Examining intangible controls

A report prepared by Project Alpha at King's College London with funding from the Swedish Radiation Safety Authority

Ian J. Stewart

With contributions from

Dominic Williams

Nick Gillard

Project Alpha
Centre for Science and Security Studies
King's College London

For all queries regarding distribution or other issues, please contact Ian J. Stewart (ian.stewart@kcl.ac.uk).

Project Alpha

Centre for Science and Security Studies

King's College London

Strand

London WC2R 2LS

United Kingdom

Telephone: +44 207 848 1342

Version 1, June 2016

Abstract

This paper examines the role of intangible technology controls in controlling the spread of proliferation-relevant technologies. An adapted capability acquisition model is presented in order to provide a tool through which to examine the contribution of intangible technology to proliferation. Using this model, several case studies are examined.

As a result of this examination, it is argued that a broader strategy is required to control intangible technology transfers that could aid proliferation. It is apparent that traditional export control approaches are not sufficient. As a result, new national laws and international mechanisms might be required. However, adoption of effective mechanisms is likely to prove to be controversial and so there is a need for a risk-based, targeted approach, as well as international cooperation. A new international forum might be required for this purpose, and it is argued that the UN Security Council's resolution 1540 mechanism might be well placed to provide this forum.

In parallel to working to put in place a broader strategy, this paper identifies certain specific measures that can be taken in relation to export controls to strengthen controls around intangible technology transfer.

Contents

Introduction

Globalisation and technological advancements are effectively making the world become smaller. Flows of information, ideas, and people are moving more rapidly than ever before. There is concern that, if taken together, these factors could undermine the concept of strategic trade controls which are used by states in an effort to prevent the proliferation of weapons of mass destruction. The purpose of this paper is to examine the interplay between these factors and identify policy recommendations.

It is perhaps in the context of so-called 'intangible technologies' that the challenges of the balance between globalisation and control above are at their greatest. Intangibles are by definition, not physical goods. As such, they can more readily be carried or transmitted across borders – particularly with the worldwide growth of digital connectivity. There is a need to understand whether and how to control intangible technology. These are the questions that are of interest to this paper.

This paper proceeds as follows. First, an adapted version of the 'capability acquisition model' is presented. This model includes refinements over a previous version of the model utilised for earlier analysis of this topic. This updated model has been used to examine a series of case studies that are included in Part Two of this report and which inform the analyses in section 2 and 3. Section 2 of the report presents the analysis of intangible technology transfer (ITT). This analysis is structured under several headings, including 'electronic transfer' and in-person transfer. Section 3 presents policy recommendations and findings.

This paper has two parts. The first part presents and applies a conceptual model for capability transfer – the adapted Capability Acquisition Model. It also presents the main findings from having applied this model to around 10 case studies. Part 2 is self-contained in a separate document and presents each of the case studies in turn.

This part of the report (part 1) is structured as follows. First, the adopted capability acquisition model is presented. Second, the results of thematically examining the case studies are discussed. Third, policy recommendations are set out.

The main finding of this report is that controls in intangible technology, while imperfect, do play an important role in non-proliferation. A key challenge for governments and the major non-proliferation regimes is in optimising these controls and aligning the measures to complement other instruments. In this context, it is argued that a broader strategy is required in relation to intangible technology transfer control that goes beyond the bounds of the traditional work of the export control community. Because of this, new forums may be needed in order to address the ITT issue. The UN Security Council's resolution 1540 (UNSCR 1540) mechanism may present one option.

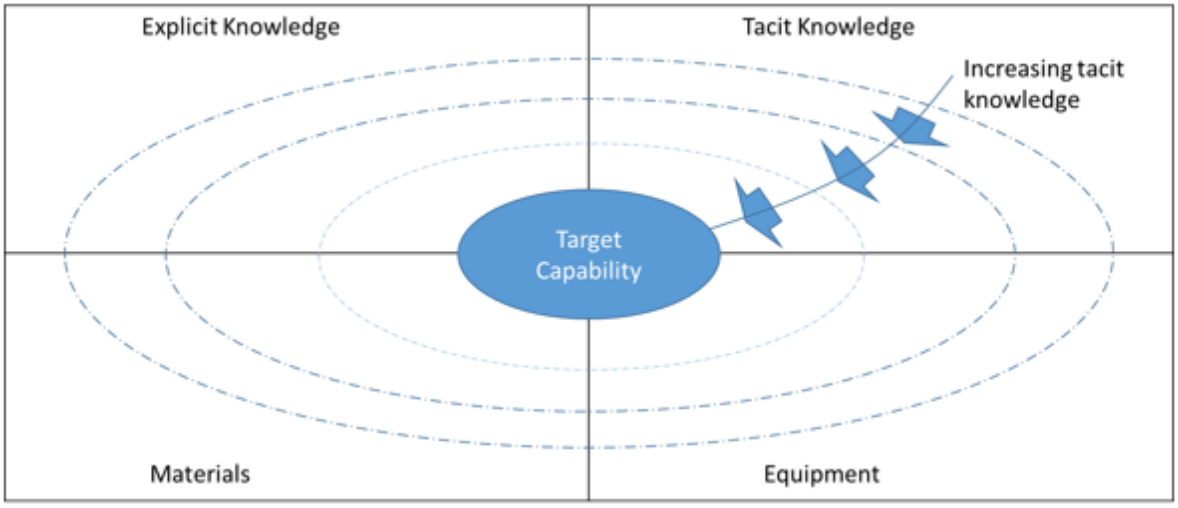
In parallel to pursuing a broader strategy, however, several steps that the export control community could take to help to mitigate the ITT issue are identified.

