sipri

INTANGIBLE TRANSFERS OF TECHNOLOGY AND SOFTWARE

Challenges for the Missile Technology Control Regime

LAURIANE HÉAU AND KOLJA BROCKMANN

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

INTANGIBLE TRANSFERS OF TECHNOLOGY AND SOFTWARE

Challenges for the Missile Technology Control Regime

LAURIANE HÉAU AND KOLJA BROCKMANN

April 2024

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

DOI No: 10.55163/HLWP1722

Contents

Acknowledgements

The authors would like to thank the German Federal Foreign Office for its generous funding, which enabled the production of this report as part of the research project 'Quo vadis MTCR II: Mapping and mitigating the potential impact of the NewSpace industry on missile technology proliferation'. They would also like to thank the officials and non-governmental experts that took part in background interviews and exchanges as part of the preparation of this report. The information contained in this report builds on previous work conducted by SIPRI on the multilateral export control regimes, intangible transfers of technology and NewSpace—including by Mark Bromley, Giovanna Maletta and Nivedita Raju—and the authors greatly benefited from their input on draft versions of the paper. The authors would also like to thank their other SIPRI colleagues and two external reviewers for their detailed comments on a previous version of the report. Finally, the authors would like to thank the SIPRI Editorial Department for its excellent work.

Summary

The Missile Technology Control Regime (MTCR) defines guidelines for controls on transfers of missiles, space launch vehicles (SLVs) and other uncrewed delivery systems, on their physical parts and components, but also on associated technical data and knowledge (collectively referred to as 'technology') and software. In many cases, technology and software transfers occur through intangible means, such as electronic transfers or oral communication. Controlling these intangible transfers of technology (ITT) and software is a known challenge, but the global growth of the NewSpace industry and advances in emerging technologies make it particularly important for MTCR partners to continue to address this topic.

The controls outlined by the MTCR in its guidelines and annex cover transfers of technology that are directly associated with any goods controlled in the MTCR control list. Technology encompasses both technical data (such as blueprints, plans, diagrams) and technical assistance (such as instruction, skills, training). The MTCR annex also outlines controls over the transfer of software, defined as a 'collection of one or more "programs", or "microprograms", fixed in any tangible medium of expression'. Exemptions are in place for basic scientific research and for technology and software already in the public domain. In 2003, the MTCR also added a catch-all clause to its guidelines, which allows a state to impose controls on a (tangible or intangible) transfer of unlisted items—goods, technology or software not captured by the control list in certain circumstances, including if 'the items may be intended, in their entirety or part, for use in connection with delivery systems for weapons of mass destruction'.

To contribute to building knowledge on the ways that unauthorized ITT and software transfers can occur and on the challenges this poses, the paper explores four cases of export control violations and cases where the risk of a possible violation was identified involving missile-related ITT or software. Each case study outlines the type of export control violation or risk of violation, as well as the type of missile-related ITT or software involved in the case; the detection, enforcement and/or prosecution efforts; and the relevance of each case to the MTCR. The case studies present some of the scenarios whereby an exporter can violate export control regulations by transferring or making available technology or software using intangible means. However, to increase understanding on the broader range of export control violations, the paper also develops a typology of violations involving missile-related ITT or software and identifies associated compliance challenges.

Key challenges emerge from the typology and the analysis of case studies. The increasing reliance on ITT and software by companies in the aerospace and NewSpace sectors and their global supply chains presents one such challenge. Digital transfers of technology and software, including through cloud-based servers, have also become easier and as a result more common. Despite this, many companies, especially recently established NewSpace and emerging technologies start-ups, lack detailed awareness of ITT and software controls or effective methods of ensuring compliance with such controls. Compliance is also a challenge among research institutes and especially in academia, where research is being undertaken in fields that are highly relevant to missile development. Actors actively seeking to acquire technology and software to advance their missile programmes can take advantage of this. They could also exploit the increasing trend for foreign direct investment (FDI) to access technology by gaining control of or ownership rights over a company.

As states continue to encounter a range of challenges in their attempts to enforce ITT and software controls, the MTCR has an important role to play in addressing these challenges. In this respect, the MTCR partners should develop—or if it already exists

publish—guidance on ITT and software controls and should strengthen awareness and compliance with such controls among the aerospace industry as well as research and academia. They should further enhance information-sharing on cases of violations of ITT and software controls as appropriate within the licensing and enforcement experts meeting, the technical experts meeting, and the joint meeting of the two with the information exchange meeting. MTCR partners should also strengthen discussions on ITT challenges with adherents and non-partners, as well as with the other regimes. Finally, the MTCR should explore linkages with complementary tools including visa screening, FDI screening and technology safeguards agreements to more effectively address the MTCR's objectives and strengthen the implementation of ITT and software controls.

Abbreviations

AECA	Arms Export Control Act
ATAS	Academic technology approval scheme
CBN	Chemical, biological and nuclear (weapons)
CFIUS	Committee on Foreign Investment of the United States
CIFER	Comprehensive identification from frequency responses
EU	European Union
FDI	Foreign direct investment
G7	Group of Seven
IEM	Information exchange meeting
ITT	Intangible transfers of technology
LEEM	Licensing and enforcement experts meeting
MTCR	Missile Technology Control Regime
NASA	National Aeronautics and Space Administration
POC	Point of contact
RPOC	Reinforced point of contact
SLV	Space launch vehicle
TEM	Technical experts meeting
TOM	Technical outreach meeting
TRL	Technology readiness levels
UAV	Uncrewed aerial vehicle
WMD	Weapons of mass destruction

1. Introduction

The Missile Technology Control Regime (MTCR) seeks to prevent the proliferation of missiles and other uncrewed delivery systems capable of delivering weapons of mass destruction (WMD). Since its creation in 1987, the MTCR has become the main multilateral instrument for setting standards on missile-related export controls, which states then implement at the national level (see box 1.1). The MTCR defines guidelines for controls on transfers of missiles, space launch vehicles (SLVs) and other uncrewed delivery systems, on their physical parts and components, but also on associated technical data and knowledge (collectively referred to as 'technology') and software. Technology and software can be transferred by tangible, that is, physical means. A USB stick taken abroad, for example, can contain controlled technical data such as a technical drawing. However, technology and software can also be transferred through intangible means. These intangible transfers of technology (ITT) and software use 'non-physical' means, such as electronic transfers or oral communication.

For the actors involved in the implementation of MTCR controls, applying controls to ITT and software effectively is a widely recognized challenge. The companies and research institutes that must comply with the controls often struggle to track all of the actual or potential intangible transfers that their activities involve. Enforcement is also more challenging for national authorities and requires alternative control measures, as intangible items do not go through customs checkpoints and cannot be inspected before they reach their destination. In addition, the challenges of ITT and software controls are exacerbated by significant differences in how states apply aspects of the controls and in the legal mechanisms their national systems provide to enforce them.

The global growth of the NewSpace industry and advances in emerging technologies make it particularly important for MTCR partners to continue to address the topic of ITT and software controls. The NewSpace industry is characterized by diverse actors, such as start-ups and innovation hubs, and by new business activities which regularly involve the use of emerging technologies. NewSpace companies rely on alternative funding models, including venture capital and foreign direct investment (FDI). These trends increase the salience of ITT and software controls and make regulatory tools complementary to traditional export controls, such as FDI screening mechanisms, increasingly relevant to and useful for addressing particular types of ITT.

While the general challenges associated with ITT and software controls have been well explored in the literature, specific challenges in the context of the MTCR have not been examined to a similar extent.[1] By focusing on intangible transfers of missile-related technology and software, this paper aims to contribute to a better understanding of the challenges in this context and to more effective export controls on intangible transfers more generally. To do so, the paper draws on a series of missile-related ITT and software case studies. Many of these cases also involve transfers of tangible items subject to controls but the focus of the case studies is on ITT or software.

Chapter 2 explores the main types of controls—and exemptions—prescribed by the MTCR on ITT and software. Chapter 3 discusses four case studies of export control violations, or where the risk of a possible violation was identified, involving missile-related ITT and software, and provides a typology of possible cases. Chapter 4 examines key challenges related to controlling missile-related ITT and software. Chapter 5 develops recommendations on how MTCR partners might more effectively address missile-related technology proliferation risks through controls on ITT and software.

[1] See e.g. Bromley, M. and Maletta, G., *The Challenge of Software and Technology Transfers to Non-Proliferation Efforts: Implementing and Complying with Export Controls* (SIPRI: Stockholm, Apr. 2018); and Brockmann, K. and Kelley, R., *The Challenge of Emerging Technologies to Non-proliferation Efforts: Controlling Additive Manufacturing and Intangible Transfers of Technology* (SIPRI: Stockholm, Apr. 2018).

