where transfers of controlled knowledge or technical assistance have occurred through these remote means. In addition, knowledge and technical assistance remains a 'key capability' that is not always available and cannot be easily acquired, especially in areas relevant to the weaponization of WMD materials.[29]

[25] Hunger and Meier (note 24), p. 11.

[26] Stewart (note 22), p. 52; and Rebolledo (note 23), pp. 8–9.

[27] Charatsis, C., 'Dual-use research and trade controls: Opportunities and controversies', *Strategic Trade Review*, vol.3, no. 4 (spring 2017), p. 49.

[28] Stewart (note 22), p. 18.

[29] Charatsis (note 27), p. 48.

3. Key proliferation challenges and transfers of software and technology

The potential for controls on transfers of software and technology to play a role in constraining proliferation varies significantly depending on the type of weapon system being considered. Studies of the spread of production capacity in a range of fields—from steel manufacturing to textile industry techniques and laser technology—emphasize that the acquisition of tacit knowledge—rather than explicit knowledge—has proved to be a more fundamental determinant of success or failure.[30] Similarly, the available evidence from the fields of nuclear weapons, biological weapons and conventional weapons indicates that while transfers of software and technical data have played an important role in cases of proliferation, their impact is often limited if they are not accompanied by the transfer of knowledge and technical assistance. However, the impact of both is often constrained further if they are not accompanied by transfers of controlled physical goods. At the same time, the relationship between explicit knowledge and tacit knowledge is subtle and complex, and can vary depending on the weapon system, the destination country and the time period in question.

Nuclear weapons and enrichment capabilities

There is evidence that the availability of tacit knowledge plays an important role in the success of states' nuclear weapon programmes and that its absence can act as a barrier or inhibitor.[31] One example, described in detail by MacKenzie and Spinardi, is the history of the Soviet Union's nuclear weapon programme.[32] The Soviet Union was able to acquire sensitive explicit knowledge from the USA through its sophisticated network of spies as well as cooperation with sympathizers working within the Manhattan Project at Los Alamos, such as Klaus Fuchs.[33] However, it took Soviet scientists four years from the time Fuchs passed them a detailed description of the first US bomb before they were able to successfully detonate their own.[34] This process, although only slightly longer than the original Manhattan Project, took a relatively long time considering that the scientists at Los Alamos had to invent that technology and code their experience in explicit knowledge. Simply relying on the documents supplied by Fuchs meant that Soviet scientists did not have access to the kind of experience and judgement, that is the tacit knowledge, that the US-based scientists had developed through repeated tests. In other words, to simply emulate their work was not enough: the Soviet scientists had to 'reinvent the processes and practices' already developed in the USA.[35] The same obstacles applied in the case of the French and Chinese nuclear weapon programmes.

According to Michael Aaron Dennis, another case in which the role of tacit knowledge becomes clear is that of Pakistan's nuclear weapon programme.[36] The country's nuclear enrichment capacities benefited from the knowledge that Abdul Qadeer Khan, well-known as the 'father' of Pakistan's nuclear bomb, drew from his work as a metal-

[30] Gorman (note 21), pp. 219–20.

[31] Gorman (note 21), pp. 219–31; Dennis, M. A., 'Tacit knowledge as a factor in the proliferation of WMD: The example of nuclear weapons', *Studies in Intelligence*, vol. 57, no. 3 (Sep. 2013); and MacKenzie, D. and Spinardi, G., 'Tacit knowledge, weapons design, and the uninvention of nuclear weapons', *American Journal of Sociology*, vol. 101, no. 1 (July 1995).

[32] MacKenzie and Spinardi (note 31).

[33] MacKenzie and Spinardi (note 31), p. 68.

[34] MacKenzie and Spinardi (note 31), pp. 68–70.

[35] Dennis (note 31), p. 6.

[36] Dennis (note 31).

lurgist at the European Uranium Enrichment Centrifuge Corporation (URENCO) in the Netherlands. More specifically, by combining the blueprints of URENCO's G-1 and G-2 centrifuges, illicitly acquired from the company before returning to his country, with his experience and his contacts with clandestine suppliers, Khan successfully managed to start Pakistan's centrifuge programme.[37] Pakistan's nuclear ambitions also benefited from China's assistance. China supplied the country, inter alia, with additional enriched uranium and weapon designs.[38] Nonetheless, Dennis argues that the Chinese support had a negligible impact on the pace at which Pakistan eventually developed its own bomb, as it 'still had to learn how to build one, and that required a reinvention of the tacit knowledge that went into the Chinese device they apparently copied'.[39] A similar view is reflected in the words of a US official quoted by Albright and Hibbs who, commenting on the Chinese supply of weapon designs to Pakistan, noted that 'cookbook design doesn't mean that you can make a cake on the first try'.[40] In Dennis' view, lack of tacit knowledge may also have acted as a barrier for some of the countries that benefited from the network of illicit nuclear trafficking that Khan was behind.[41]

These examples suggest that in the context of proliferation and export controls a lack of tacit knowledge may not be a 'show stopper' but it can be a 'show slower'. If countries possess 'the resources, the time, and a civilian nuclear power program' and are determined enough to acquire and/or develop nuclear weapons, even the tacit knowledge barrier will not stop them in the long run.[42] In addition, some of the obstacles faced by the 'first generation' of nuclear programmes have been overcome over the years by the wider availability of explicit knowledge, the partial transformation of relevant tacit knowledge into explicit knowledge and, not least, by the introduction and wide availability of many 'black box' technologies relevant to weapon design and production, such as digital computers able to perform calculations and assessments once carried out manually by people.[43]

Biological weapons

Concerns over the transfer of knowledge and technical assistance with the proliferation of WMD-related technology have also been raised with reference to biological weapons. Relatively rapid and remarkable achievements in the life sciences, together with the salience that bioterrorism acquired after the events of 11 September 2001, have contributed to the development of a narrative that these disciplines are becoming more 'predictable' in their progress and more accessible around the globe.[44] Synthetic genomics could be seen as a suitable example. Synthesizing genes, if not entire genomes, is becoming relatively easy due to the advent of 'automated, high-throughput DNA synthesizers' able to physically reproduce '[a] pathogenic gene or an infectious virus'

[37] Kile, S. N., 'The Khan nuclear network' in 'Nuclear arms control and non-proliferation', *SIPRI Yearbook 2005: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2005), pp. 552–55.

[38] Jeffrey Smith, R. and Warrick, J., 'Pakistani nuclear scientist's accounts tell of Chinese proliferation', *Washington Post*, 13 Nov. 2009.

[39] Dennis (note 31), p. 6.

[40] Albright, D. and Hibbs, M., 'Pakistan bomb: out of the closet', *Bulletin of the Atomic Scientists*, vol. 48, no. 6 (July/Aug. 1992), pp. 42–43.

[41] For an overview of the Khan network see Kile (note 37); and Powell, B. and Mcgirk, T., 'The man who sold the bomb', *Time Magazine,* 6 Feb. 2005.

[42] Dennis (note 31), p. 8.

[43] MacKenzie and Spinardi (note 31), p. 78.

[44] Revill, J. and Jefferson, C., 'Tacit knowledge and the biological weapons regime', *Science and Public Policy*, vol. 41, no. 1 (Oct. 2014), pp. 597–610.

from a DNA sequence stored in a computer.[45] The productivity of these instruments seems to be growing at a pace that is inversely proportional to their cost.[46]

On the other hand, the availability of these technologies is of limited use without the right set of skills and the tacit knowledge required to carry out the next step—their 'weaponization'. Some have claimed that the training necessary to make use of these new biotechnologies is not extremely sophisticated and that 'basic manipulations rely on widely available chemicals'.[47] However, others argue that this narrative overlooks the crucial role that tacit knowledge would have to play in 'bioweaponeering', as going beyond efforts to 'simply' spread a disease, to obtain, handle, culture, scale and weaponize an agent, would require deeper knowledge of the materials and processes involved.[48]

This was the case, for example, with Dr Rihab Rashida Taha, popularly known as 'Dr Germ', the Iraqi scientist who led the development of Iraq's biological weapons programme at the Salman Pak facility between the end of the 1980s and the beginning of the 1990s. Taha is likely to have acquired the necessary knowledge to contribute to this programme during the PhD courses she attended at the University of East Anglia in Norwich, England, in 1979, just before the start of the 1980–88 Iran–Iraq War.[49] Here, working under the supervision of Dr John Turner, the head of the university's biology department, she focused on plant pathogens, diseases that attack crops such as wheat and tobacco, but also gained exposure to basic studies on various animal diseases.[50] It is not clear whether Taha was specifically sent abroad by the Iraqi regime in order to acquire this strategic knowledge or her expertise just happened to fit the country's WMD programme. The father of Iraq's nuclear weapons programme, Jafar Jafar, however, followed a similar early career path.[51]

Conventional weapons

Transfers of military and dual-use technology can also play an important role in fostering the development of states' military and defence capabilities. In the case of arms transfers, for example, it is not only goods in the form of finished weapon systems that can be transferred, but, more often, foreign technology to be integrated into equipment assembled by licensed companies in the importer country. This could mean that transfers of technology in the context of arms deals might contribute to the development of the recipient's capabilities to replicate or reverse-engineer complete weapon systems or their parts and components.[52] This, of course, is subject to the existence of certain conditions. A good example in this regard is provided by the achievements of China. Development of the country's capabilities can be considered the result of several factors, such as investment in R&D, structural reform and the deployment of a highly skilled workforce, but also the acquisition of foreign technology and development of the capacity to absorb and integrate it into indigenous weapon programmes.[53] Throughout the 1950s China relied heavily on foreign technology acquisitions, especially from the Soviet Union, to develop its defence industry and to train

[45] Tucker J. B., 'The bioweapons threat is broader and closer than commonly thought', *Bulletin of the Atomic Scientists*, 26 Mar. 2008.

[46] Carlson, R., 'Tracking the spread of biological technologies', *Bulletin of the Atomic Scientists*, 21 Nov. 2008.

[47] Carlson (note 46).

[48] Revill and Jefferson (note 44), p. 598.

[49] Windrem, R., 'The world's deadliest woman?', NBC News, 23 Sep. 2004.

[50] Windrem (note 49); and Stewart, I., 'Examining intangible controls: Part II', *Project Alpha*, p. 34.

[51] Windrem (note 49); and Stewart (note 50), p. 34.

[52] Gruselle, B. and Le Meur, P., *Technology Transfers and the Arms Trade Treaty: Issues and Perspective* (Fondation pour la Recherche Stratégique: Paris, 2012), pp. 5–6.

[53] Cheung, T. M., 'Innovation in China's defense technology base: Foreign technology and military capabilities', *Journal of Strategic Studies*, vol. 39 (2016), pp. 728, 732, 736.

its engineers and personnel.[54] This support, however, was not matched by internal efforts—particularly increases in R&D spending—aimed at boosting domestic absorption and innovation capacities. Nor was there a clear distinction between the military and commercial sectors.