Section 1: The Adapted Capability Acquisition Model

This paper utilises the Capability Acquisition Model previously developed by the author.[1] The Capability Acquisition Model draws upon existing theories from the knowledge management discipline. The model is based upon the simple observation that to produce any item, several prerequisites must be brought together in a certain way. These prerequisites include equipment, materials, and information, where information can be split into 'tacit' and 'explicit' information. The model also reflects the fact that simply having each component is not enough: it is usually necessary to iteratively advance the capability towards production of the end product.

In practice, for strategically-important items, there are usually barriers to the acquisition of these elements, meaning that capability acquisition takes place iteratively over a period of time. This relates not only to export controls, but also to the nature of tacit knowledge, which cannot easily be transferred via impersonal means. It also relates to the natural desire of companies to protect their intellectual assets (including intellectual property) and market share.

Figure 1. Original Capability Acquisition Model



The author has previously applied this model to a case study related to Chinese efforts to indigenise the production of carbon fibre. In that case, the model was utilised to understand the substantial barriers that exist to the production of carbon fibre in China – a country that had prioritised indigenisation of carbon fibre production as part of its 2011 five-year plan.[2]

The study showed that Chinese firms have legitimately employed a number of techniques to acquire the various prerequisites for producing carbon fibre, including procuring equipment from overseas; buying out overseas firms; and hiring consultants and outside experts.

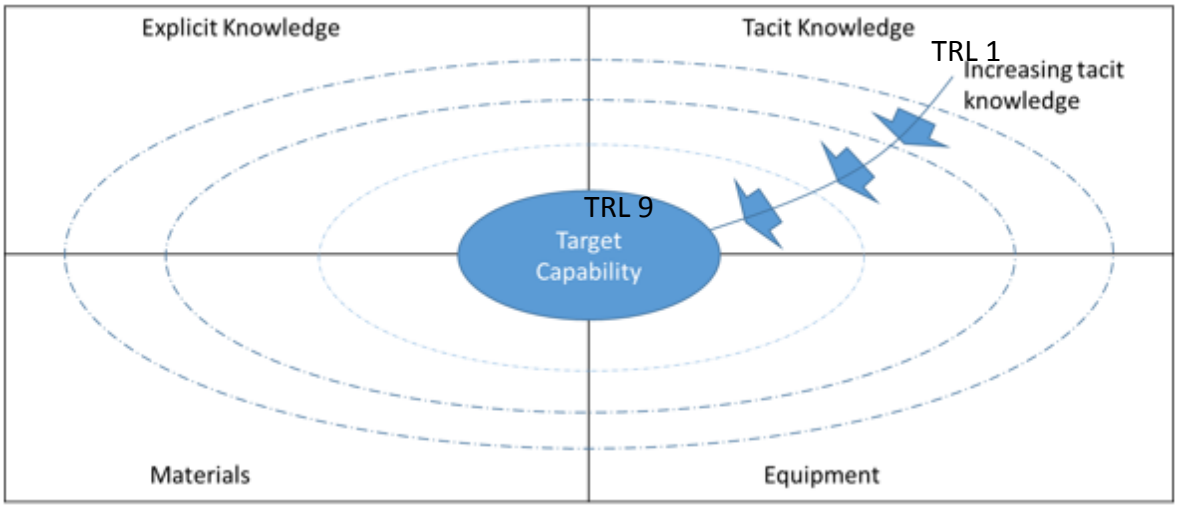
[1] Stewart, Ian. "The Contribution of Intangible Technology Controls in Controlling the Spread of Strategic Technologies". Strategic Trade Review, Edition 1. Available online at: http://www.str.ulg.ac.be/current-issue/ (Accessed 07/02/2016)
[2] Ibid.

However, despite substantial investments, Chinese producers have not succeeded in mastering production of anything beyond the most common industrial grades of carbon fibre in quantities larger than batch size. Interviews with sectoral experts highlighted that the key barrier was bringing together all of the components to produce the final item. Shortcuts could not be taken to reach the desired end step: instead, it would be necessary for Chinese producers to progressively improve production over a period of time. This supports the idea of 'iteration' as included in the capability acquisition model.