Box 1.1. The Missile Technology Control Regime

The Missile Technology Control Regime (MTCR) is an informal political understanding among a group of 35 supplier states that aims to limit the proliferation of missiles and other uncrewed delivery systems capable of delivering chemical, biological or nuclear (CBN) weapons—referred to by the MTCR as weapons of mass destruction. It was established by the Group of Seven (G7) largest industrialized states in 1987, originally as an instrument to help prevent the proliferation of nuclear weapons by controlling missiles capable of delivering them. The scope of the MTCR has since expanded to include ballistic and cruise missiles capable of delivering CBN weapons. Through the MTCR, the participating states (MTCR partners) harmonize their export controls, following the MTCR Guidelines for Sensitive Missile-Relevant Transfers (MTCR guidelines) and by maintaining a control list (MTCR Equipment, Software and Technology Annex) that covers missiles and certain uncrewed aerial vehicles (UAVs) and relevant dual-use goods and technologies. The annex divides the items it covers into two categories:

Category I includes any complete missile or UAV 'capable of delivering a payload of at least 500 kg to a range of at least 300 km' (e.g. ballistic missiles, space launch vehicles, cruise missiles and reconnaissance drones); complete major subsystems (e.g. rocket stages and engines, guidance systems and re-entry vehicles); related software and technology; and specially designed production facilities. For all Category I items, the partners commit to exercising an 'unconditional strong presumption of denial', meaning that no licences for exports of such items should be issued under all but the most exceptional circumstances. The export of Category I production facilities is prohibited without exception.

Category II includes dual-use missile- and UAV-related components, and complete missile and UAV systems with a range of at least 300 km, regardless of their payload capability. Exports of such systems destined for any CBN weapon delivery end-use are also subject to a strong presumption of denial. All other exports of Category II items are subject to licensing procedures and are to be assessed with consideration of the criteria outlined in the guidelines.

The MTCR takes decisions—for example, on admitting new partners or making amendments to the annex—by consensus and these decisions are politically rather than legally binding. The main decision-making body of the MTCR is the plenary that is convened every year, usually in October, and is hosted by the annually rotating chair. The MTCR has several subsidiary bodies that cover different topical areas and operational functions: the technical experts meeting (TEM), the information exchange meeting (IEM), the licensing and enforcement experts meeting (LEEM), point of contact (POC) meetings and reinforced point of contact (RPOC) meetings.

Sources: MTCR, 'Objectives of the MTCR', [n.d.]; and MTCR, 'Frequently asked questions (FAQs)', [n.d.].

2. Controlling intangible transfers of missile-related technology and software through the MTCR

The MTCR partners have been discussing the challenges posed by ITT and software for over 20 years. Partners first 'agreed to take steps to develop national procedures to subject MTCR-controlled ITT to export controls, in accordance with their national legislation' at the 2003 MTCR plenary meeting.[2] Since then, the issue of ITT and software has been a recurring item on the agenda of MTCR meetings, in particular in the licensing and enforcement experts meeting (LEEM).[3] This chapter explores the controls outlined by the MTCR in its guidelines and annex on ITT and software; and discusses the exemptions for basic scientific research and information in the public domain, the application of catch-all controls to unlisted items and the limited guidance materials on ITT controls produced by the MTCR to date.

Intangible transfers of technology

'Technology' is defined in the MTCR as the specific information 'required for the "development", "production" or "use" of a product'. Technology can take two forms: 'technical data' or 'technical assistance'.[4] The general technology note in the MTCR annex further states that the 'transfer of "technology" directly associated with any goods controlled in the Annex is controlled according to the provisions in each Item'.[5] This means that transfers of any information that meets the definition of technology, unless otherwise specified in a control list entry, generally require a licence. However, any approval of the export of an annex item 'also authorizes the export to the same end-user of the minimum "technology" required for the installation, operation, maintenance, or repair of the item'.[6]

Technical data

Technical data is described in the MTCR annex using a list of examples: 'blueprints', 'plans', 'diagrams', 'models', 'formulae', 'engineering designs and specifications' and 'manuals and instruction written or recorded on other media or devices such as: disk, tape, read-only memories'.[7] Technical data can be tangible or intangible; that is, have a physical or non-physical form. This paper is mainly concerned with technical data that either has an inherently intangible form or is transferred by intangible means. For example, making available or providing access to technical data by intangible means, such as cloud computing, can constitute a controlled transfer if upload and download are performed in different states, even if they are performed by branches of the same company. The definitional framework for transfers of technology provides room for interpretation and is not legally binding. Differences in how relevant provisions are integrated into national legislation and translated into national practices mean that there continue to be differences in the implementation of controls on transfers of technical data by states, including among MTCR partners.

[2] MTCR, 'Plenary meeting of the Missile Technology Control Regime, Buenos Aires, Argentina, 19–26 September 2003', Press release, 26 Sep. 2003.

[3] See the references to discussions on ITT in the press releases on annual MTCR plenary meetings, 2003 to 2023, <https://www.mtcr.info/en/press-releases>. The LEEM provides a forum for partners to share experiences of and good practices on implementation of the MTCR guidelines, with a focus on national licensing processes, enforcement measures and efforts to counter illicit procurement.

[4] MTCR, 'Equipment, software and technology annex', MTCR/TEM/2023/Annex, 3 Nov. 2023, p. 13.

[5] MTCR, 'Equipment, software and technology annex' (note 4), p. 7.

[6] MTCR, 'Equipment, software and technology annex' (note 4), p. 7.

[7] MTCR, 'Equipment, software and technology annex' (note 4), p. 14.

Technical assistance

According to the MTCR annex, technical assistance can take the form of 'instruction', 'skills', 'training', 'working knowledge' or 'consulting services'.[8] Examples include academic courses and presentations at conferences or individual training or consulting services to assist with specific activities. Technical assistance therefore often means a transfer of what is commonly described as 'tacit knowledge', defined as knowledge or know-how that cannot simply be learned from a book but requires apprenticeship and practice to acquire.[9] In the context of missile programmes, a significant amount of know-how is required to successfully develop and adapt missile designs.[10] Technical assistance has generally been understood to include in-person transfers of know-how through hands-on training, instruction and the development of specialized skills. However, as means of remote teaching, digitized laboratories or workshop set-ups and more immersive communication tools become more common, there are increased possibilities for technical assistance to be provided remotely rather than in person.

Intangible transfers of software

Software is defined in the MTCR annex as a 'collection of one or more "programs", or "microprograms", fixed in any tangible medium of expression'.[11] Over the past 25 years, methods of transferring or 'making available' software have become increasingly intangible, such as through email attachments, server downloads and uploads, and cloud computing services.[12] This often means sharing access to software with foreign customers or between different branches of the same company or research institution. The MTCR annex limits the application of controls on transfers of software through a 'General Software Note' and a 'General Minimum Software Note'.[13] The former stipulates that software '[g]enerally available to the public' or 'in the public domain' (see below) is exempt from controls, while the latter stipulates that 'the minimum "software" . . . required for installation, operation, maintenance or repair' of a controlled item is also exempt. The design and testing of missiles are greatly facilitated by specialized software, use of which has become the norm in the industry.[14] However, the development of specialized design or testing software, for example to run or analyse hypersonic wind tunnel tests, still presents technological barriers to states seeking to start a missile programme. Controls on such software are therefore particularly important.[15]

The 'basic scientific research' and 'in the public domain' exemptions

Mirroring the provisions in the Wassenaar Arrangement, the MTCR annex provides two main exemptions from the provisions of the general technology note. These are particularly relevant in the context of ITT. First, basic scientific research, defined as 'experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed

[8] MTCR, 'Equipment, software and technology annex' (note 4), pp. 13–14.

[9] See e.g. Polanyi, M., *Personal Knowledge: Towards a Post-critical Philosophy* (University of Chicago Press: Chicago, 2015); 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), pp. 44–99.

[10] Brockmann and Kelley (note 1), p. 28.

[11] MTCR, 'Equipment, software and technology annex' (note 4), p. 13.

[12] Bromley and Maletta (note 1), p. 5.

[13] MTCR, 'Equipment, software and technology annex' (note 4), pp. 7–8.

[14] See e.g. Category II, Item 16, 'Modelling and design software' in US Government, *Missile Technology Control Regime (MTCR) Annex Handbook 2017* (MTCR: 2017), p. 202.

[15] Brockmann, K. and Stefanovich, D., *Hypersonic Boost-glide Systems and Hypersonic Cruise Missiles: Challenges for the Missile Technology Control Regime* (SIPRI: Stockholm, Apr. 2022), p. 19.

towards a specific practical aim or objective', is exempt from controls.[16] Second, software or technology is also exempt if it is already 'in the public domain', meaning that it 'has been made available without restrictions upon its further dissemination'.[17] Both exemptions are highly relevant in the context of generating and disseminating knowledge, particularly in the research and academic sectors. This is especially important in emerging and high-technology fields, such as hypersonic missile technology, where much of the scientific research may appear fundamental in nature, but is conducted with specific applications in mind.[18]

Catch-all controls

Catch-all controls allow a state to impose a licensing requirement on a (tangible or intangible) transfer of unlisted items—goods, technology or software not captured by the control list—in certain circumstances. The MTCR added a catch-all clause to its guidelines in 2003, which the partners implement as part of their national control systems.[19] A state can impose licensing requirements by informing the exporter 'that the items may be intended, in their entirety or part, for use in connection with delivery systems for weapons of mass destruction other than manned aircraft'.[20] However, due to the difficulty of detecting transfers, and intangible transfers in particular, states are usually reliant on information provided by their intelligence services to either anticipate future transfers or be aware of past transfers so they can interject and impose a licensing requirement. Catch-all controls can also apply if an exporter is 'aware that non-listed items are intended to contribute to such activities, in their entirety or part'. This awareness creates an obligation to notify national authorities, which can then decide whether to impose a licensing requirement.[21] In the context of the MTCR, actors such as universities and research centres with aerospace engineering schools, and NewSpace and emerging technology start-up companies, which often lack effective compliance programmes, could be targeted by foreign entities attempting to acquire non-listed items or items that are just below the thresholds provided in the annex.[22]