The long path to the development of Chinese jet engines is a clear example of the difficulties the country encountered. The first attempt to acquire this technology was made in the 1970s, when Xian Aero-Engine Co. (XAE) approached Rolls-Royce to purchase and locally assemble the Spey Mk 202 jet engine.[55] The ultimate goal of XAE was to acquire the capability to reverse engineer the engine and manufacture its own version domestically. Although XAE obtained valuable insights into the technology—and was also offered the chance to receive training and assistance from its British partners—its ambitions were largely thwarted. In particular, XAE failed to master the jet engine technology due to the small size of the production run and its reluctance to share what it was doing with its British counterparts. This made it very difficult for XAE to make full use of the assistance provided.[56] This failure can also be attributed to the national acquisition strategy on which China relied until the end of the 1980s, which was based mainly on dependence on foreign transfers of complete weapon systems.

The imposition of an arms embargo by Western states in 1989 in response to the violent suppression of protests in Tiananmen Square made the import of complete weapon systems impossible. China's defence acquisition strategy therefore shifted. In the years since, China has increasingly focused on the acquisition of dual-use technologies to be integrated into its domestically developed weapon systems. This has included the acquisition of technology through scientific exchanges, industrial espionage and foreign investments. This strategy has been complemented by increased investment in R&D and subsidies to national enterprises aimed at strengthening Chinese 'defence technological and industrial capacity' and promoting 'indigenous innovation'.[57] The lack of transparency and open-source data makes it difficult to assess the impact of Western technology transfers on the development of the Chinese military. Nonetheless, it seems clear that the Chinese military benefited from the transfer of dual-use items and non-controlled civilian items 'in a number of areas, particularly in the fields of propulsion, helicopters, radars and electronic equipment'.[58] Therefore, the evidence seems to point to the fact that any attempt to legitimately or illegitimately acquire key military or dual-use technologies, coupled with efforts to make a country's civilian and defence sector a suitable recipient for mastering these technologies, can eventually lead to rapid advances in indigenous capabilities.

[54] Bräuner, O., Bromley, M. and Duchatel, M., 'Western arms export to China', SIPRI Policy Paper no. 43 (Jan. 2015), pp. 41–43; and Cheung (note 53), p. 742.

[55] Cheung (note 53), pp. 739–41.

[56] Cheung (note 53), pp. 739–41.

[57] Bräuner, Bromley and Duchatel (note 54), pp. 38–39; see also Bräuner, O., 'Beyond the arms embargo: EU transfers of defense and dual-use technologies to China', *Journal of East Asian Studies*, vol. 13 (2013), pp. 457–82; and Duchatel, M. and Bromley, M., 'Influence by default: Europe's impact on military security in East Asia', *Policy Brief* (European Council on Foreign Relations: London, May 2017).

[58] Bräuner, Bromley and Duchatel (note 54), p. 52.

4. Export controls and transfers of software and technology

UN instruments, the various export control regimes, and EU dual-use and arms export controls all oblige states to implement controls on transfers of certain types of software and/or technology. However, the content and coverage of these controls differ significantly. Some only apply to technology and do not mention software, others only apply to WMD-related items, while others only cover transfers of software and technical data and do not cover knowledge and technical assistance. US re-export controls—with which EU-based companies and research institutes are obliged to comply—also include requirements relating to transfers of software and technology. These requirements differ in certain key respects from EU controls. This section examines the different ways in which controls on transfers of software and/or technology are included in UN instruments, the various export control regimes, EU dual-use and arms export controls, and US re-export controls.

UN instruments

UN arms embargoes generally require states to implement national controls on the transfer of certain types of technology—including knowledge and technical assistance—to the target state.[59] For example, the UN arms embargo on North Korea calls on all states 'to exercise vigilance and prevent specialized teaching or training of [Democratic People's Republic of Korea] DPRK nationals within their territories or by their nationals, of disciplines which could contribute to the DPRK's proliferation sensitive nuclear activities and the development of nuclear weapon delivery systems'.[60] States are also required to impose controls on transfers of certain types of technology in accordance with UN Security Council Resolution 1540.[61] This addresses, among other things, concerns about the illicit trafficking of nuclear weapons technology raised by the discovery of the so-called Khan Network.[62] The resolution instructs all states to 'take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials'.[63] The definition of 'related materials' refers not only to 'equipment' but also to the 'technology covered by relevant multilateral treaties and arrangements, or included on national control lists' and 'which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery'.[64]

The multilateral export control regimes

During the cold war a number of Western states maintained highly restrictive policies on transfers of military equipment and dual-use items to the Eastern Bloc through the Coordinating Committee on Multilateral Export Controls (COCOM). COCOM was established in 1950 with an initial membership of Belgium, France, Italy, Luxembourg,

[59] UN Security Council Resolution 2216, 14 Apr. 2015, para. 14; UN Security Council Resolution 2127, 5 Dec. 2013, para. 54; and UN Security Council Resolution 2270, 2 Mar. 2016, para. 17.

[60] UN Security Council Resolution 1874, 12 June 2009, para. 28; and UN Security Council Resolution 2270, 2 Mar. 2016, para. 17.

[61] UN Security Council Resolution 1540, 28 Apr. 2004; see also 'UNSCR 1540 resource collection', NTI website, 8 June 2015.

[62] The expression refers to the network of illicit nuclear trafficking led by A. Q. Khan, which was discovered in 2004. See Kile (note 37), pp. 552–55.

[63] UN Security Council Resolution 1504, 28 Apr. 2004.

[64] UN Security Council Resolution 1504 (note 61).

the Netherlands, the United Kingdom and the USA.[65] Controls on technology were covered by COCOM controls under its 'General Principle'.[66] The controls on technology—particularly those relating to dual-use items—were among the most contentious aspects of the COCOM regime, and states and companies in Europe frequently complained about their economic impact or questioned their effectiveness as a means of restricting the Soviet Union's economic development or influencing its policies.[67] In the 1970s, the controls on technology were further refined through the adoption of a 'General Technology Note', which stated that technology—in the form of technical data or technical assistance for the development, production and use of all items on the COCOM lists—should be controlled 'insofar as national legislation allowed'.[68] The language was an attempt to reflect the challenges that states might face in applying these controls while also recognizing their importance.[69]

In the early 1990s discussions took place within the COCOM regime on narrowing the controls on technology. These led to the creation of a specific sub-category—'E Technology'—for each control list category. This established case-by-case controls depending on the sensitivity of the individual goods. In addition, a new General Technology Note was agreed, which specified that only the technology 'required' for the development, production or use of a controlled item should be covered.[70] The structure adopted by COCOM for controlling technology was used as the baseline for technology controls in the Wassenaar Arrangement, the AG, the MTCR and the NSG. All four require controls on transfers of technical data, knowledge and technical assistance under their various controls on 'technology', which is defined using more or less common wording.[71] Moreover, the regimes also include controls on transfers of certain types of software. Each regime also specifies that the controls do not apply if the technical data, knowledge or technical assistance in question is 'in the public domain' or refers to 'basic scientific research'. Software in the public domain is also exempted from controls and the same applies when it is 'generally available to the public'.

Wassenaar Arrangement

The Wassenaar Arrangement was established in 1995 'in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations. The aim is also to prevent the acquisition of these items by terrorists'.[72] The Wassenaar Arrangement maintains detailed control lists of both military equipment and dual-use items. The dual-use list includes a General Technology Note which states that the controls also apply to transfers of technology, which is defined as the 'specific information necessary for the "development", "production" or "use" of a product'.[73] This information 'takes the form of technical data or technical assistance'. Technical data can be 'blueprints, plans, diagrams,

[65] US Office of Technology Assessment, 'Ch. VIII: Multilateral Export Control Policy, The Coordinating Committee (CoCom)', *Technology and East-West Trade* (US Office of Technology Assessment: Washington, DC, 1979), p. 153. By 1952 these states had been joined by Norway, Denmark, Canada, West Germany, Portugal, Japan, Greece and Turkey.

[66] Wahren, J., 'Technical briefing note on intangible transfers of technology (ITT)', Oct. 2017, Unpublished.

[67] US Office of Technology Assessment (note 65).

[68] Wahren (note 66).

[69] Wahren (note 66).

[70] Wahren (note 66).

[71] See Wassenaar Arrangement, 'General Technology Note', in 'List of Dual-Use Goods and Technologies and Munitions List', p. 3; Missile Technology Control Regime, 'MTCR Equipment, Software and Technology Annex', p. 14; Nuclear Suppliers Group, 'Guidelines for nuclear transfers', p.11; and Australia Group, 'Control list of Dual-use Chemical Manufacturing Facilities and Equipment and Related Technology and Software'.

[72] Wassenaar Arrangement, 'Introduction'.

[73] Wassenaar Arrangement (note 71), p. 227.

models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories' while technical assistance can assume the shape of 'instruction, skills training, working knowledge, consulting services' and may involve the 'transfer of "technical data"'.[74] The note also provides definitions of 'development', 'production' and 'use'. Development relates 'to all stages prior to serial production'; production refers to 'all production stages'; and use to 'operation', 'installation' and 'maintenance'.[75]

The aim of the General Technology Note is to limit controls to key technologies. Hence, a controlled technology is what is 'required' for the development, production or use of a controlled item. The term 'required' is in turn defined as that 'portion' of the technology necessary to achieve 'the controlled performance levels, characteristics or functions'.[76] The General Technology Note also states that the controls apply 'according to the provisions in each Category'. Each control list category includes a subcategory E for technology. In principle, the wording of each sub-category is the same, specifying that the controls apply to technology for the development, production or use of the goods listed.[77] In certain cases the dual-use list also imposes controls on specific technologies without making any reference to another controlled item. For example, category 7E102 imposes controls on '"Technology" for protection of avionics and electrical subsystems against electromagnetic pulse (EMP) and electromagnetic interference (EMI) hazards, from external sources'.[78] As noted above, the General Technology Note also limits the coverage of the controls by specifying that they do not apply to information available in the 'public domain', 'basic scientific research' or the 'minimum necessary information for patent applications'.[79] In this context, 'public domain' is defined as '"technology" or "software" which has been made available without restrictions upon its further dissemination'.[80] Meanwhile, basic scientific research is defined as 'experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective'.[81]

The dual-use list also includes a General Software Note. However, unlike the General Technology Note, it does not describe which software is subject to control. Instead, each control list category includes a Subcategory D which imposes controls on software 'specially designed or modified for the "development", "production" or "use"' of specific listed items. For example, Category 5.A of the Wassenaar Arrangement dual-use list imposes controls on '"Information security" systems, equipment and components . . . designed or modified to use "cryptography for data confidentiality"' while Category 5.D imposes controls on related software. However, the General Software Note includes a set of decontrols that describe which software is not covered by the controls. This specifies that software that is 'generally available to the public', 'in the public domain' or the 'minimum necessary "object code" for the installation, operation, maintenance (checking) or repair of those items whose export has been authorised' is not covered. However, even with these decontrols in place, many different forms of computer software that are used in banking and information technology security are still subject to dual-use export controls.