MTCR guidance and resources on ITT and software controls

There is currently only very limited guidance available on ITT and software controls. Other than the MTCR Annex Handbook, which provides brief explanations on the individual items in the MTCR annex, the MTCR has not issued any public guidance materials.[23] However, the partners maintain and regularly update the MTCR Enforcement Handbook, a key resource which is not public but shared only among the licensing and enforcement officers of MTCR partners. The Enforcement handbook provides 'an overview of export controls relating to the MTCR, indicators to identify suspect permit applications and suspect exports, as well as intelligence indicators and information to increase enforcement staff's abilities to target shipments suspected of being intended for use in delivery systems for WMD'.[24]

[16] MTCR, 'Equipment, software and technology annex' (note 4), p. 9.
[17] MTCR, 'Equipment, software and technology annex' (note 4), p. 9.
[18] Scott, E. et al., *Catalogue of Case Studies on Intangible Technology Transfers from Universities and Research Institutes* (King's College Centre for Science & Security Studies: London, Sep. 2020), pp. 47–50.
[19] See question 12, MTCR, 'Frequently asked questions (FAQs)', [n.d.].
[20] MTCR, 'Guidelines for sensitive missile-relevant transfers', [n.d.], para. 7.A.
[21] MTCR, 'Guidelines for sensitive missile-relevant transfers' (note 20), para. 7.B.
[22] Brockmann, K. and Raju, N., *Newspace and the Commercialization of the Space Industry: Challenges for the Missile Technology Control Regime* (SIPRI: Stockholm, Oct. 2022), p. 16.
[23] US Government (note 14).
[24] Leenman, K., Background briefing provided to the authors, July 2022.

3. Case studies of ITT and software control violations and risks

To contribute to building knowledge on the ways that unauthorized ITT and software transfers can occur and on the challenges this poses, this chapter explores concrete cases of export control violations, and cases where the risk of a possible violation was identified involving intangible transfers of missile-related technology or software. The aim is to derive lessons on good practices that MTCR partners can take up and promote in order to strengthen implementation of controls on ITT and software.

Methodology and selection of cases

To select the case studies, the authors reviewed available open source material on government websites as well as research reports.[25] The authors gathered 22 case studies on missile-related technology transfers involving 4 exporting and 24 importing states (see annex). Diversity was sought, to the extent possible, in terms of the countries in which the violations occurred. However, most ITT and software cases that are prosecuted and on which public information can be consulted involve United States companies or have been prosecuted by the USA. This is in part because US national legislation has a broader scope of controls, such as controls on the release of controlled technology to foreign nationals present in the US, or 'deemed exports', that are not covered in many other MTCR partners' export controls.[26] In addition, the US system appears to place greater focus on enforcing export control regulations through prosecuting violations and publicizing the cases. As a result, the authors relied heavily on US cases to identify compliance challenges and derive the good practices that are elaborated on below.

The four case studies presented in this chapter were selected based on their relevance to the MTCR, in terms of the type of technology or software exported and the types of exporters involved (e.g. industry or academia). Preference was given to cases on which there is more material available, such as a violation that was prosecuted and on which all the documentation can be consulted. Each case outlines the type of export control violation or risk of violation, as well as the type of missile-related ITT or software involved in the case; detection, enforcement and/or prosecution efforts; and the relevance of each case to the MTCR.

3D Systems and Quickparts: Emerging technologies and business practices in a globalized world

Export control breach and type of ITT or software

Between 2012 and 2019, 3D Systems Corporation (3D Systems) was alleged to have violated US arms and dual-use export control regulations by: (*a*) exporting controlled aerospace and spacecraft technology to its then subsidiary, Quickparts.com, Inc. (Quickparts) in China; (*b*) backing up controlled technology to a server in Germany; (*c*) re-exporting controlled technology from China to Taiwan; and (*d*) making available

[25] See e.g. Boyd, D., Lewis, J. G. and Pollack, J. H., 'Advanced technology acquisition strategies of the People's Republic of China', Defense Threat Reduction Agency, Sep. 2010; Stewart, I. J. with contributions from Williams, D. and Gillard, N., 'Examining intangible controls part 2: Case studies', King's College, London, June 2016; and Scott et al. (note 18), pp. 47–50.

[26] US Department of Commerce, Bureau of Industry and Security, 'Deemed exports', 2020, accessed 18 Feb. 2024.

controlled technology to an Indian and a British citizen (deemed export), all without obtaining the required licences.[27]

3D Systems produces 3D printers and provides on-demand 3D printing and related services, including for the aerospace and defence industry.[28] 3D Systems provided on-demand additive manufacturing services to industry customers under contract with the US Department of Defense and the National Aeronautics and Space Administration (NASA), producing controlled spacecraft parts and military-grade electronics equipment. 3D Systems worked with its subsidiary in China and other suppliers in third countries to generate price quotes in response to customer inquiries, and on the execution of print jobs. According to the proposed charging letters, 3D Systems employees sent controlled technical data in the form of computer-aided design/engineering files by email to the subsidiary in China on numerous occasions. These emails were subsequently backed up to a server in Germany. However, the licences required for these transfers were never sought, and nor were appropriate records kept about the transfers.[29] Within 3D systems, controlled technical data was also made available to two employees in the USA with foreign citizenship, an action that is deemed an export under US national legislation, without the required licences. These violations were probably not identified by the company due to serious inadequacies in its compliance procedures, its lack of a formal internal compliance system, poor labelling of controlled items and deficient access/rights management system.

Detection, enforcement and prosecution

The violations were discovered by an interagency investigation involving the US Department of Defense, NASA and the US Department of Commerce.[30] Initial indications of possible company malpractice were detected following a voluntary disclosure by a Quickparts customer and an outreach visit by a federal agent.[31] The case documents show no intention on the part of the company or any individual to export controlled missile technology for the purpose of supporting a missile programme. However, the case highlights several vulnerabilities that can result from handling controlled technical data without the necessary precautions and without internal compliance systems in place to prevent violations from happening. The company's actions resulted in 151 alleged violations of arms and dual-use export control legislation.[32] Related allegations involved breaches of the False Claims Act, since some of the actions concerned technical data received as part of contracts awarded by the US Department of Defense and NASA.[33] 3D systems entered into three settlement/consent agreements and accepted penalties of up to US$ 27 million. It also agreed to comprehensive obligations to strengthen its

[27] US Department of Commerce, Bureau of Industry and Security, 'Order relating to 3D systems corporation', 27 Feb. 2023; and US Department of State, Directorate of Defense Trade Controls, 'Proposed Charging Letter: Alleged Violations of the Arms Export Control Act and the International Traffic in Arms Regulations by 3D Systems Corporation', [n.d.].

[28] 3D Systems, 'Additive Manufacturing for Aerospace and Defense', [n.d.].

[29] See charges 1–2 and 7–10, US Department of Commerce (note 27).

[30] United States Attorney's Office, Northern District of Texas, '3D printing company to pay up to $4.54 million to settle false claims act allegations for export violations in connection with NASA and DOD contracts', Press release, 27 Feb. 2023.

[31] See charges 3–6, US Department of Commerce (note 27), paras 8–10.

[32] The charging letters allege 19 violations of the Export Administration Regulations (EAR) covering dual-use items, and 132 violations of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) covering defence articles and services.

[33] US Department of Commerce, Bureau of Industry and Security, 'BIS imposes $2.77 million penalty on 3D printing company for exports to China and Germany, including aerospace and military design documents', Press release, 27 Feb. 2023; US Department of State, 'US Department of State concludes $20,000,000 settlement of alleged export violations by 3D Systems Corporation', Media note, 27 Feb. 2023; and United States Attorney's Office, Northern District of Texas (note 30).

compliance and reporting systems, and to audit requirements.[34] These agreements involved extensive obligations to strengthen the company's export compliance system, additional suspended penalties and even export bans. This is an example of an alternative means of pursuing a prosecution that provides an opportunity, where appropriate, for a company to improve its practices despite the extent of its violations.

Relevance for the MTCR

This case is illustrative of globalized supply chains where electronic transfers and providing access to digital engineering files are part of daily business. Additive manufacturing is a specific emerging technology that has become increasingly important in the context of missile and space launch vehicle technology.[35] It is also an example of where advances in technology have led to the emergence of new business practices. Companies can now offer on-demand printing services that often involve additional design or optimization steps which require access to technical data in the form of engineering files. The case shows that routine parts of a company's operations, such as its workflow to generate quotes for customers and the back-up system for the company's email server, can result in a significant number of export control violations if controlled technology is not marked or subject to an access management system. This is exacerbated where there is a general lack of awareness of licensing requirements or complacency despite knowledge of possible issues with export licensing requirements.[36]

Hamid Reza Karimi: University professor expelled from Norway for transferring knowledge to China

Export control breach and type of ITT or software

Hamid Reza Karimi, an Iranian-German professor at the University of Agder, was expelled from Norway in January 2015. He was found to have transferred knowledge that could be used to develop hypersonic cruise missiles to Chinese researchers without having obtained any prior authorization or licence.[37] At the time, Karimi was working with and supervising the research of a Chinese PhD student, Hu Xiaoxiang, who was also expelled. Together, they had co-authored five articles on the management and control of hypersonic aircraft, in particular on scramjet engines, in collaboration with Chinese researchers. Notably, the articles had been written before Hu moved to Norway, while he was still based in China, and the research was disclosed as part of his application for a residence permit in Norway.[38] While the information did not emerge publicly at the time, it has since been revealed that prior to moving to Norway Hu was affiliated with the Rocket Force Engineering University, a missile research centre linked to the Chinese military, and had received funding from China for a three-year research project on hypersonic aircraft.[39]

[34] US Department of Commerce (note 27); US Department of State, Bureau of Political-Military Affairs, 'Consent Agreement', 24 Feb. 2023; US Department of State, Bureau of Political-Military Affairs, 'Order', 24 Feb. 2023; and United States Attorney's Office, Northern District of Texas (note 30).

[35] Brockmann, K., *Additive Manufacturing for Missiles and Other Uncrewed Delivery Systems: Challenges for the Missile Technology Control Regime* (SIPRI: Stockholm, Oct. 2021).

[36] See charges 3–6, US Department of Commerce (note 27), paras 7–11.

[37] Government of Norway, 'Høring: forslag til endringer i eksportkontrollforskriften' [Consultation: proposal for changes to the export control regulations], 28 Mar. 2022.

[38] Kubens, V., 'Anklage: UiA-ansatte truer Norges sikkerhet' [Accusation: UiA employees threaten Norway's security], Fædrelandsvennen, 21 Aug. 2015.

[39] Joske, A., 'Picking flowers, making honey: The Chinese military's collaboration with foreign universities', *Australian Strategic Policy Institute*, Policy Brief 10/2018, 30 Oct. 2018, pp. 13–14.

Detection, enforcement and prosecution

Following their expulsion, Hu returned to China and Karimi initially continued to work for a university based in Germany.[40] The respective lawyers for the professor and his student took the case to the Oslo District Court, which overturned the expulsions in September 2015, arguing that the researchers were carrying out basic scientific research.[41] It is not known whether a legal challenge was lodged in Hu's case, as there is no publicly available information. Public statements by the Norwegian authorities do not mention Hu's affiliation with missile research centres in China, probably because the information is classified, but Hu has since published further articles from such centres, including the Air and Missile Defense College at the Air Force Engineering University in Xi'an.[42]

The Norwegian authorities successfully appealed the District Court's judgment in the case of Karimi. The Appeal Court found that he had carried out a transfer of knowledge in breach of export control regulations and in particular that research at doctoral level involved the mobilization of knowledge and expertise beyond what is available in the public domain.[43] It also found that the research should be considered applied research, due to its specific military application for the development of hypersonic vehicles.[44] The Appeal Court stressed that the research collaboration—rather than the published articles themselves—constituted a transfer of knowledge.[45] Information related to the case is limited because some of the court documents remain confidential due to their sensitive nature.[46]

Relevance for the MTCR

This case is an example of the challenges that must be addressed when determining whether academic research is covered by export control regulations, and particularly whether it constitutes applied or basic scientific research, and the technology produced by the research was already in the public domain. It also demonstrates the difficulty of determining when certain theoretical research can effectively contribute to the development of missile technology. In this case, it also remains unclear whether the research was part of a university project or carried out by the researchers alongside their university work, and therefore who is considered the exporter. Nonetheless, an apparent lack of awareness of the risks appears to have resulted in a lack of understanding by the university of why the research required a licence.[47]

This and a similar case appear to have contributed to Norway beginning a process of strengthening regulations on knowledge transfer.[48] In particular, while compliance efforts by universities remain central, the changes seek to give additional tools to academia by providing definitions of and further information on knowledge transfers, and giving a bigger role to national authorities to support the determination of what constitutes applied research that should be controlled.

Finally, in this case a more thorough visa screening procedure would have been beneficial as the articles on sensitive dual-use research co-authored by Karimi and Hu

[40] Scott et al. (note 18), pp. 47–50.
[41] Lie, T., Tonessen, E. and Vold, S., 'Agder-forskere vant mot PST' [Agder researchers win against PST], Khrono, 16 Sep. 2015.
[42] Scott et al. (note 18), pp. 47–50.
[43] Government of Norway (note 37).
[44] Lie et al. (note 41).
[45] Government of Norway (note 37).
[46] Kubens (note 38).
[47] Scott et al. (note 18), pp. 47–50.
[48] Government of Norway (note 37).

that formed part of the case were submitted to Norway as part of the student's visa application.

Firefly and Noosphere: FDI screening leads to divestment request in relation to small launcher manufacturer

Risk of export control breach and type of ITT or software

In 2021, the US Committee on Foreign Investment (CFIUS), the committee in charge of screening investments in the USA, requested that Noosphere Venture Partners (Noosphere) divest its stake in Firefly Aerospace, Inc. (Firefly), a small launch vehicle manufacturer based in the USA, for national security reasons.[49] Noosphere, which at the time reportedly had a 50 per cent stake in Firefly, was owned by Ukrainian-born investor Max Polyakov.[50]

Polyakov made his initial investment in Firefly in 2017, after it had filed for bankruptcy. In September 2021, Firefly conducted a first launch attempt of its 'Alpha' small launch vehicle in the USA. Its technical characteristics mean that the Alpha rocket developed by Firefly is covered by the MTCR annex as a Category I item.[51] With Polyakov, Firefly also opened a subsidiary in Dnipro, Ukraine in May 2018 to conduct research and development activities, including on automation aggregates, parts of combustion chambers and turbo-pumps. This involved making high-quality metal parts and components using a 3D-printer intended for industrial manufacturing.[52] At the time, Firefly was negotiating and had reportedly obtained a Technical Assistance Agreement, which allowed it to share information between its US and Ukrainian facilities.[53] Through these activities, know-how and technical data were probably shared with the Ukrainian subsidiary of Firefly that had been established under its ownership, and could have been made available to Noosphere.

Detection, enforcement and prosecution

When CFIUS made its request, Firefly was about to conduct a second Alpha launch attempt. At the time of the announcement, the US government suspended all launch preparations. Beyond the stated 'national security reasons', CFIUS did not make public any details of what prompted the divestment request. In a statement, Noosphere speculated that it was linked to growing tensions between Russia and Ukraine, and to reports of plans by Russia to launch a full-scale invasion of Ukraine.[54] The risk that missile-related technology could have made its way to Russia and possibly to other nations trying to develop rocket programmes may therefore have prompted the request. Noosphere announced that it would sell its interest in Firefly, and in March 2022 AE Industrial Partners, a private equity company already known in the NewSpace market, bought Noosphere's shares.[55] Firefly has since resumed work on the

[49] Foust, J., 'Firefly halts launch preparations after federal government seeks divestment of foreign ownership', Space News, 30 Dec. 2021.

[50] Foust (note 49).

[51] Firefly Aerospace, 'Alpha Launch Vehicle', accessed 8 Feb. 2024.

[52] Firefly Aerospace, Inc., 'Firefly Aerospace opens research and development center in Dnipro, Ukraine', Press release, 23 May 2018.

[53] Timtchenko, I., 'Firefly looks to bolster aerospace ties with US, investing in Ukraine for the long-haul', *Kyiv Post*, 20 Aug. 2018; and Shishatsky, E., 'Макс Поляков, Firefly Aerospace: Мы будем делать 8 ракет в год [Max Polyakov, Firefly Aerospace: We will make eight rockets a year]', LIGA, 26 Dec. 2018.

[54] Foust (note 49).

[55] Noosphere Ventures, 'Noosphere Ventures LP to sell a major stake in Firefly Aerospace to AE Industrial Partners', 23 Mar. 2022.

NASA contracts it was involved in and signed an agreement to cooperate with the US Department of Defense.[56]

Relevance for the MTCR

While the MTCR prescribes controls on the making available of missile-related technical data, these do not extend to requesting controls on changes in company ownership that could lead to such a situation. This case therefore illustrates the role that policy tools other than export controls, such as FDI screening mechanisms, can play in preventing the risk of technology proliferation, and especially in intervening prior to the occurrence of a possible export control violation. The case also demonstrates that company due diligence should be a dynamic process. Before 2021, it appears that Firefly enjoyed fruitful cooperation with the US authorities and had obtained all the necessary authorizations.[57] Probably as a result of the changing geopolitical context, however, the risk profile increased, leading the national authorities to take action.