[74] Wassenaar Arrangement (note 71), p. 227.
[75] Wassenaar Arrangement (note 71), pp. 208, 220, 228.
[76] Wassenaar Arrangement (note 71), p. 222
[77] Wahren (note 66).
[78] Wahren (note 66).
[79] Wassenaar Arrangement (note 71), pp. 3, 203.
[80] Wassenaar Arrangement (note 71), p. 206.
[81] Wassenaar Arrangement (note 71), p. 206.

New controls on certain types of software and technology have been added to the Wassenaar Arrangement in recent years. In 2013 the Wassenaar Arrangement added controls on 'technology' and 'software' used in the development or use of 'intrusion software', which law enforcement agencies (LEAs) and intelligence agencies use to remotely monitor computers and mobile phones. Since the adoption of the controls on intrusion software, companies and researchers working in IT security have argued that the language used describes not just the types of systems used by intelligence agencies and LEAs, but also systems and processes that are essential to IT security, particularly systems used for 'penetration testing' and processes of 'vulnerability disclosure'.[82] In 2016 and 2017 the USA proposed amendments to the content of the controls at the Wassenaar Arrangement.[83] In 2017 more detailed explanatory notes were added to the controls on intrusion software, specifying that they did not apply to software that was designed to provide 'software updates' as well as 'vulnerability disclosure' and 'cyber incident response'.[84]

The Wassenaar Arrangement recognizes that the implementation of controls on software and technology represents an important aspect of participating states' export control systems. A Statement of Understanding attached to the General Technology Note states that participating states have agreed to treat controlled technology 'with vigilance in accordance with national policies and the aims of this regime'.[85] The particular importance of enforcing controls on ITT is stressed in the Statement of Understanding from 2001, which notes that 'national export control legislation should therefore permit controls on transfers of listed "software" and "technology" irrespective of the way in which the transfer takes place'.[86] This is also stressed in the 'Best Practices for Implementing Intangible Transfer of Technology' document agreed by the participating governments at the 2006 plenary.[87] In particular, the 2006 document notes that ensuring that these controls are implemented is considered crucial to the 'credibility and effectiveness' of domestic export control regimes.[88] However, the Wassenaar Arrangement also notes that controlling ITT is a particularly challenging undertaking. A second Statement of Understanding notes that 'Member Governments are expected to exercise controls on intangible "technology" as far as the scope of their legislation will allow'.[89]

The scope of the Wassenaar Arrangement's controls on military equipment is outlined in its munitions list. Until 2004 a General Technology Note for the Wassenaar Arrangement munitions list used very similar wording to the one attached to the dual-use list. In 2004 this note was removed and replaced with a separate control list category—ML22—which covers 'Technology'.[90] In principle, ML22 imposes the same controls on transfers of technology as those imposed by the General Technology Note in the dual-use list.[91] One important difference is that ML22 includes controls

[82] Bratus, S. et al., '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. 'Penetration testing tools' are used to test the security of a network by simulating attacks against it in order to locate vulnerabilities. 'Vulnerability disclosure' is the means through which software vulnerabilities are identified and reported.

[83] Cardozo, N. and Galperin, E., 'Victory! State Department will try to fix Wassenaar Arrangement', Electronic Frontier Foundation, 29 Feb. 2016. However, due to resistance from other participating states, only minor adjustments to the controls were adopted. Thomson, I., 'Wassenaar weapons pact talks collapse leaving software exploit exports in limbo', *The Register*, 21 Dec. 2016.

[84] Wassenaar Arrangement, 'List of Dual-use Goods and Technologies and Munitions List', 7 Dec. 2017.

[85] Wassenaar Arrangement (note 71), p. 233.

[86] Wassenaar Arrangement, 'Statement of Understanding on Intangible Transfers of Software and Technology (Agreed at the 2001 plenary)'.

[87] Wassenaar Arrangement (note 3).

[88] Wassenaar Arrangement (note 3).

[89] Wassenaar Arrangement (note 71), p. 233.

[90] Wahren (note 66).

[91] Wahren (note 66).

on a specific kind of integration-technology in ML22.b.1, 'key technology for design, assembly and use of complete production installations for items on the munitions list, even if their components are not controlled'.[92] Controls on software are imposed in the Wassenaar Arrangement munitions list through ML21, which covers software designed or modified for the development, production and maintenance of equipment and software specified in the munitions list or for the development or production of any material specified on the munitions list.[93] The list also covers controls on software specifically designed for 'modelling, simulating or evaluating' military weapon systems or operational scenarios; for assessing the effects of 'conventional, nuclear, chemical or biological weapons'; or for Command, Communications, Control and Intelligence (C3I) and Command, Communications, Control, Computer and Intelligence (C4I) applications.[94]

Other export control regimes

The MTCR, the NSG and the AG are each intended to address a particular set of proliferation challenges related to WMD and their associated delivery systems. The MTCR is focused on controlling transfers 'that could make a contribution to delivery systems (other than manned aircraft)' for WMD.[95] The NSG aims to avert the proliferation of nuclear weapons through 'procedures in relation to the transfer of certain equipment, materials, software, and related technology that could make a major contribution to a "nuclear explosive activity", an "unsafeguarded nuclear fuel-cycle activity" or acts of nuclear terrorism'.[96] Finally, the AG aims to prevent 'the risks of proliferation and terrorism involving chemical and biological weapons (CBW) by controlling tangible and intangible transfers that could contribute to CBW activities by states or non-state actors'.[97]

The MTCR, the NSG and the AG control software and technology that are 'specially designed' for the development, production or use of certain controlled items using language that differs only slightly from that used in the Wassenaar Arrangement control lists, and these differences have no substantial implications.[98] The MTCR, the NSG and AG control lists also place limits on the scope of these controls using language that is broadly similar to the language in the Wassenaar Arrangement's General Technology Note and General Software Note. The scope of these controls varies from regime to regime. For example, the AG list only includes controls on one type of software, specifically dedicated software for 'toxic gas monitors and monitoring systems'.[99] In addition, although all four regimes include so-called catch-all controls—which place controls on certain goods, software and technology that do not appear on their control lists—their precise scope varies from case to case. The Wassenaar Arrangement catch-all control applies to non-listed dual-use items being transferred for a military end-use in 'destinations subject to a binding United Nations Security Council arms embargo, any relevant regional arms embargo either binding on a Participating State or to which a Participating State has voluntarily consented to adhere'.[100] In contrast, the MTCR,

[92] Wahren (note 66).
[93] Wassenaar Arrangement (note 84), p. 206
[94] Wassenaar Arrangement (note 84), p. 206.
[95] Missile Technology Controls Regime, 'Guidelines for sensitive missile relevant transfers', [n.d.].
[96] Nuclear Suppliers Group (note 71), p. xii.
[97] Australia Group, 'The Australia Group'.
[98] Wahren (note 66).
[99] Australia Group, 'Control list of dual-use chemical manufacturing facilities and equipment and related technology and software', May 2017.
[100] Wassenaar Arrangement, 'Statement of Understanding on Control of Non-Listed Dual-Use Items (Agreed at the 2003 Plenary)'.

the NSG and the AG catch-all controls apply to non-listed items—as opposed to just non-listed dual-use items—and apply to all destinations, regardless of whether they are subject to an arms embargo. The MTCR catch-all covers non-listed items that may be intended 'for use in connection with delivery systems for weapons of mass destruction other than manned aircraft'.[101] The NSG catch-all applies to non-listed items that may be intended 'for use in connection with a "nuclear explosive activity"'. The AG catch-all applies to non-listed items that may be intended 'for use in connection with chemical or biological weapons activities'.[102]

The EU export control regime

The Dual-use Regulation

Controls on EU member states' trade in dual-use goods are governed by EC Regulation 428/2009, the 'EU Dual-use Regulation'.[103] Annex I of the EU Dual-use Regulation incorporates the control lists of the multilateral export control regimes. The language in the General Technology Note, which applies to the items in categories 1 to 9 of the EU dual-use list and the decontrols on software and technology, are, apart from some minor editorial changes, the same as those in the Wassenaar Arrangement. However, the controls on nuclear-related technology in the EU Dual-use Regulation differ slightly from those of the NSG. The NSG guidelines use similar language to the Wassenaar Arrangement's General Technology Note and define controlled technology as the 'specific information required for the "development", "production", or "use" of' an item. In the EU Dual-use Regulation, the Nuclear Technology Note states that technology 'directly associated' with items listed in Category 0 of Annex I, which covers the NSG 'Trigger List', are subject to control. In addition, the Nuclear Technology Note in the EU Dual-use Regulation does not address the decontrol for technology, which is the 'minimum necessary information for patent applications', that appears in the General Technology Note of the EU Dual-use Regulation. This means that a wider range of technology is subject to control at the EU level than is directly required under NSG guidelines.

The EU Dual-use Regulation also provides a detailed definition of export that includes language on what constitutes an intangible transfer of software and technology. This states that an export can be the:

> transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and partnerships outside the Community. This definition of export also applies to oral transmission of technology when the technology is described over the telephone.[104]

The definition contains two important components that reflect the legal basis for the EU export control regime and create differences between the EU Dual-use Regulation and the multilateral export control regimes.

First, since the EU Dual-use Regulation forms part of the EU's 'common commercial policy', it cannot be used to regulate the cross-border movement of people. Hence, while the Dual-use Regulation includes the Wassenaar Arrangement's definition of technology, it defines 'export' as only covering the oral transmission of

[101] MTCR, 'Guidelines for sensitive missile-relevant transfers'.

[102] Nuclear Suppliers Group (note 71).

[103] Council of the European Union, Council Regulation (EC) 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*, L 134, p. 13.

[104] Council of the European Union (note 103), p. 2.

technology when 'described over the telephone'.[105] Certain forms of 'in-person transfers' of knowledge and technical assistance are regulated by Council Joint Action 2000/401/CFSP.[106] Since it forms part of the EU's Common Foreign and Security Policy, the Joint Action could be used to require EU member states to impose controls on the cross-border movement of people. Hence, Article 2 of Council Joint Action 2000/401/CFSP states that technical assistance related to WMD or their related delivery mechanisms shall be subject to control when it is provided outside the EU by a 'natural or legal person established in the European Community'. Technical assistance is, in turn, defined as taking a range of forms, such as 'instruction, training, transmission of working knowledge or skills or consulting services'. In addition, Article 3 states that EU member states should consider applying such controls to any technical assistance relating to military end-uses that is provided in countries subject to EU, Organization for Security and Co-operation in Europe (OSCE) or UN arms embargoes.[107] However, this leaves the provision of knowledge and technical assistance associated with other controlled dual-use items outside the scope of EU controls.