Jonathan Yet Wing Soong: Export of specialized aeronautics software through an intermediary to a Chinese university

Export control breach and type of ITT or software

Jonathan Yet Wing Soong, a US national, was convicted of violating US export control law by conspiring to export controlled software through an intermediary to a university in Beijing that is listed on the US Entity List for its ties to Chinese missile and UAV programmes.[58] Soong worked as programme administrator at the Universities Space Research Association, a non-profit research corporation focused on 'advancing space science and technology', where he was 'conducting and servicing software license sales, conducting export compliance screening of customers, generating software licenses, and exporting software pursuant to purchased licenses'.[59] In 2017, Soong was approached by Beihang University—also known as Beijing University of Aeronautics and Astronautics—about the purchase of CIFER (Comprehensive Identification from Frequency Responses) flight test data software for modelling aircraft performance. The Beihang University representative proposed exporting the software package through an intermediary—Beijing Rainbow Technical Development Ltd—and Soong ultimately made the sale despite knowledge of the software being subject to US export controls and the end-user being included on the Entity List. Soong also arranged for the passcodes for the software package to be forwarded to Beihang University in July 2018.[60] By intentionally exporting controlled software to a restricted party without acquiring a licence, and by creating the appearance of a different end-user, Soong violated the licensing requirements created by the listing of both the software and the entity identified as the ultimate end-user.

[56] Fernholz, T., 'Firefly Aerospace tapped to compete for US spy sat launches', *Payload Space*, 26 Jan. 2024; and Firefly Space, 'Firefly Aerospace selected to demonstrate launch and on-orbit services for US Defense Innovation Unit', 21 Mar. 2024.

[57] Foust (note 49).

[58] United States Attorney's Office, Northern District of California, 'Castro Valley resident pleads guilty to illegally exporting American Aviation technology to Beijing University', Press release, 17 Jan. 2023. 'The Entity List is a US government compilation of foreign individuals, companies, and organizations deemed a national security concern, subjecting them to export restrictions and licensing requirements for certain technologies and goods', see US Department of Commerce, Bureau of Industry and Security, 'Entity list', accessed 27 Mar. 2024.

[59] United States Attorney's Office, Northern District of California (note 58).

[60] United States Attorney's Office, Northern District of California (note 58).

Table 3.1. Compliance challenges relevant to the specific type of violation and case scenario in the missile technology context

Types of unauthorized export potentially constituting a violation	Relevant types of missile-related technology transfers	Associated compliance challenges
Intangible transfers of technical data (TD) and/or software (S)		
Sharing of controlled TD or S via local or cloud-based servers and digital exchange files	Sharing 3D printing engineering files; Uploading controlled training materials	Lack of information security and/or access management procedures; Lack of data encryption
Sharing of controlled TD or S with customers or supply chain entities based abroad	Sharing technical drawings, blueprints, user manuals	Lack of effective export compliance system throughout the supply chain (including licence obligations and provisions); Possible misclassification of controlled items
Sale of controlled TD or S (including via third parties)	Selling aeronautics or modelling software	Possible falsification of licence application; Lack of due diligence and end-use checks
Making available TD or S following company/controlling interest acquisition through FDI	Granting access to controlled proprietary information	Lack of information security and/or access management procedures; Lack of FDI screening procedure
Making available TD or S to foreign visiting employees/researchers	Granting access to controlled TD or S	Lack of or improper screenings and checks; Lack of information security and/or access management procedures
Provision of technical assistance (TA)		
Provision of TA to foreign visiting employees/researchers	Publishing applied dual-use research in e.g. hypersonic flight or heat-resistant aerospace materials and/or at high Technology Readiness Levels; Sharing expertise in the aerospace industry	Lack of or proper visa screening; Lack of due diligence checks; Lack of information security procedures; Lack of awareness and/or understanding of the exemptions for basic scientific research and information in the public domain
Provision of TA during in-person visit abroad	Presentation at an international conference; Conducting launch failure analysis using controlled technology	Lack of awareness
Provision of TA through virtual means (e.g. videoconference)	Providing remote instruction and training; Participating in remote meetings	Lack of information security procedures
Sale of TA	Providing engineering expertise as a consulting service (know-how transfer)	Lack of due diligence and end-use checks

Detection, enforcement and prosecution

Soong was charged in September 2022 and pleaded guilty to all charges. He was convicted in April 2023 and sentenced to 20 months in prison and three years supervised release, and ordered to pay US$ 168 885 in restitution.[61] Public reports on the case do not specify how the violations were detected but state that the prosecution was the result of an interagency investigation involving the US Bureau of Industry and Security, the Defense Criminal Investigative Service and the Federal Bureau of Investigation with assistance from NASA, the US Army and the Department of Homeland Security.[62]

Relevance for the MTCR

Illicit procurement through universities of specialized software and technology relevant to missile programmes is a common strategy of states pursuing missile programmes that lack access to such software or technology. China in particular, through its civil-military fusion strategy, but also Iran and North Korea have been found to take advantage of academic relations or the idea that universities are non-threatening end-users to acquire controlled software and technology.[63] This case highlights the issue of a potential lack of understanding of the sensitivity of transfers to a university end-user, and of the possibly misguided leniency of exporters under such circumstances. Notably, the use of intermediaries, as found in this case, is a common strategy in illicit procurement that is not specific to MTCR-relevant software and technology.

Typology of export control violations involving intangible transfers of missile-relevant technology or software

The case studies discussed above present only a few of the possible scenarios whereby an exporter can violate export control regulations by transferring or making available technology or software using intangible means. It is therefore important to consider the broader range of export control violations and the corresponding types of transfers of missile-related technology that can result in such violations if performed without obtaining the required licences or without respecting the provisions of the licences obtained. A better understanding of the typology of violations and of possible cases and scenarios in the missile proliferation context can help to raise awareness, sensitize relevant stakeholders and improve vigilance. Based on this typology, table 3.1 identifies compliance challenges relevant to the specific type of violation and case scenario in the missile technology context. Chapter 4 zooms in on five key challenges that emerge from the typology and the analysis of the case studies provided above.

[61] US Department of Commerce, Bureau of Industry and Security, 'In the matter of: Jonathan Yet Wing Soong [...]; and order denying export privileges', *Federal Register*, vol. 88, no. 245 (22 Dec. 2023), pp. 88565–66.

[62] US Department of Commerce, Bureau of Industry and Security, 'South Bay resident charged with smuggling and exporting American Aviation technology to Beijing University', Press release, 5 Feb. 2024.

[63] Dathan, M. and Kenber, B., 'HMRC accuses British universities of inadvertently aiding Chinese military', *The Times*, 8 Feb. 2021; Joske (note 39); Pollack, J. and LaFoy, S., 'North Korea's international scientific collaborations: Their scope, scale, and potential dual-use and military significance', *CNS Occasional Paper*, no. 43 (Dec. 2018); and Yerushalmy, J. and Bhuiyan, J., 'Academics in US, UK and Australia collaborated on drone research with Iranian university close to regime', *The Guardian*, 14 Feb. 2024.

4. Key challenges posed by intangible transfers of missile-related technology and software

Global supply and value chains: An increased reliance on ITT

Due to the complexity of the products it develops and uses, the aerospace industry largely relies on global supply chains.[64] Many start-up companies—including in the NewSpace industry—have followed a similar path by externalizing non-core business tasks in their value chains.[65] In industries with global supply and value chains, transfers of technical data between companies and their subsidiaries, supply chain partners and clients are usually necessary for product development, production, sales and use.

The business model of additive manufacturing companies providing on-demand 3D printing services is a useful example. Additive manufacturing is becoming of increasing relevance to the aerospace sector, as more and more parts and components for space launch vehicles with highly specific performance characteristics are produced using additive techniques.[66] Some additive manufacturing companies have their headquarters and engineering departments producing high-tech machines in one country, while their design teams, sales teams and other auxiliary functions are based in other countries. This means that different entities in the same company, or in the same supply chain, must transfer on a regular basis technical data in the form of design files and blueprints to their subsidiaries or suppliers abroad, for example to obtain price quotes, and ultimately to have the items 3D-printed.[67] In addition, technical data is also transferred between companies and their clients for on-demand printing services.

The structure of global supply and value chains means that all stakeholders require a thorough understanding of the export control regulations that apply to the transfer of missile-related technical data, as well as appropriate internal compliance systems in place throughout the chain. Where suppliers and other stakeholders are established in different states, the regulatory frameworks of several states must be considered.[68] This can present challenges for established companies, but even more so for new actors in the NewSpace industry, and those working with emerging technologies or entities with limited knowledge of export controls and ITT controls. Due to their small size and relatively recent establishment, many NewSpace companies, particularly start-ups, often lack a dedicated export control compliance department.[69] This risks companies sharing controlled technology with supply chain entities, subsidiaries and clients without obtaining the required licences, or failing to respect the conditions on the licences they have been granted.

[64] See e.g. 'Invested in global supply chain for best value', Magellan Aerospace, [n.d.].

[65] Denis, G. et al., 'From new space to big space: How commercial space dream is becoming a reality', *Acta Astronautica*, vol. 166 (Jan. 2020), pp. 433–35.

[66] Brockmann, K. and Bauer, S., '3D printing and missile technology controls', SIPRI Background Paper, Nov. 2017.

[67] See e.g. US Department of Commerce (note 33); and US Department of Commerce, Bureau of Industry and Security, 'Temporary denial order issued for illegal export of satellite, rocket and defense technology to China', Press release, 8 June 2022.

[68] Stewart, I. and Brewer, J., 'Engaging the private sector in nonproliferation: Reflections from practitioners', *Strategic Trade Review*, vol. 2, no. 3 (Autumn 2016).

[69] Brockmann, K. and Héau, L., 'Developing good practices in export control outreach to the NewSpace industry', *SIPRI Insights on Peace and Security* no. 2023/04 (Mar. 2023).

Cloud computing and advances in digital transfers: The multiplication of ITT channels

Advances in cloud computing and other digital means of information and file exchange have enabled easier and more frequent ITT transfers. Cloud computing is 'the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer'.[70] The technical data needed to conduct activities such as rocket engineering and modelling is increasingly stored digitally. Most transfers of technical data and software occur using electronic, non-physical means. For example, companies are increasingly using digital file exchange tools to transfer computer-aided design files, including for 3D printing.[71] Transfers and the making available of technical data and software also increasingly take place through servers, whether local or cloud-based. As the number of commercial spaceports multiplies, space launches provide an illustration of an expanding area of business activity that involves the digital sharing of technical data between a wide range of actors—from satellite and space launch vehicle manufacturers, to launch service providers and launch facility operators.[72] Specifically, in the case of failures, launch failure analysis might involve the sharing of launch or flight test data as well as technical assistance in order to understand the cause of the failure and to remedy it.[73]

Advances in communications technology mean that technical assistance can be provided more easily using a variety of means, beyond in-person instruction. Many digital means of communications are becoming common in the daily work of companies and research institutes. In addition to traditional means such as telephone calls and in-person meetings and instruction, video conferencing, digital learning platforms and other means of remote instruction and teaching have become omnipresent since the Covid-19 pandemic—further expanding the means available to provide technical assistance. After several years of remote working and use of these means in day-to-day work, some may have become less alert to what might constitute transfers of technical data or technical assistance that requires an export licence.

The use of cloud computing and other digital transfer and communication tools makes it difficult for exporters to track all the transfers that are taking place through these various channels, and for states to enforce export controls in cases where controlled technology is transferred through these channels. To track transfers, effective information security systems, which include marking export-controlled data, determining and mapping which employees need to be granted access to it and raising awareness among staff, are key. Protecting data through end-to-end encryption and other cybersecurity measures has also been identified as good practice, not least to prevent theft and unauthorized access.[74] The enforcement of export controls in the context of cloud computing and global server architectures presents even more challenges, as in prac-

[70] Dryfhout, M. and Hewer, S., 'What is cloud computing?', Scout Technology Guides Blog, 11 Apr. 2019.

[71] See e.g. 'DEXcenter', International TechneGroup Incorporated, accessed 18 Feb. 2024.

[72] Brockmann and Héau (note 69).

[73] United States House of Representatives, Select Committee, *US National Security and Military/Commercial Concerns with the People's Republic of China*, vol. 1 (US Government Printing Office: Washington, DC, Jan. 1999).

[74] German Federal Office for Economic Affairs, *Export Control and Academia Manual*, Second edn (Nov. 2023), p. 108; French Secretariat-General for National Defence and Security, 'Guide de bonnes pratiques en matière de communication, d'usage et de stockage d'informations, sans mouvement d'un support physique, susceptibles de relever du contrôle des exportations de matériels de guerre' [Good practice guide on communication, use and storage of information, without movement of a physical medium, likely to come under the controls on exports of war material], Apr. 2023; and Suri, N., 'Emerging technologies and the challenges of controlling intangible technology exports', *Strategic Trade Review*, vol. 6, no. 9 (winter/spring 2020).

tice the location of the server, access rights management and other factors are assessed differently by different states' export control authorities.[75]

Applying the 'basic scientific research' and 'in the public domain' exemptions to academia

Universities are important actors in the field of ITT because much of the research they produce can be transferred in intangible forms such as informal exchanges between researchers, articles in scientific publications, training and inviting foreign researchers to work on dual-use research. In the context of the MTCR, cutting-edge research on optics, hypersonics and other advanced fields that are highly relevant to missile development is currently being conducted in academic and research institutes.

However, determining what constitutes basic scientific research continues to be a challenge in academia, in part because it often does not correspond with the classification of fundamental as opposed to applied research that researchers make in a scientific context.[76] The Technology Readiness Levels (TRLs) originally developed by NASA are one tool for assessing the status of technology development.[77] Use of TRLs is now common in universities, including within European research and innovation programmes, to assess the maturity of new and emerging technologies. However, this relies on university and research actors making a technology readiness assessment and cannot be the sole basis for determining whether the basic scientific research exemption is applicable. For example, a research output that stems from low TRL research—generally considered to be basic scientific research—but funded by an industry partner with a specific technological or commercial objective could constitute applied research that falls outside of the scope of the exemption.[78]

Determining when information is already in the public domain is equally challenging in practice. Even where technology development is based on sources and methods that are in the public domain, this could be covered by export controls if new knowledge is created by the research.[79] The lack of clarity over the exemptions for basic scientific research and information in the public domain means that universities have often struggled to understand the scope and meaning of these exceptions.[80] This problem has been heightened by the lack of resources and expertise available in academic institutions to operate an effective internal compliance programme or adequately train an ever-changing research staff.[81] As a result, universities have in many cases been too slow to comply or not proactive enough in effectively complying with ITT and software controls, and more broadly developing a culture of compliance.

[75] Bromley, M. and Brockmann, K., 'Implementing the 2021 recast of the EU dual-use regulation: Challenges and opportunities', *Non-proliferation and Disarmament Papers*, no. 77 (Sep. 2021).

[76] German Federal Office for Economic Affairs (note 74), p. 19.

[77] Office of the Chief Technologist, National Aeronautics and Space Administration (NASA), *Technology Readiness Assessment: Best Practices Guide*, SP-20205003605, [n.d.].

[78] European Commission, 'Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items', *Official Journal of the European Union*, L338/1, 23 Sep. 2021.

[79] German Federal Office for Economic Affairs (note 74), p. 78.

[80] Government of Norway (note 37).

[81] ECORYS and SIPRI, *Data and Information Collection for EU Dual-use Export Control Policy Review*, final report, 6 Nov. 2015.

Demand side challenges: Attempts at technology and software acquisition

States and non-state actors in pursuit of missile capabilities actively seek to acquire technology—especially know-how—and software, which heightens proliferation risks in this area for both industry and academia. Within industry, individual staff currently working or having previously worked in aerospace companies can be targeted or recruited.[82] In other cases, malevolent actors use covert acquisition methods to try to hide the real end-user and importer of the technology or software. A particular compliance challenge for companies attempting to prevent illicit procurement is therefore to gain accurate knowledge of the genuine end-use of the software or technology prior to exporting it.[83]

Academic research collaboration provides another avenue through which actors attempt to acquire missile-related technology. For example, China has been active in sending scientists to work at Western universities in fields such as hypersonic flight and heat-resistant aerospace materials and seeking opportunities to establish joint research centres.[84] Some of the scientists concealed their association with conglomerates involved in developing and supplying missiles to the Chinese military. Regarding North Korea, a 2021 report by the United Nations Panel of Experts monitoring the implementation of sanctions against North Korea indicated that it was considering information on 161 potential cases of joint research, studies or jointly published papers with North Korean scholars since 2017, many of which are likely to involve missile-related technology.[85]

Understanding the full range of situations in which technical assistance can occur in this context is a serious challenge. For example, a collaboration on sensitive research between a foreign visiting researcher and local university staff in the state where the researcher is studying or working can constitute a provision of technical assistance. Moreover, while in most cases a research outcome that takes the form of a publication or conference presentation will not be considered technical data or assistance in the export control sense, the content of the exchanges that take place throughout the collaboration could be.[86] In other cases, foreign universities are indicated as the—seemingly non-sensitive—end-users of an exported technology even though those universities are actually involved in and will pass technology and know-how on to a state's missile or space launch vehicle programme.[87]

Evidence of attempts at illicit technology and software acquisition only strengthens the case for further improving the export compliance programmes of industry, research and academia, and for states to raise awareness of the specific risks posed by certain illicit procurement strategies. In addition, it highlights that complementary control instruments such as visa screening tools or dedicated vetting programmes such as the United Kingdom's Academic Technology Approval Scheme (ATAS) can be an important tool for detecting and preventing illicit procurement and technology acquisition.[88] These instruments should be used carefully to avoid discriminating against researchers and hampering international cooperation, but with sufficient vigilance to reduce risks.[89]

[82] United States Attorney's Office, Northern District of California (note 58); and Boyd, Lewis and Pollack (note 25), p. 35.

[83] 'What you don't know can hurt you', Novis Trade Consultancy, 19 Jan. 2024.

[84] Joske, A., 'The China Defence Universities Tracker: Exploring the military and security links of China's universities', *Australian Strategic Policy Institute*, Policy Brief no. 23/2019.

[85] United Nations Security Council, Panel of Experts assisting the 1718 DPRK Sanctions Committee, 'Final report', S/2021/211, 4 Mar. 2021.

[86] Government of Norway (note 37).

[87] United States Attorney's Office, Northern District of California (note 58).

[88] British Government, Guidance, 'Academic Technology Approval Scheme (ATAS)', Updated 19 Feb. 2024.

[89] Government of Norway (note 37).