Second, the Dual-use Regulation defines 'export' as 'an export procedure within the meaning of Article 161 of Regulation (EEC) No. 2913/92 (the Community Customs Code)'.[108] As such, the Dual-use Regulation regulates the cross-border movement of goods to destinations outside the EU. The only intra-community transfers that are subject to licensing requirements are the more sensitive items listed in Annex IV of the Regulation. This focus on the cross-border movement of items means that transfers between two different branches of the same company are subject to control, even if the goods stay under that company's ownership, when one is located inside the EU and one is located outside. This means that an email containing controlled software or technical data sent from a company branch inside the EU to a company branch outside the EU—or the upload of controlled data to a server located outside the EU—would require an export licence. However, a transfer of knowledge or technical assistance that occurs within national borders—such as those that may occur when a foreign citizen enters the EU to attend university courses or to participate in industry training programmes—would not require an export licence. This is not necessarily the way that controls are implemented at the EU level since the requirements contained in the EU Dual-use Regulation are supplemented by additional national regulations. However, the precise way in which this is done can vary between EU member states (see below).

In 2011 the European Commission launched a review of the EU Dual-use Regulation. Following a series of consultations, the Commission published a proposal in the form of a draft 'recast' of the regulation in September 2016. In addition to addressing a range of other issues, the proposal attempts to bring greater clarity to the application of controls on software and technology, and particularly ITT. For example, under the proposed recast language, controls would only apply when the technology is made available to 'legal and natural persons and partnerships' outside the EU, rather than simply 'a destination' outside the EU as is currently the case.[109] The Commission has described the new language as—in part—an attempt to 'facilitate the use of cloud services'.[110] However, Digital Europe has argued that use of the term 'making available' could be interpreted as meaning that a company supplying technology that

[105] Council of the European Union (note 103), p. 2.

[106] Council Joint Action of 22 June 2000 concerning the control of technical assistance related to certain military end-uses, *Official Journal of the European Union*, L 159, 22 June 2000.

[107] Council Joint Action of 22 June 2000 (note 106).

[108] Council of the European Union (note 103), p. 2.

[109] 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, 28 Sep. 2016, p. 19.

[110] European Commission (note 109), p. 7.

allows another company to provide cloud services would be held responsible for who downloads information from the cloud.[111] It is therefore unclear whether the new language would generate a harmonized approach to cloud computing in member states' arms export controls. The Commission has also proposed a new EU General Export Authorization (EUGEA) for 'Intra-company transmission of software and technology'.[112] The Commission has described the proposal as aimed at facilitating transfers of dual-use technology within a company and its affiliates in non-sensitive countries, in particular for research and development purposes.[113] During an impact assessment conducted by the Commission in 2016, the proposed new licence was identified by companies that responded to a survey as the most popular of a range of potential new EUGEAs, and 85 per cent supported its introduction.[114]

The Commission's proposal is also seeking to address gaps in the coverage of the controls on technical assistance by providing a legal definition of technical assistance and clarifying related applicable controls.[115] The Commission argues that following the entry into force of the Lisbon Treaty, the 'supply of technical assistance services involving a cross-border movement falls under Union competence'.[116] The proposed definition of technical assistance will cover 'any technical support related to repairs, development, manufacture, assembly, testing, maintenance, or any other technical service, and may take forms such as instruction, advice, training, transmission of working knowledge or skills or consulting services, including verbal forms of assistance'.[117]

The review of the EU Dual-use Regulation has also created an opportunity to revisit debates about whether, and if so how, export controls should be applied to publications, intrusion software and—particularly—encryption. Since the 1990s, the USA has eased controls on exports of software and other systems that employ cryptography through the use of exemptions and 'open licences' that allow for multiple shipments under the same authorization.[118] Many of these exemptions and open licences are not replicated in Europe. The Foreign Affairs Committee of the European Parliament emphasized in its opinion on the Commission's proposal that 'not every technology requires controls' and argued that 'exports of technologies that actually enhance human rights protection, such as encryption, should be facilitated'. However, EU member states appear to be broadly in favour of retaining the existing controls on cryptography. One of the appeals of the existing controls is that they enable governments to have oversight of—and the potential to control—items that are not directly subject to export control but which are nonetheless of potential interest from a national security or human rights perspective. For example, before they were added to the Wassenaar Arrangement control list, exports of intrusion software and other cyber-surveillance technologies were subject to export controls on the basis of the level of cryptography that they employed.[119]

[111] 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).

[112] European Commission (note 109), p. 8.

[113] European Commission (note 109), p. 7.

[114] European Commission, '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 (recast)', 28 Sep. 2016, p. 32.

[115] European Commission (note 109), p. 7.

[116] European Commission (note 109), p. 13.

[117] European Commission (note 109), p. 20–21.

[118] See Grimmett (note 2).

[119] 'British Government admits it has already started controlling exports of Gamma International's FinSpy', Privacy International, 9 Sep. 2012.

EU Common Position on Arms Exports

EU member states adopted the EU Code of Conduct on Arms Exports in 1998. This was transformed into a legally binding Common Position in 2008.[120] The Common Position includes operative provisions on information exchange and consultation that aim to harmonize member states' application of eight common criteria for assessing arms export licences, as well as an agreed EU military list that defines the range of goods that are subject to control. The EU military list is based on the munitions list of the Wassenaar Arrangement. All of the controls on technology and software on the EU military list are identical to those on the Wassenaar Arrangement military list.[121]

US re-export controls

The re-export of items of US origin on the US military list, which mostly consists of items on the Wassenaar Arrangement military list, is subject to control under the US International Traffic in Arms Regulations.[122] These controls apply even if the item is integrated into another system, regardless of what percentage of the new system is of US-origin. The re-export of items of US origin on the Commerce Control List (CCL), which mostly consists of items listed on the Wassenaar Arrangement dual-use list, is subject to control under the Export Administration Regulations.[123] Certain re-exports of CCL items to less sensitive destinations are subject to licensing exemptions, and if the item is integrated into another system and only a certain percentage of the new system is of US-origin the controls do not apply. However, US companies do not always inform foreign companies about the Export Control Classification number of the exported CCL item since they do not necessarily need a licence for the export. This makes it extremely difficult to know what percentage of a particular system is of US origin and remains subject to US re-export controls.[124] In addition, exports to certain more sensitive destinations—particularly China, Cuba, Iran, North Korea, Sudan and Syria—are controlled regardless of what percentage of the new system is of US-origin. US re-export controls apply equally to transfers of tangible and intangible items and remain in place throughout the lifecycle of the item. Unlike in the case of the Dual-use Regulation or the EU Common Position, US controls also apply to so-called deemed exports—the release of controlled technology or software in the USA to a national of another country—and deemed re-exports—the release of controlled technology or software 'in one foreign country to a national of another foreign country'.[125] The USA also has a number of programmes in place aimed at ensuring that its controls are respected, and often uses legal measures such as substantial fines, prison sentences and debarments to penalize violations.[126]

[120] Council of the European Union, 'European Union Code of Conduct on Arms Exports', 8675/2/98 Rev. 2, 5 June 1998; and 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.

[121] Wahren (note 66).

[122] Gustavus, J. D., 'What US and Chinese companies need to know about US export control laws applicable to China', World ECR, no. 26 (Oct. 2013).

[123] US Department of Commerce, Bureau of Industry and Security (BIS), 'Scope of the Export Administration Regulations', pp. 11–12; and US Department of Commerce, Bureau of Industry and Security (BIS), 'Guidance on Reexports/Transfers (in-country) of US-Origin Items or Non-US-made Items Subject to the Export Administration Regulations (EAR)'.

[124] Thomas, B., Export Compliance Manager, IMEC, Communication with the authors, 5 Mar. 2018.

[125] US Department of Commerce, Bureau of Industry and Security (note 123).

[126] US Department of Justice, 'Retired university professor sentenced to four years in prison for arms export violations involving citizen of China', Press release, 1 July 2009.

5. National practices in the EU and key challenges

Although the Dual-use Regulation forms part of the EU's 'common commercial policy', member states have substantial leeway in terms of how export controls are implemented at the national level. This involves determining whether particular items are subject to control, whether controls are implemented through the use of individual or open licences, whether licences are approved or denied, and what additional control measures companies will be required to implement via—for example—the use of end-user certificates. EU member states have even more leeway when it comes to implementing controls on exports of military goods. This leads to key differences in the way controls on transfers of software and technology are implemented by EU member states. These can generate compliance-related challenges for companies and research institutes, particularly those with operations and supply chains in two or more countries. However, they are also a potential source of good practice and provide indications of areas where agreed EU standards and guidance material could be generated. This section summarizes the main differences in the way EU member states implement controls on transfers of software and technology. The section highlights some of the main challenges for national authorities when seeking to implement controls, and for companies and research institutes when seeking to comply with them.

National practices among EU member states

Which software and technologies are subject to control

One clear, but difficult to assess, area of difference between the policies of EU member states concerns whether a particular piece of software or technology is subject to control. This is more of an issue in the field of dual-use export controls than military goods, given that the latter are more clearly defined and understood. Moreover, it is also something that is particularly true in the field of technology controls, where establishing what is and is not subject to control can be a difficult process that is open to interpretation. In particular, even though the term 'required' is defined in the EU Dual-use Regulation (see above), there is room for interpretation of whether particular software or technology, tangible or intangible, is *required* for the 'production', 'development' or 'use' of a specific control list item. This is often raised as a particular issue for ITT controls, but in many ways it is equally challenging for both tangible and intangible transfers. The means of transfer—that is whether it is technical data sent by email or included in a hard-copy manual—is of no relevance when determining whether it is subject to control.

A number of EU member states have sought to provide greater clarity with regard to how they determine which software or technology is or is not subject to control.[127] In June 2016 the German export licensing authority—the German Federal Office for Economic Affairs and Export Control (BAFA)—published a guidance document that provides examples of the kind of technology that is covered—and therefore subject to control—and what is not.[128] In the Netherlands national guidance material stipulates that when technology is described over the telephone, it only becomes subject

[127] Wahren (note 66).

[128] Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), 'Technologietransfer und Non-Proliferation: Leitfaden für Industrie und Wissenschaft' [Transfer of technology and non-proliferation: Guideline for industry and academia], Eschborn, June 2016, pp. 11–12.

to control if the description is detailed enough to allow the receiver to reproduce the information.[129]

However, there is little in the way of agreed guidance at the EU level to clarify whether a particular piece of software or technology is subject to control. In 2016 the EU published a guidance note on the application of the cryptography note exemption, which applies to both the Wassenaar Arrangement and the EU Dual-use Regulation.[130] The cryptography note exemption outlines the situations in which a particular export is exempt from the controls on the export of software and other items that contain a certain level of encryption. The note 'also sets out good practices for interpreting the relevant provisions of the EU Dual-use Regulation' with the aim of reducing 'divergences in their application'.[131] However, the document provides no concrete examples of which systems should or should not be controlled. It also makes clear that, although it has been agreed by all EU member states, the guidance is not binding and does not override rulings by national authorities.