Transfers of and making available technology as a result of foreign direct investment and changes in ownership

Many companies developing or working with emerging technologies, including NewSpace start-ups, increasingly rely on private funding sources and capitalization models as part of their business models.[90] Rather than depending on public funding and government contracts like much of the traditional space industry, many NewSpace and emerging technology companies fund their activities through venture capital acquired in open funding rounds or joint ventures. Funding received through these channels can include FDI and lead to company acquisitions or acquisition of controlling interests by foreign investors. Foreign investors can gain access to controlled technology as access is granted as part of the investment process, or by gaining access to a company's proprietary information in the case of controlling interests and company acquisitions. This is not limited to the design of the technology itself but also extends to the knowledge required to manufacture the items, the research skills and quality assurance procedures.[91] Without appropriate safeguards, start-up companies that are highly dependent on private investment are especially vulnerable to FDI being used as a technology procurement strategy.

When potential investors show an interest in gaining ownership of or a controlling interest in a company, that company needs to ensure that it is compliant with applicable FDI screening procedures. These allow the government to scrutinize the investment and discover any potential illicit procurement efforts. Moreover, where investment or the provision of funding comes with certain conditionalities that would allow the investor access to certain proprietary information or technology, any such transaction should be scrutinized, and where necessary the required export licences will need to be obtained. In all cases, companies will need to establish access and rights management systems, which involves limiting and controlling access to sensitive technical data and know-how by foreign investors. National FDI screening mechanisms can be a helpful tool for identifying and preventing transfers of technology.[92] However, they are dependent on companies and foreign investors applying for authorization, and they may not always be aware of their obligations. FDI screening can result in requests that further information related to sensitive activities must be protected, and in procedures being put in place on the sharing of information.[93] In cases where the security risks are too high, or where vulnerabilities have been identified by national security authorities, FDI screening mechanisms can be used to block certain foreign investments in companies.

[90] Brockmann and Raju (note 22).

[91] British Parliament, Intelligence and Security Committee, 'China', HC1605, 13 July 2023, para. 359.

[92] Brockmann and Héau (note 69).

[93] Government of France, French Ministry of Economics and Finance, French Treasury, 'FAQ: Foreign Direct Investment Screening in France', Oct. 2023.

5. Strengthening the MTCR's efforts to address proliferation risks posed by ITT and software

Export control and proliferation challenges related to transfers of missile-related technology and software are not new but current developments warrant a continued focus on the topic. Companies in the aerospace and NewSpace sectors and their global supply chains increasingly rely on ITT and software for their activities. Digital transfers of technology and software, including through cloud-based servers, have also become easier and as a result more common. Despite this, many companies, in particular recently established NewSpace and emerging technologies start-ups, lack detailed awareness of ITT and software controls or effective methods of ensuring compliance with such controls. Compliance is also a challenge among research institutes and especially in academia, where research is being undertaken on fields that are highly relevant to missile development. Actors actively seeking to acquire technology and software to advance their missile programmes can take advantage of this. They could also exploit the increasing trend for FDI to access technology by gaining control of or ownership rights over a company.

As states continue to encounter a range of challenges in their attempts to enforce ITT and software controls, the MTCR has an important role to play in addressing these. The recommendations below suggest ways to strengthen the role of the MTCR in preventing the proliferation of missile-related technology and software.

Produce targeted guidance on ITT and software controls

The MTCR partners should develop—or if it already exists publish—guidance on ITT and software controls. Such guidance would help to strengthen implementation and improve the consistency of how MTCR partners apply ITT and software controls. A guidance document should not only contain detailed explanations of the definitions provided in the annex, but also elaborate on their interpretation and on cases particularly relevant to missile technology proliferation—with case studies from across the typology identified in this paper. Guidance should also be provided on establishing or strengthening the necessary resources of national licensing and enforcement authorities, including intelligence and investigative services and specialized prosecutors.

For an MTCR guidance document on ITT controls to be particularly impactful, it should be publicly available for the benefit of states beyond the membership of the MTCR, with the necessary limitations regarding some case details. Publishing such guidance materials—at least in a limited format—on the MTCR website would have the benefit of adding to the public goods provided by the multilateral export control regimes and help to improve perceptions of the MTCR among adherents and non-partners.

Strengthen awareness-raising and compliance with ITT and software controls among the aerospace industry, researchers and academia

Complying with ITT and software controls is a significant challenge for all exporters, but particularly for start-ups, research institutes and academic institutions. In addition to targeted guidance materials, states should therefore strengthen their outreach and awareness-raising efforts targeted at NewSpace and emerging technology industry stakeholders, and relevant research institutes and academic institutions involved in teaching aerospace engineering and rocketry or in developing aerospace and SLV technology. Few states have experience of industry mapping or targeted outreach to

the NewSpace industry. The MTCR should be used as a forum for exchanging such experience and feeding it into good practice materials.[94]

The topic of ITT and software controls, and complementary instruments such as FDI and visa screening procedures, should be a central component of targeted outreach and awareness-raising efforts. Increasing awareness, strengthening internal compliance programmes and technology access management systems, and generating buy-in from relevant stakeholders are also key to the effective implementation of catch-all controls.

Enhance information-sharing on cases of violations of ITT and software controls

While missile-related ITT and software are becoming more common and their significance is increasing, many states—even among the MTCR partners—have little experience of detecting, investigating and successfully prosecuting where such transfers violate export controls. It is therefore even more important for partners to make effective use of the information exchange systems provided for in the MTCR. In particular, notifications should not just be shared where formal denials are issued. Where appropriate, information should also be shared about cases where other avenues were chosen to discourage exporters from pursuing certain business relations that might otherwise involve transfers or making available missile-related technology or software.

States should continue to present ITT and software cases—not necessarily limited to missile technology—and specific insights on legal systems, detection, investigation and prosecution through the LEEM. Sharing good practices among enforcement officers, and particularly between national prosecutors, could help to overcome the persistent difficulties in conducting successful investigations and enable the prosecution of export control violations involving ITT. Given the cross-cutting nature of ITT, states should also continue to hold exchanges on ITT and software in the technical experts meeting (TEM) to address relevant technical aspects, as well as in joint meetings between the information exchange meeting (IEM), the LEEM and the TEM.

Strengthen discussions with adherents and non-partners

By producing guidance, exchanging outreach best practices and sharing information about concrete cases of export control violations, MTCR partners would be helping to increase knowledge about ITT control breaches and possible ways of addressing them. Sharing such information with adherents and non-partners that might be facing similar challenges would be particularly useful. For adherents, this could take place through sharing the ITT-related presentations made by partners at the LEEM, in bilateral meetings with the MTCR Chair and through the technical outreach meetings (TOMs). In addition, as the number of fully prosecuted cases remains small, the value of disclosing information by making presentations on cases to adherents and non-partners, for example during TOMs, would be particularly high. Adherents could also present their own export control policies in the TOMs.[95] This would be an opportunity to include discussions on ITT controls and related challenges, and to hear best practices and experiences from MTCR partners and adherents, notably those that already apply MTCR guidelines. Outreach missions to non-partners should also include exchanges on ITT controls, especially in states with an aerospace industry or that are developing a NewSpace industry.

[94] Brockmann and Héau (note 69).

[95] Brockmann, K., Bromley, M. and Héau, L., *The Missile Technology Control Regime at a Crossroads: Adapting the Regime for Current and Future Challenges* (SIPRI: Stockholm, Dec. 2022), p. 12.

Strengthen inter-regime dialogue

While it is useful to examine the specificity of ITT controls in the context of the MTCR, strengthening inter-regime dialogue is also key to addressing common challenges.[96] Such a dialogue could focus on the impact on the regimes of advances in emerging technologies such as cloud computing and additive manufacturing. In addition, it should seek to further clarify and gain a common understanding of some of the key terms associated with ITT controls, such as what is meant by 'in the public domain' and 'basic scientific research', with a view to reducing differences among states in how software and technology are made subject to controls, and how the controls are applied.[97]

Explore linkages with complementary tools

The MTCR controls on ITT and software and their implementation by a growing number of states beyond the MTCR partners are key to preventing and addressing potential missile technology proliferation risks. Traditional export controls are naturally limited in scope, however, and could be strengthened by the use of additional or alternative tools. Visa screening mechanisms are not new but their use could be increased, for example, when it comes to foreign nationals interested in enrolling in sensitive academic disciplines, but also for screening foreign employees in the aerospace and emerging technology fields. Other tools that could play a role have emerged more recently. FDI screening mechanisms play an important role in regulating transfers before an export control violation occurs. Advances in the NewSpace sector have led to the multiplication of commercial spaceports. The technology safeguards agreements that some states have adopted in this context are an effective means of establishing rules on limiting access to technical assistance and technical data as part of space launches.[98] Increased exchanges among MTCR partners about the utility of each of these complementary tools to achieving the MTCR's objectives, as well as on national practices for linking these different tools, would be a useful step in strengthening implementation of ITT and software controls.

[96] The 3 other multilateral export control regimes are the Nuclear Suppliers Group, the Australia Group and the Wassenaar Arrangement.

[97] Bromley and Maletta (note 1), p. 34.

[98] See e.g. New Zealand Treaties Online, 'Agreement between the Government of New Zealand and the Government of the United States of America on Technology Safeguards Associated with United States Participation in Space Launches from New Zealand', Entry into force 12 Dec. 2016; and Foreign, Commonwealth and Development Office, 'UK–US Technology Safeguards Agreement (TSA) for Spaceflight Activities: Understanding the TSA', Updated 8 Feb. 2021.

Annex. List of cases of missile-related ITT and software control violations and risks

Date	Name of entity	State from which the technology was exported	Description of the missile-related ITT or software control violation or risk	Means of enforcement
Intangible transfers of technical data and/or software				
Sharing of controlled technical data and/or software via local or cloud-based servers and digital exchange files				
2024	Boeing	USA	Exports and retransfers of technical data (including on several missile systems) to foreign-person employees and contractors in 19 countries via the company digital technical document repository[a]	Prosecution
2021	Honeywell International	USA	Export and retransfers of technical data (technical drawings) to Canada, China, Ireland, Mexico and Taiwan via digital file exchange tool[b]	Prosecution
2009	Georgia Institute of Technology	USA	Release of restricted course materials on infrared technology for weapon systems online involving downloads from China, Iran and Pakistan[c]	No action taken beyond disclosure of the breach
Sharing of controlled technical data and/or software with customers or supply chain entities based abroad				
2023	3D Systems and Quickparts	USA	Export of aerospace and spacecraft technical data (design documents) to subsidiary in China; backing up technical data to a server in Germany; re-export of technology from China to Taiwan; and making available technology to an Indian and a British citizen[d]	Prosecution
2022-23	Quicksilver, Rapid Cut and US Prototype	USA	Export of technical data (technical drawings and blueprints used to 3D print satellite, rocket, and defense-related prototypes) to China[e]	Temporary denials of export privileges to prevent 'imminent violation' of export controls
2019	AeroVironment	USA	Export of technical data (UAV user manuals) to Australia, France, Canada and Thailand[f]	Prosecution
2019	Darling Industries	USA	Export of technical data and provision of technical assistance to end-users in Canada[g]	Prosecution

Date	Name of entity	State from which the technology was exported	Description of the missile-related ITT or software control violation or risk	Means of enforcement
2017	Bright Lights USA	USA	Export of technical data (redacted versions of technical drawings) to China and India[h]	Prosecution
Sale of controlled technical data and/or software (including via third parties)				
2024 (ongoing)	Chenguang Gong	USA	Alleged theft of trade secrets (technology to track missiles and detect launches) which could have resulted in transfer of technical data to China[i]	Prosecution (case ongoing)
2022	Jonathan Yet Wing Soong	USA	Export and sale of CIFER flight test data software to Chinese university on the US Entity List[j]	Prosecution
Making available of technical data and/or software following company/controlling interest acquisition through FDI				
2021	Firefly	USA	National security risk identified following acquisition of small launch manufacturer by Ukrainian investor[k]	FDI screening resulting in divestment request
2021	Momentus	USA	National security risk identified regarding ownership of in-space transportation company by Russian nationals[l]	FDI screening resulting in divestment request
2020	Impcross Limited	UK	National security risk identified in proposed FDI transaction that would have resulted in acquisition of Impcross by a Chinese-owned aerospace company[m]	Pre-emptive Action Order to prevent acquisition
Making available of technical data and/or software to foreign visiting employees/researchers				
2009	NASA	USA	Improper access to controlled technology granted to foreign employee working as NASA contractor[n]	Investigation by the US Government Accountability Office (GAO) resulting in a report and in (recom-mendations to NASA
2009	John Reece Roth	USA	Conspiracy to export technical data to develop plasma technology for UAVs to foreign employee[o]	Prosecution
Provision of technical assistance				
Provision of technical assistance to foreign visiting employees/researchers				

Date	Name of entity	State from which the technology was exported	Description of the missile-related ITT or software control violation or risk	Means of enforcement
2015	Imperial College London	UK	Risk of provision of technical assistance as part of research project aimed at forming lighter and stronger aircraft components conducted in cooperation with China aerospace manufacturer[p]	No action
2016	Centre for Space Science and Technology Education in Asia and the Pacific	India	Risk of provision of technical assistance to North Korean and Iranian students during technical courses on space science and technology[q]	No action
2015	Hamid Reza Karimi	Norway	Provision of technical assistance related to hypersonics to China[r]	Prosecution
Provision of technical assistance during in-person visit abroad				
2003	Hughes Space and Communications	USA	Provision of technical assistance and export of technical data to China through launch failure analysis[s]	Prosecution
2003	Space Systems/ Loral	USA	Provision of technical assistance and export of technical data to China through launch failure analysis[t]	Prosecution
Sale of technical assistance				
2011	Noshir Gowadia	USA	Provision of technical assistance related to cruise missiles by US engineer to China[u]	Prosecution

Note: While a case may fit into several categories, for conciseness in this annex each case is listed in a single category.

[a] US Department of State, 'US Department of State concludes $51 million settlement resolving export violations by the Boeing company', Media note, 29 Feb. 2024.

[b] US Department of State, 'US Department of State concludes $13 million settlement of alleged export violations by Honeywell International, Inc.', Media note, 3 May 2021.

[c] Scott, E. et al., *Catalogue of Case Studies on Intangible Technology Transfers from Universities and Research Institutes* (King's College Centre for Science & Security Studies: London, Sep. 2020).

[d] US Department of Commerce, Bureau of Industry and Security, 'BIS imposes $2.77 million penalty on 3D printing company for exports to China and Germany, including aerospace and military design documents', Press release, 27 Feb. 2023; and US Department of State, 'US Department of State concludes $20,000,000 settlement of alleged export violations by 3D Systems Corporation', Media note, 27 Feb. 2023.

[e] US Department of Commerce, Bureau of Industry and Security, 'Quicksilver Manufacturing, Inc. [...]; Order Renewing temporary denial of export privileges', *Federal Register*, vol. 88, no. 108 (6 June 2023), pp. 37007-09.

[f] US Department of State, 'US Department of State concludes $1,000,000 settlement of alleged export violations by AeroVironment, Inc.', Media note, 20 Nov. 2019.

[g] US Department of State, 'US Department of State concludes $400,000 settlement of alleged export violations by Darling Industries, Inc.', Media note, 20 Nov. 2019.

[h] US Department of State, 'State Department concludes settlement of alleged export violations by Bright Lights USA, Inc.', Media note, 12 Sep. 2017.

[i] United States Attorney's Office, Central District of California, 'Engineer arrested for allegedly stealing trade secret technology designed to detect nuclear missile launches and track missiles', Press release, 7 Feb. 2024.

[j] United States Attorney's Office, Northern District of California, 'South Bay resident charged with smuggling and exporting American aviation technology to Beijing University', Press release, 26 May 2022.

[k] Foust, J., 'Firefly halts launch preparations after federal government seeks divestment of foreign ownership', Space News, 30 Dec. 2021.

[l] US Securities and Exchange Commission, 'Momentus finalizes and signs National Security Agreement', Press release, 9 June 2021.

[m] British Government, 'Proposed acquisition of Impcross Ltd by Gardner Aerospace: undertakings accepted', Notice, 8 Sep. 2020.

[n] US Government Accountability Office, 'Export controls: NASA management action and improved oversight needed to reduce the risk of unauthorized access to its technologies', Report to Congressional Requesters, 15 Apr. 2014.

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

[p] Stewart, I. J. with contributions from Williams, D. and Gillard, N., 'Examining intangible controls part 2: Case studies', King's College, London, June 2016.

[q] Scott, E. et al., *Catalogue of Case Studies on Intangible Technology Transfers from Universities and Research Institutes* (King's College Centre for Science & Security Studies: London, Sep. 2020).

[r] Government of Norway, 'Høring: forslag til endringer i eksportkontrollforskriften' [Consultation: proposal for changes to the export control regulations], 28 Mar. 2022.

[s] Helder, J. et. al., 'International trade aspects of outer space activities', in *Outer Space Law: Legal Policy and Practice, First* (Globe Law and Business Ltd: Nov. 2017).

[t] Helder et al. (note s).

[u] US Department of Justice, Office of Public Affairs, 'Hawaii man sentenced to 32 years in prison for providing defense information and services to People's Republic of China', Press release, 25 January 2011.

About the authors

Lauriane Héau (France) is a Researcher with SIPRI's Dual-use and Arms Trade Control Programme. As part of her work, she follows developments within the main instruments and regulations established to regulate the arms and dual-use trade at the national, European and international levels. Her recent work has focused on the Missile Technology Control Regime (MTCR), the impact of NewSpace, and intangible transfers of technology. She also conducts research on mitigating arms diversion risks, and follows developments within the Arms Trade Treaty.

Kolja Brockmann (Germany) is a Senior Researcher (non-resident) with SIPRI's Dual-Use and Arms Trade Control Programme. He is the project lead of the project 'Quo vadis MTCR II: Mapping and mitigating the potential impact of the NewSpace industry on missile technology proliferation' and its predecessor 'Quo vadis MTCR? The Missile Technology Control Regime at a crossroads'. His recent work has focused on the multilateral export control regimes, the European Union's dual-use export controls, post-shipment controls, and non-proliferation and export control challenges linked to additive manufacturing, artificial intelligence, hypersonic missile technology and the NewSpace industry.

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