Which transfers are subject to control

As noted above, the definition of export used in the Dual-use Regulation means that it is the act of moving software or technology to locations outside the EU that is subject to export licensing procedures. However, EU member states differ on the precise application of this principle, with some focused on the act of crossing a border while others focus more on the act of someone accessing controlled items outside the EU. How these differences manifest themselves at the national level depends on the definition of export that the member state uses, what kind of guidance material it issues and the types of open licences that companies and research institutes are allowed to use when implementing export controls. While these issues are not necessarily specific to ITT—or even controls on software and technology—many of the more contentious cases arise in these fields. For example, one area where EU member states are understood to differ is on accessing emails overseas when the email in question—or an attachment to the email—contains controlled technology or software. The issue can become more complex if the recipient is unaware that the email contains controlled technology or software, or the sender is unaware that the recipient is in a foreign country at the time it is sent. According to one analysis, 'some states consider that reading such e-mails and their attachments abroad constitutes an export, and thus a licensable act. Other states take a more pragmatic approach [and] advise that if the recipient does not divulge the contents of an e-mail to anyone abroad they have not breached controls'.[132] Similar issues apply with regard to taking laptops overseas.[133]

The differences in member states' controls have become more noticeable as a result of ongoing discussions about whether or how dual-use and arms export controls should apply to the field of cloud computing. This issue is particularly complex because of the ways in which data is stored and shared, and the presence of third-party service providers. There are at least two areas in which the way states' controls on software and technology apply to cloud computing differ.

[129] 'Tweede Kamer der Staten-Generaal, Regels inzake de controle op diensten die betrekking hebben op strategische goederen (Wet strategische diensten)', Memorie van toelichting, 2011, p. 2. Cited in 'The Netherlands', eds O. Jankowitsch-Prevor and M. Quentin, *European Dual-use Trade Controls: Beyond Materiality and Borders* (Peter Lang SA, 2014).

[130] European Commission, Directorate-General Trade, 'FAQ on controls of "information security" items and implementation of the cryptography note exemption', Guidance note, Oct. 2016.

[131] Bauer, S. et al., 'Internal compliance and export control guidance documents for the Information and Communications Technology sector', SIPRI Good Practice Guide: Export Control ICP Guidance Material no. 2 (SIPRI: Stockholm, 2017).

[132] Chilvers (note 8).

[133] Chilvers (note 8).

First, there is the question of whether controls take account of the location of the servers where the software or technology is stored. In Germany, the act of moving technology, data or software to a server located outside of the EU constitutes an export and is subject to licensing controls.[134] In addition, the act of granting access to the software or technology to user's outside the EU may also be subject to control, as either an export—in the form 'provision'—or an act of brokering.[135] The UK applies the principle that it is the location of the person accessing the data, rather than the location of the server, that determines whether a licence is required.[136] Hence, while the act of uploading controlled technology to a server outside the UK would not be controlled, allowing someone based outside the UK—or the EU depending on whether the controlled technology is military or dual use—to access that data would constitute an export. Controls in the Netherlands are also focused on the location of the person accessing the data rather than the location of the server, but only if the server is secure.[137] However, the Netherlands can place restrictions on server location in the case of items on the military list or particularly sensitive dual-use items.[138]

A second difference concerns the steps companies are required to take in order to ensure that technical data or software uploaded to a cloud is kept secure. The Netherlands has indicated that a company would need to ensure that information stored on the cloud is 'protected according to an encryption standard that is customary in your sector' and—at a minimum—that this should involve the use of end-to-end encryption.[139] The UK does not require, but would advocate, that companies put in place adequate measures to prevent unauthorized access to the data and does not explicitly call for the use of end-to-end encryption.[140] Its position is that end-to-end encryption is not a solution or a substitute for the need to comply with export controls.[141] Moreover, it can help companies if they are able to use alternative solutions that meet both their own commercial interests and the needs of export controls.[142] Finally, Italian legislation was recently updated in order to clarify that 'exporters, brokers and suppliers of technical assistance' making use of these data transfer systems must adopt 'secure and trackable access procedures' and 'systems able to report the access'.[143]

The way in which controls are applied

Even in the many cases where there is clear agreement about whether particular software or technology—or a particular transfer—should be controlled, there can still be differences over which type of licence is used to apply those controls. Exports can be controlled through individual licences, which allow for single shipments to a particular end-user, or open licences, which can allow multiple shipments to one or more end-users. For dual-use items the EU has agreed a number of EU General Export Authorizations (EUGEAs) that can be used by all companies and research institutes in the EU.[144] For example, General Export Licence EU001 can be used for exports of

[134] BAFA (note 128), p. 20.

[135] BAFA (note 128), p. 20.

[136] Gallacher, D., UK Department for International Trade, Communication with the author, 8 Dec. 2017.

[137] Netherlands Ministry of Foreign Affairs, 'Factsheet: Export via de cloud' [Fact sheet: Export via the cloud], 1 Mar. 2018.

[138] Sprangers, J., Directorate-General for International Trade Policy and Economic Governance, Netherlands Ministry of Foreign Affairs, Interview with the author, 27 Oct. 2017.

[139] Netherlands Ministry of Foreign Affairs (note 137).

[140] Gallacher (note 136).

[141] Gallacher (note 136).

[142] Gallacher (note 136).

[143] Decreto Legislativo del 15 Dicembre 2017 no. 231 [Legislative Decree of 15 Dec. 2017, no. 231], Gazzetta Ufficiale Serie Generale no. 32, 8 Feb. 2018, pp. 1–10.

[144] There are currently six EUGEAs, covering exports: (*a*) to Australia, Canada, Japan, New Zealand, Norway, Switzerland and the USA; (*b*) of certain dual-use items to certain destinations; (*c*) for repairs or of replacement parts;

dual-use items to Australia, Canada, Japan, New Zealand, Norway, Switzerland and the USA unless they are covered by Annex IV of the Dual-use Regulation. None of the EUGEAs are specifically targeted at transfers of software or technology, or ITT but all of them can—to a greater or lesser extent—be used for such transfers.

As long as they meet certain conditions, EU member states are also largely free to issue National General Export Authorizations (NGEAS). Member states vary in the type of NGEAs they issue for a number of reasons, such as the presence and the degree of development of specific industrial sectors on their territory. However, there are difficulties associated with finding accurate data on the coverage—and especially the use—of NGEAs. This makes it hard to measure differences in the practices of EU member states and the extent to which the controls on transfers of software, technology or ITT are applied. However, only nine of the 28 EU member states report having issued NGEAs, which implies that national practices differ at least to a certain extent.[145]

For example, Austria has an NGEA for 'frequency changers specified in entry 3A225 and related software and technology'.[146] Germany has issued a general licence for 'telecommunications and data security'.[147] The UK has an open general export licence (OGEL) for 'Technology for Dual-Use items'.[148] The UK also has an OGEL for 'software and source code for military goods' and 'technology for military goods'.[149] In January 2017 the UK published a new OGEL 'allowing people who are temporarily based abroad to access their business technology and information technology systems in the UK'.[150] The open licences issued by the UK in this area form part of a wider effort in recent years to encourage exporters to utilize open licences rather than individual licences where possible 'and where the exports do not raise significant concerns against the UK Consolidated Criteria'. [151] The use of open licences in the UK is supported by regular compliance visits by the export licensing authorities. The UK's approach when issuing a company with an open licence is to consider—among other things—their track record with individual licences. Inspectors then visit regularly to check that the company is complying with its obligations.[152]

Whether exports are controlled using individual licences or open licences can make a significant difference to the regulatory burden imposed on a company or research institute. In 2014 it was reported that Germany was controlling exports of intrusion software produced by Gamma International through individual licences for each transfer, and requiring the submission of end-user certificates stating that the products would not be used to infect any device located in, or associated with, Germany.[153] It was later reported that Gamma Group had moved its work on intrusion software to

(*d*) of a temporary nature for exhibitions or fairs; (*e*) of certain types of telecommunications equipment; and (*f*) of certain types of chemical. UK Department for International Trade, Export Control Joint Unit, 'Guidance: EU General Export Authorisations', 14 Dec. 2017.

[145] European Commission, Information note, Information on measures adopted by Member States in conformity with articles 5, 6, 8, 9, 10, 17 and 22 of Council Regulation (EC) 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, *Official Journal of the European Union*, C 304/03.

[146] European Commission, Information note (note 145).

[147] European Commission, Information note (note 145).

[148] European Commission, Information note (note 145).

[149] UK Government, 'Open General Export Licence (software and source code for military goods)', 20 Jan. 2017; and 'Open General Export Licence (technology for military goods)', 13 July 2017.

[150] UK Government, 'Open General Export Licence (access overseas to software and technology for military goods: individual use only)', 20 Jan. 2017.

[151] House of Commons Committees on Arms Exports Controls, *Scrutiny of Arms Exports and Arms Controls (2015): Scrutiny of the Government's Strategic Export Controls Annual Report 2013, the Government's Quarterly Reports from October 2013 to June 2014, and the Government's Policies on Arms Exports and International Arms Control Issues* (Stationary Office: London, Mar. 2015), p. 38.

[152] Gallacher (note 136).

[153] Page, K., 'Six things we know from the latest FinFisher documents', Privacy International, 15 Aug. 2014.

offices in countries that are not members of the Wassenaar Arrangement.[154] In contrast, until April 2016 it was reported that Italy was controlling exports of intrusion software produced by Hacking Team through the use of general licences, meaning that they received a single licence for exports of intrusion software that was valid for multiple years and destinations.[155] There are no reports to indicate that Hacking Team has ever considered leaving Italy. However, determining the extent to which these differences are a factor is extremely difficult given the lack of publicly accessible data on licences granted.

Other control requirements in related areas also have the potential to affect the way transfers of software or technology are regulated at the member state level. For example, French national controls on cryptography, when this is treated as a dual-use technology, put in place a two-step procedure to be followed for the issue of licences for exports outside the EU. First, the provider of the 'means of cryptography' (moyen de cryptologie) must submit an authorization request to the National Agency for Information Systems Security (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI). Then the exporter must submit an export licence request to the competent authority, Le Service des biens à double usage (SBDU), which must include the above-mentioned document issued by the ANSSI.[156] The ANSSI is also responsible for classifying which means of cryptography can be considered in the public domain and therefore exempt from export controls. [157]

The application of controls to 'deemed exports'

Another key difference is the question of how member states regulate transfers that may occur through a foreign citizen attending a university course or participating in an industry training programme. As noted above, such transfers are not covered by either the Dual-use Regulation or Council Joint Action 2000/401/CFSP. This means that member states have to supplement these instruments with additional legal measures at the national level if such transfers are to be made subject to control, something that several EU member states have done.[158] In Germany, the 'supervision of graduate, doctoral or post-doctoral students in the area of higher education' is given as an example of how a transfer of technical assistance might take place.[159] The transfer of knowledge through seminars or other forms of training is also considered technical assistance in the Foreign Trade and Payments Act.[160] Similar language is used in the relevant Italian legislation, where technical assistance is now explicitly placed under the control of the state and defined, inter alia, as the transfer of instructions, competences, skills and training.[161] In Hungary it is made clear that export control

[154] Omanovic, E., 'Surveillance companies ditch Switzerland, but further action needed', 5 Mar. 2014, Privacy International; 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.

[155] Currier, C. and Marquis-Boire, M., 'A detailed look at hacking team's emails about its repressive clients', The Intercept, 7 July 2015. In Apr. 2016 it was reported that the general licence for the export of intrusion software had been suspended, and since then Hacking Team has had to apply for individual licences. 'Hacking Team, revocata l'autorizzazione globale all'export del software spia: stop anche per l'Egitto dopo il caso Regeni' [Hacking Team, global authorization for the export of spy software revoked: stop also on Egypt after the Regeni case], *Il Fatto Quotidiano*, 6 Apr. 2016.

[156] ANSSI, 'Contrôles réglementaire sur la cryptographie' [Regulatory controls on cryptography].

[157] ANSSI, 'Démarches à accomplir' [Steps to take].

[158] Rebolledo (note 23), p. 8.

[159] BAFA (note 128), p. 24.

[160] Foreign Trade and Payments Act of 6 June 2013 (Federal Law Gazette [BGBl.] Part I, p. 1482).

[161] Decreto Legislativo del 15 dicembre 2017 [Legislative Decree of 15 Dec. 2017, no. 231] (note 143).

obligations apply even if the controlled technology is transferred to a foreign national on Hungarian territory.[162]

However, in many EU member states these types of transfer are approved not through the use of export licensing procedures, but through the use of visa-screening procedures. The UK has put in place an Academic Technology Approval Scheme (ATAS) that screens applications by postgraduate researchers from abroad to study potentially proliferation-sensitive fields.[163] This scheme 'requires all international students subject to existing UK immigration permissions' who wish 'to study for a postgraduate qualification in certain sensitive subjects', that is subjects where knowledge could be used in WMD programmes or their means of delivery, 'to apply for an ATAS certificate before they can study in the UK'.[164] This requirement applies to all citizens of all states outside the European Economic Area (EEA) and Switzerland.[165] In November 2011, France adopted a law specifically addressed to research centres, universities, enterprises and higher education institutes to protect the scientific and technical potential of the country against the risks of misappropriation, diversion and use for terroristic ends or the development of weapons of mass destruction and their delivery systems.[166] The law requires security clearance in order to work in specific protected sectors (secteurs protégés), which are outlined in the French legislation, or to access restricted areas (zones à régime restrictif) where sensitive material is stored in order to carry out research, prepare a doctoral thesis or undergo professional training.[167] The law does not impose any particular restrictions based on nationality. In Sweden, although transfers of technical assistance are not controlled in-country, 'consular vigilance' is an integral part of the country's export control policy. This vigilance is exercised through the assessment of applications for 'admission or residence permits for studies' related to 'sensitive information and technologies'.[168] These measures also include 'cooperation between the authorities concerned' aimed at increasing proliferation awareness 'with regard to sensitive university study programmes or research partnerships'.[169]

These models have not been systematically adopted by all EU member states, however, due in some instances to domestic legal constraints. In the Netherlands, the application of nationality-based screening procedures to students undertaking potentially proliferation-relevant studies has been challenged in the courts. The rulings handed down uphold the principle that unless these restrictions are based on an international legal obligation, their implementation is discriminatory.[170] For this reason, such controls can legitimately be applied to students who can plausibly be linked to the North Korea Nuclear Programme—or to any other programme where relevant UN sanctions are in place—but not to the programmes of other countries of concern. The Dutch

[162] Stefan, L., 'Intangible technology controls in Hungary', eds O. Jankowitsch-Prevor and Q. Michel, *European Dual-use Trade Controls: Beyond Materiality and Borders* (Peter Lang SA, 2014), pp. 115–21; and Government Decree no. 13/2011 (II.22), Article 8.

[163] UK Foreign and Commonwealth Office, 'Guidance: Academic Technology Approval Scheme (ATAS)', 3 Mar. 2017.

[164] UK Foreign and Commonwealth Office (note 163).

[165] UK Foreign and Commonwealth Office (note 163).

[166] Legifrance, 'Décret no. 2011-1425 du 2 novembre 2011 portant application de l'article 413–7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation'[Decree no. 2011-1425 of 2 November 2011 applying articles 413–17 of the penal code with reference to the protection of the scientific and technical potential of the country].

[167] Legifrance (note 166), Article 1; and Legifrance, 'Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation' [Order of 3 July 2012 referring to the protection of the scientific and technical potential of the country].

[168] Government of Sweden, 'Government communication 2015/16, 114: Strategic Export Control in 2015, Military Equipment and Dual-Use Items', 17 Mar. 2016.

[169] Government of Sweden (note 168).

[170] Recht, Nl, 'Parket bij de Hoge Raad, 14-12-2012 / 11/03521' [Parquet at the Supreme Court, 14 Dec. 2012 / 11/03521], 5 May 2017.

national authority has recognized, however, that the transfer of knowledge that may occur through education, scientific cooperation or company visits is a form of ITT that could pose risks of proliferation. A policy to fully address this risk is currently in development.[171]

Steps could be taken to develop an agreed EU-wide policy in the field of visa screening but the development of such a policy would face specific challenges. In particular, existing screening standards for short-term visas within the Schengen area do not take account of WMD proliferation concerns but mainly address 'the risks of illegal immigration, terrorism and crime'.[172] In addition, 'long-term visas are an exclusive national competence in all EU member states, irrespective of their adherence to Schengen'.[173]

Publishing scientific research

As noted above, transfers of technology—and particularly technical data—can occur through the publication and dissemination of sensitive scientific research. Scientific publications can therefore also be subject to export controls within the EU. This issue is particularly contentious in the EU since academic freedom is enshrined as a core value in Article 13 of the EU's Charter of Fundamental Rights.[174] At the same time, however, the fundamental right of people to security and to be protected by their governments can also be used as a legal argument for interpreting this article in a more restrictive way. A key challenge in this area is to determine when the decontrol note on 'basic scientific research' and 'information available in the public domain' applies. The Dual-use Regulation does not provide any additional clarification on the application of the decontrol note. EU member states have therefore developed their own interpretations of and approaches to the issue.

At the national level, different practices appear to have developed with regard to how export control measures apply to the publication of scientific research of dual-use concern. This became a central issue in disputes in the Netherlands between 2012 and 2015 over the publication of research on influenza A by Dr Ron Fouchier of Erasmus University.[175] On the basis that the planned publication demonstrated how a strain of avian influenza can be adapted to be transmissible to mammals, the Dutch licensing authority required Fouchier to apply for a licence before publication. Fouchier applied for and received an export licence but he and Erasmus University went on to twice challenge the legality of the original requirement to apply for a licence on the grounds that the content of the publication was 'basic scientific research' and all the information it contained was already 'in the public domain'.[176] In the first ruling the court upheld the decision of the Dutch Government to impose a licence requirement and found that the exemptions contained in the EU Dual-use Regulation did not apply.[177] The second ruling found that Erasmus University had no standing in the case, since it had been granted a licence and was therefore not negatively affected by the government's decision to impose a licensing requirement.[178]

[171] Sprangers, J., Directorate-General for International Trade Policy and Economic Governance, Netherlands Ministry of Foreign Affairs, Intervention at the SIPRI workshop on 'Controlling Intangible Transfers of Technology (ITT): Mapping Key Challenges and Good Practices and Identifying Areas of Improvement', Stockholm, 1–2 Feb. 2018.

[172] Rebolledo (note 23), p. 11.

[173] Rebolledo (note 23), p. 11; see also European Commission, Home Affairs and Migration, 'Schengen Area'.

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

[175] Enserink, M., 'Dutch appeals court dodges decision on hotly debated H5N1 papers', *Science*, 16 July 2015.

[176] Charatsis, C., 'Dual-use research and trade controls: Opportunities and controversies', *Strategic Trade Review*, vol.3, no. 4 (spring 2017), p. 70.

[177] Court of North Holland, G. A. van der Veen vs the Minister for Foreign Trade and Development Cooperation, Case no. AWB 13/792, 20 Sep. 2013 (in Dutch).

[178] Amsterdam Court of Appeal, [Judgment of the multiple customs chamber on the appeal against the decision in case AWB 13/792 of the District Court of North Holland], 15 July 2015 (in Dutch).

To date no similar cases have been publicly documented, either in the Netherlands or elsewhere in the EU. It is therefore difficult to accurately map and assess national approaches in this area, or to determine how widely the approach of requiring a researcher to apply for an export licence before publishing sensitive research is applied in different EU member states. However, there is anecdotal evidence that thinking on this issue differs. In particular, a number of EU member states appear to place greater emphasis on controlling the publication of sensitive scientific research through processes of self-regulation within a university or research institute rather than through export control regulations. For example, in Flanders, Belgium, researchers have an obligation to report to an ethics committee or dual-use contact point, which issues opinions on the feasibility of certain projects and the publication of research results.[179] At the very least, there appears to be a great deal of uncertainty within academia in different EU member states about if and when export controls apply in this area.[180]

One option put forward as a way of addressing the issue is the development and application of the concept of 'export-controlled research' or 'dual-use research'. Such a concept might cover 'scientific and technological activities involving items, technologies, and processes restricted under relevant trade control law'.[181] According to this definition, export controlled research 'concerns primarily civil research activities that are considered as integral to the design, construction, use, and delivery of Weapons of Mass Destruction and in some instances of conventional weapons'.[182] Another concept that is already in use and has been discussed as a potentially useful parameter for applying the decontrol note is that of technology readiness levels (TRLs). TRLs were introduced by NASA and have been adopted within the framework of Horizon 2020. They 'are a type of measurement system used to assess the maturity level of a particular technology'.[183]

Key challenges in implementing and complying with controls

Controls on transfers of technology and software—and particularly controls on ITT—are frequently presented as posing a particularly significant challenge from both an enforcement- and a compliance-related perspective. As one export licensing official noted in 2003, controls on ITT present 'significant challenges to export controls traditionally based on national boundaries' and require 'unique policies and practices for effective administration and enforcement'.[184] The intangible nature of such technologies, the transfer of which does not require the physical crossing of any border, challenges the traditional structure of export control measures. This is particularly the case with regard to transfers of technical assistance and knowledge, since the implementation of effective controls may require placing restrictions on the movement of people that go beyond the scope of any export control regime. That said, many of the challenges that are frequently highlighted are relevant for technology and software controls in general, as opposed to ITT controls in particular. In addition, others are

[179] Thomas, B., Export Compliance Manager, IMEC, Intervention at SIPRI workshop on 'Controlling Intangible Transfers of Technology (ITT): Mapping Key Challenges and Good Practices and Identifying Areas of Improvement', Stockholm, 1–2 Feb, 2018.

[180] Thomas (note 179).

[181] Charatsis, C., 'Interferences between non-proliferation and science: "exporting" dual-use know-how and technology in conformity with security imperatives', Doctoral Thesis, University of Liège and Joint Research Centre of the European Commission, 16 June 2016, p. 237.

[182] Charatsis (note 181), p. 237.

[183] NASA, 'Technology readiness levels'; and European Commission, 'Horizon 2020: Work programme 2016–2017, General Annexes', p. 29.

[184] Clinton, T., Export Policy Analyst, US Department of Commerce, 'Intangible Technology Transfer and Catch-All Controls', Presentation, 18 June 2003.

of a more general concern for export controls in general, as opposed to software and technology controls in particular.

National authorities

One particularly challenging aspect of software, technology and—especially—ITT controls for licensing and enforcement personnel is detecting illicit transfers. Although the identification of illicit tangible transfers also presents significant obstacles, the challenges are to a certain extent greater for ITT through electronic means. The challenges are greater still when it comes to detecting illicit in-person transfers of knowledge and technical assistance. To track and control these transfers would entail the investment of additional resources in investigations, auditing processes and outreach activities.[185] Moreover, carrying out audit checks in order to determine whether unauthorized transfers have taken place is particularly challenging in the field of ITT and even more so for in-person transfers of knowledge and technical assistance. The conditions of a licence may require a company to keep internal records of any transfers that have taken place, but it could be difficult to determine whether records have been falsified. This is particularly true when it comes to verifying whether the required controls on how data is stored and shared in cloud computing services are being implemented. In the Netherlands customs authorities have voiced concerns about the ability to carry out effective compliance checks. They can demand high levels of security for data but it is unclear how customs would be able to check that they are being complied with or detect cases where a company is generating false data.[186]

As a result, good compliance procedures within the companies that produce or have access to controlled dual-use goods and technologies are essential to identifying and preventing illegal transfers. At the same time, engagement with the private sector is proving increasingly problematic, not least because of the expanding range of items and activities subject to control, and increases in the number and types of actor involved in the dual-use supply chain—due to technological developments as much as the design and expansion of EU and UN sanctions. Thus, today's exporters of technology and software are not only companies, but also academics and the so-called do-it-yourself communities. In some cases academia has proved fairly unresponsive to outreach initiatives and reluctant to actively engage with such activities.[187] The same applies in cases where national governments have tried to reach out to do-it-yourself communities in the field of bio-research.[188] In addition, the positive and long-term results of outreach to academia have also been challenged by the frequent turnover of management staff in the targeted institutions, with the consequent 'loss' of referent interlocutors for the authority.[189]

Furthermore, national authorities may find it difficult to keep up with the pace of technological developments that are making the sharing of sensitive knowledge increasingly easy. Significant attention has been paid to cloud computing but this masks deeper and more profound changes in the speed with which companies are developing new methods of sharing information that are increasingly hard to under-

[185] Bauer S., 'Improvement of EU dual-use export controls in the context of the European Commission's reform proposal', eds S. Bauer and I. J. Stewart, *Workshop: Dual Use Export Controls* (European Parliament, Directorate General for External Policies of the European Parliament: Brussels, Oct. 2015), p. 58.

[186] Sprangers (note 138).

[187] Bauer et al. (note 131), pp. 27–30.

[188] French Government official, Intervention at SIPRI workshop on 'Controlling Intangible Transfers of Technology (ITT): Mapping Key Challenges and Good Practices and Identifying Areas of Improvement', Stockholm, 1–2 Feb. 2018.

[189] Stefan, L., Ministry for National Economy, Hungary, Intervention at SIPRI workshop on 'Controlling Intangible Transfers of Technology (ITT): Mapping Key Challenges and Good Practices and Identifying Areas of Improvement', Stockholm, 1–2 Feb. 2018.

stand, track and police. As one official noted, there is a lot of focus on cloud computing at the moment but equally challenging issues are raised by the increased use of email and other methods of sharing data electronically.[190] Finally, the simple fact that controls on the movement of people, which could still pose proliferation concerns, fall under the competence of different authorities suggests that a proportion of these transfers may not be controlled at all. As mentioned above, there are cases in which this gap has been filled through targeted visa screenings. However, the application of these controls is highly dependent on effective cooperation between the different national authorities involved.[191]

Companies

A key challenge for companies seeking to comply with software, technology and—especially—ITT controls is that of having a system in place that effectively keeps track of all the cases in which transfers occur. There are software packages available that can help companies to achieve this goal but these cannot necessarily act as an effective substitute for well-functioning routines. Some software is better able than others to keep track of the information that must be collected in order to be in compliance with record-keeping requirements.[192] However, the main issue remains ensuring that all of the company personnel who are potentially involved in transfers of controlled items understand their obligations to comply with export controls, which can prove a difficult goal to achieve, especially in the case of ITT.[193] This is particularly true in large multinational companies where controlled technology may be passed between company branches, and to customers or suppliers in different countries. The need to verify export classifications, authorizations and destinations, as well as recipients, makes the tracking of each of these transfers a complex process that can ultimately affect a company's attempts to win contracts or reduce supply chain costs.[194] In addition, companies must also keep track of individuals with knowledge of controlled technology, which can be even more challenging. This is why, in addition to defining procedures for storing and securing technical data and keeping records of every transfer, a fundamental part of compliance involves properly training company staff. This is particularly important not only when personnel travel abroad, but increasingly also to ensure the responsible use of marketing tools, promotional material and even social media.[195]

Complying with different national control mechanisms, even within the EU, is also an issue, particularly for companies that operate in several different states. This emerges clearly in the case of companies that make use of cloud computing services and whose technology or software is subject to dual-use export controls. In this regard, given the lack of clarity and consistency on how controls should operate, companies have been advised to take a precautionary approach and seek assurances from their service providers about the location of the servers they are using and even the nationality of the staff they employ. In particular, it has been recommended that companies should,

> conduct due diligence of cloud service providers and consider negotiating terms into contracts providing for restrictions on: the locations through which controlled software or technology may be routed; where it may be stored; how access by any unauthorized person (including system

[190] Sprangers (note 138).
[191] Stefan (note 189).
[192] Gallacher (note 136).
[193] Gallacher (note 136).
[194] Bromley, M. and Bauer, S., 'The Dual-Use Export Control Policy Review: Balancing security, trade and academic freedom in a changing world', EU Non-Proliferation Paper no. 48 (SIPRI: Stockholm, Mar. 2016), p. 10.
[195] Rosanelli, R., AIM Norway, Intervention at SIPRI workshop on 'Controlling Intangible Transfers of Technology (ITT): Mapping Key Challenges and Good Practices and Identifying Areas of Improvement', Stockholm, 1–2 Feb. 2018.

administrators) will be prevented; the right to audit the provider's compliance; and obligations for providers to notify promptly any known or suspected breaches.[196]

However, companies that provide cloud computing services are often unable or unwilling to provide such assurances. As one company representative has noted 'most cloud service providers will not take responsibility for the export control compliance of the data entrusted to their clouds; they force the user to be responsible for control and management'.[197]

Complying with US re-export controls is also a particular challenge for both companies and research institutes. In particular, controls on 'deemed re-exports' mean that companies and research institutes in the EU that have purchased or obtained dual-use items or military goods of US-origin may be required to keep track of the nationality of their employees, students and sub-contractors in order ensure that they are in compliance. The fact that US partners normally export to EU companies and/or research institutes using 'licence exceptions' makes it difficult for the recipients to comply with these re-export regulations since the imported technology is not necessarily labelled as an export-controlled item.[198] Companies in the defence and aerospace sector are more likely to be affected by US controls on re-exports.[199] 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, as mentioned above, 'deemed exports', such as the release of technology or source code.[200] In order to comply with these controls, additional screening and protective measures are necessary to prevent visual access to sensitive material by third parties.[201] Compliance with US re-export controls may also mean paying particular attention to avoiding the transfer, or the transportation through physical means (such as laptop computers), of controlled technical data during international business travel.[202] In this regard, using software tagging keywords to trace emails containing controlled data can be a useful tool for ensuring that technical data cannot be accessed while travelling.[203]

Academia and research institutions

When it comes to complying with controls on transfers of software, technology and ITT, most of the challenges highlighted for companies also apply to research bodies and academia. However, these actors face an additional set of compliance-related challenges, although many of these relate to export controls more generally. Some of these challenges relate to the fact that research and academia are built around a culture that values the free exchange of knowledge and ideas, and seeks to foster international collaboration. This obviously presents an additional set of issues. A number of efforts are currently focused on ensuring open access to scientific publications and data as a principle of conduct to guarantee the highest level of research integrity.[204] In this context, convincing researchers of the need to comply with export control requirements that may involve seeking permission to present their work at a seminar or checking the nationality of their potential project partners may be a difficult process.

[196] Tauwhare (note 10); and Braverman and Wong (note 15).
[197] Rolls-Royce (note 13).
[198] Thomas (note 124). A Licence Exception is an authorization that allows the export or re-export under certain conditions of items subject to Export Administration Regulations (EAR) that would otherwise require a licence.
[199] Rosanelli (note 195).
[200] Bauer et al. (note 131), p. 13.
[201] Rosanelli (note 195).
[202] Rosanelli (note 195).
[203] Rosanelli (note 195).
[204] European Federation of Academies of Sciences and Humanities (ALLEA), 'The European Code of Conduct for Research Integrity', Revised edn Mar. 2017, Berlin.

A second set of challenges relates to the low level of awareness about export controls within sections of research and academia. As highlighted above, academic and research institutions within the EU may be subject to export control legal obligations not only when transferring physical items, but also when disseminating sensitive scientific knowledge. Very few scientists, however, are sufficiently aware of or trained in export control- and compliance-related matters. In some cases, even when researchers are well informed, it may be difficult to apply export control regulations correctly. For example, there will often be some information that it is impossible to provide at the time a researcher is applying for an export licence. This is often true with regard to both the value of the technology to be exported and its end-use, since its deployment could potentially be multipurpose.[205] Another difficulty, according to representatives from the sector, is how to interpret correctly the decontrol note on basic scientific research. Although both national laws protecting academic freedom and the various control lists contain language that exempts certain types of academic research from export controls, these provisions have proved difficult to interpret.[206] There have been divergent court rulings in EU member states and the USA on how these concepts should be applied.[207]

Some governments have sought to fill this void by issuing specific guidance material or undertaking outreach and awareness raising programmes. BAFA published such guidance in 2005.[208] The UK has also issued specific guidance on export control legislation for academics and researchers.[209] Nonetheless, the very nature and internal structures of this sector, which are very different from, for instance, what would be found in a private sector company, can also present challenges in terms of trade compliance. It has been highlighted that, in this context, it may be difficult to source higher education-specific guidance from experts and to interpret concepts such as 'goods' and 'exports' in ways that are meaningful to academic researchers.[210] Furthermore, the latter seem in many cases to lack awareness of their responsibility to assess the potential risks associated with their research.[211] Nonetheless, some representatives of the academic and research sectors have taken the initiative to tackle these challenges by issuing guidance materials and codes of conduct to their research staff.[212] These documents pursue various paths, such us explaining when an export licence is required or providing details of the applicable legislation with case studies.[213] In certain cases, guidance material has been issued which covers both compliance with dual-use and arms export controls and broader issues relating to the need to guard against the potential misuse of research for unethical or illegal purposes.[214]

[205] Thomas (note 124).

[206] Bauer et al. (note 131).

[207] Bauer et al. (note 131).

[208] 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', Aug. 2005.

[209] UK Department for Business Innovation and Skills, Export Control Organisation, 'Guidance on export control legislation for academics and researchers in the UK' (Mar. 2010).

[210] Bauer et al. (note 131).

[211] Bauer et al. (note 131).

[212] Bauer et al. (note 131).

[213] Bauer et al. (note 131).

[214] See Ghent University et al., 'Guidelines for researchers on dual use and misuse of research', Oct. 2017.

6. Conclusions and recommendations

Enhancing the effectiveness of export control measures on tangible and intangible transfers of software and technology can be achieved in many ways. Relevant efforts in this direction can be made on the regulatory as well as the compliance side. These include, for example, providing more clarity in terms of definitions and applicable controls. In addition, as these types of transfer affect a wide and varied range of sectors and actors, outreach activities should be tailored to specific features and needs. Controls could also be improved by building links between export control tools and other means through which governments can better monitor and regulate certain types of transfers of software and technology, such as visa screening and regulations on foreign acquisitions. These efforts could be complemented by equally significant endeavours on the compliance side, such as the promotion of training or awareness raising, and the establishment of improved internal compliance programmes that are better able to manage issues relating to transfers of intangible technology. The conclusions and recommendations set out below focus on three levels: the multilateral export control regimes, including the EU Dual-use Regulation and its ongoing review; national governments, particularly EU member states; and companies and research institutes.

The multilateral export control regimes

- *Clarification of key terms*: There is currently no clarity either in the export control regimes or at the EU level on what is meant by several key terms that have a direct impact on the way controls on transfers of software and technology, and ITT are applied at the national level. These include, for example, 'intangible transfers of technology', 'public domain' and 'basic scientific research'. This leads to differences in the way software, technology and activities are made subject to controls, and the way controls are applied. A common agreement on the interpretation of these terms should be sought within the framework of the multilateral export control regimes. In the meantime, the recast of the Dual-use Regulation could be used to generate language that aims to bring clarity to some of these points, while also creating mechanisms for drafting guidelines to address others. In each case, it will be important to ensure that the process of drafting these definitions and guidelines is as open and inclusive as possible and takes account of the views of all the affected sectors and actors.
- *Develop better harmonized approaches to controls among EU member states*: There is significant scope to build on the recast of the Dual-use Regulation in order to explore the steps that could be taken to develop better harmonized approaches among EU member states to controls on transfers of software and technology, and ITT. This could begin with an analysis of how EU member states define and apply key concepts in this area. This mapping of national practices could also cover the penalties associated with violations of controls, and outreach and awareness raising strategies and approaches, as well as national practices with regard to the issuing of licences for transfers of software, technology and ITT, and relevant enforcement activities.

- *Produce detailed guidelines on how controls should apply to cloud computing*: One key demand from industry—particularly from companies that operate in several locations—is for more standardized practices in terms of how export controls should apply to cloud computing. This could potentially involve introducing clear standards on whether controls take account of the location of the servers and what measures companies are required to take to ensure that data is being safely stored and protected. The analysis in this paper indicates that reaching an agreement on these points would require a level of detail that has not been achieved to date in the best practice documents created by the different regimes. However, if it can be done, it seems likely that the EU would provide the best avenue for achieving success.
- *Provide clarification on the application of the decontrol note on basic scientific research*: The decontrol note attached to the Wassenaar Arrangement and other export control regimes does not clarify what constitutes fundamental research of dual-use concern. Development of the concept of 'export-controlled research' or 'dual-use research' may be helpful in this regard. In addition, further thought should be given to whether and how the concept of TRLs might be used as guidance when determining how the decontrol note should be applied. At the same time, there is also a need for a coordinated and harmonized approach so that the discussions that take place on these issues within different export control regimes are joined up and do not run in parallel.

National governments

- *Adopt a layered approach to controlling intangible transfers*: As highlighted in this paper, export controls are only one means through which restrictions can be placed on the transfer of sensitive intangible goods. Other mechanisms include controls on who is able to study particular courses or which companies can make foreign acquisitions. Moreover, research institutes—particularly in the bio-sciences—have developed mechanisms for self-regulation that seek to ensure that the research they carry out does not have unintended consequences or lead to serious harm. At the national level, governments should seek to map the different tools that are being deployed—and those which could be deployed—in order to avoid both gaps and unnecessary duplication of effort.
- *Facilitate communication and exchange among the relevant competent authorities*: To ensure that the layered approach works effectively, national governments should maintain effective communication between the different authorities involved and exchange useful information with their counterparts in partner countries. For example, this would involve maintaining effective lines of communication between the authorities responsible for issuing visas to foreign students and those responsible for issuing export licences. These exchanges would be useful for identifying potential cases of concern that could, in turn, be shared with like-minded states.
- *Enhance 'consular vigilance'*: To enable better controls on transfers of technical assistance and knowledge, the EU should consider making

the proliferation of WMD one of the risks to take into account when granting a Schengen visa. Overall risk assessment should also be based on information such as nationality (in cases where the country of origin is hosting programmes of concern) and business links. All EU member states, including those not in the Schengen Area, should be encouraged to take the same steps. The legal grounds for introducing these further elements of control could be drawn from the 2008 New Lines of Action by the European Union in combating the proliferation of WMD and their delivery systems.

- *Develop targeted compliance-related guidance material*: As noted above, controls on transfers of software and technology, and ITT have been included in a number of guidance documents produced by national governments. Nonetheless, there is a need for more targeted material to help particular sectors and actors affected by arms and dual-use export controls implement this particularly difficult aspect of such controls. This guidance should, for example, specify when technology is controlled and how this is reflected in both licensing and compliance requirements, such as on the level of IT security required to store sensitive data. These requirements should be formulated in a way that ensures some degree of proportionality based on the issue they seek to tackle (e.g. export of dual-use technology, export of military technology, etc.). One particular gap that has been frequently highlighted is the need for better guidance for research and academia on how to apply ITT controls. Such guidance should also address licensing requirements, for example in the context of scientific cooperation with foreign partners.
- *Implement existing enforcement tools effectively*: Although enforcing controls on ITT could represent a challenge for all the reasons outlined above, there are some feasible measures that could be adopted to facilitate the work of the competent authorities. Following an initial suspicion concerning the violation of export control regulations, investigative and enforcement agencies could make use of the large variety of instruments which they already have to conduct checks on transfers occurring via phone, fax or email. Evidence of possible violations through electronic transfers would include business documents, internal communications and financial transactions.[215] This is also the case for illicit transfers of know-how through technical assistance. Although the knowledge that scientists, engineers and designers could transfer while travelling abroad is difficult to control, it is not uncommon for tangible—and therefore trackable—sources of information to be brought along to support an individual's know-how.[216]
- *Consider ways to restructure outreach efforts*: Currently, outreach and assistance efforts are generally targeted by sector, and research institutes and academia are treated separately from private companies. However, the challenges that research centres face are far more similar to those of a company than a university, not least due to their frequent cooperation

[215] Pietsch, G., German Federal Office for Economic Affairs and Export Control (BAFA), 'The control of intangible transfers of software and technology via the internet', Presentation, Dec. 2017.

[216] Pietsch G., German Federal Office for Economic Affairs and Export Control (BAFA), 'A changing environment of controlling ITT for licensing and enforcement authorities', Presentation, 13 June 2013.

with the private sector.[217] There may therefore be value in restructuring outreach efforts to target stakeholders that are dealing with particular types of controlled software and technology.

Companies and research institutes

- *Integrate ITT controls into ICPs*: Academia and research institutions can take many steps to effectively comply with controls on the transfer of controlled knowledge and technical assistance. Most of these measures can be covered by an ICP that tackles ITT and outlines clearly the obligations of all relevant employees. In addition, an important role in ensuring effective compliance with ITT controls can be played by the production of internal guidance material addressed to those issues of most concern in a research context, such as check-lists before leaving on a business trip and the steps to be followed when publishing sensitive findings.
- *Combine export control guidance material with information aimed at avoiding the misuse of research*: The importance of developing guidance material that can help researchers to avoid situations in which their research could be misused has already been recognized in the life sciences.[218] In addition, as noted above, steps have been taken to combine this kind of material with guidance that is focused on compliance with dual-use and arms export controls.[219] Such guidance can provide criteria on how to assess the dual-use potential of research and its outputs while also offering practical advice on how to implement existing regulations instead of imposing new ones. This type of approach could serve as a model for other guidance documents. In particular, by combining the two issues, the material can effectively underline the areas where the requirements related to complying with export controls overlap with or diverge from the steps that need to be taken to avoid the misuse of research. This will give researchers a clearer sense of their obligations and a deeper understanding of how these two goals can complement and reinforce each other.

[217] Thomas (note 124).

[218] Meier, O., 'Dual-use technology transfers: Finding the right balance between control and cooperation', ed. O. Meier, *Technology Transfers and Non-proliferation: Between Control and Cooperation* (Routledge: London, 2014), pp. 255–57.

[219] See Ghent University et al. (note 214).

About the authors

Mark Bromley (United Kingdom) is the Director of the SIPRI Dual-use and Arms Trade Control Programme. His areas of research include the dual-use and arms export control policies of EU member states; combating the illicit trade in small arms and light weapons; the Arms Trade Treaty; and controls on the trade in cyber-surveillance systems.

Giovanna Maletta (Italy) is a Research Assistant in the SIPRI Dual-use and Arms Trade Control Programme. Her research on export control covers compliance and enforcement issues with a particular focus on the dual-use and arms export control policies of EU member states. Her work also involves activities related to SIPRI's participation in the EU Non-proliferation and Disarmament Consortium.

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