A further refinement of this model emerged during the course of the research leading to the production of this paper. This involved the integration of the 'technology readiness levels' (TRL) model. It has become increasingly common for an industry, academia, and governments to assess the maturity of technology based upon the TRL concept. The TRL concept was first developed by NASA in the 1970s in order to provide insight into how far advanced a technology was for the purpose of deploying it in the United States space programme.[3] The TRL concept has since been incorporated in a wide variety of other domains, including the EU's Horizon 2020 research programme.[4] The TRL is shown below with the corresponding levels used by the EU's Horizon 2020 programme.

Integration of the TRL concept to the Capability Acquisition Model is relatively straightforward - at least conceptually. The 'target capability' is evidently TRL 9; TRL 1 is the outer ring on the CAM diagram (see below).

Figure 2. Adapted Capability Acquisition Model



[3] "Technology Readiness Level" NASA Website. Available online at https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html. (Accessed 26/05/2016)

[4] Horizon 2020 is the financial instrument implementing the Innovation Union, a Europe 2020 initiative aimed at securing Europe's global competitiveness. It is the biggest EU research and innovation program that has ever existed. €80 billion of funding is to be made available over seven years (2014-2020). This figure does not include any additional private investment that will be attracted.

A key reason for integrating TRLs into the CAM model is that it allows the model to be used to consider the contribution of research and development to the acquisition of a capability. This is particularly important in relation to intangible technology controls, as research and development can fall within the scope of controls as currently drafted – but the nature and scope of these controls is generally poorly understood. A particular challenge in this context is that a decontrol (an exemption to controls) exists for “basic scientific research”. Basic scientific research is thus exempted from export controls, despite this being an often loosely-defined or poorly-understood concept.

Table 1: Overview of Technology Readiness Levels

	NASA[5]	EU Horizon 2020[6]
TLR 1	Basic principles observed and reported: Transition from scientific research to applied research. Essential characteristics and behaviours of systems and architectures. Descriptive tools are mathematical formulations or algorithms.	Basic Principles Observed
TLR 2	Technology concept and/or application formulated: Applied research. Theory and scientific principles are focused on specific application area to define the concept. Characteristics of the application are described. Analytical tools are developed for simulation or analysis of the application.	Technology Concept Formulated
TRL 3	Analytical and experimental critical function and/or characteristic proof of concept: Proof of concept validation. Active Research and Development (R&D) is initiated with analytical and laboratory studies. Demonstration of technical feasibility using breadboard or brass board implementations that are exercised with representative data.	Experimental Proof of concept
TRL 4	Component/subsystem validation in laboratory environment: Standalone prototyping implementation and test. Integration of technology elements. Experiments with full-scale problems or data sets.	Technology Validated in lab
TRL 5	System/subsystem/component validation in relevant environment: Thorough testing of prototyping in representative environment. Basic technology elements integrated with reasonably realistic supporting elements. Prototyping implementations conform to target environment and interfaces.	Technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 6	System/subsystem model or prototyping demonstration in a relevant end-to-end environment (ground or space): Prototyping implementations on full-scale realistic problems. Partially integrated with existing systems. Limited documentation available. Engineering feasibility fully demonstrated in actual system application.	Technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 7	System prototyping demonstration in an operational environment (ground or space): System prototyping demonstration in operational environment. System is at or near scale of the operational system, with most functions available for demonstration and test. Well integrated with collateral and ancillary systems. Limited documentation available.	System prototype demonstrated in operational environment
TRL 8	Actual system completed and "mission qualified" through test and demonstration in an operational environment (ground or space): End of system development. Fully integrated with operational hardware and software systems. Most user documentation, training documentation, and maintenance documentation completed. All functionality tested in simulated and operational scenarios. Verification and Validation (V&V) completed.	System complete and qualified

[5] "Technology Readiness Level", NASA Website. Available online at https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html (Accessed 02/02/2016).

[6] Technology readiness levels (TRL), Horizon 2020 – Work Programme 2014/2015: General Annexes. Available online at: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf (Accessed 02/02/2016).

TRL 9	Actual system "mission proven" through successful mission operations (ground or space): Fully integrated with operational hardware/software systems. Actual system has been thoroughly demonstrated and tested in its operational environment. All documentation completed. Successful operational experience. Sustaining engineering support in place.	Actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

Section 2: Examining Intangible Technology Controls

The purpose of this section is to examine the need and opportunity for controls on intangible technology. This section uses as its starting point the conceptual model presented in the previous section. It also utilises the results of the examination of numerous case studies, which are presented in the appendices and summarised below. After providing an overview of the case studies, this section examines issues around explicit knowledge transfer and tacit knowledge transfer.

Overview of case studies

Several cases involving the transfer of intangible technology were examined in the course of this research and are presented in Part 2 of this report. The case studies were selected to allow for the exploration of different aspects of intangible technology control.

Where relevant, the adapted Capability Acquisition Model was utilised to examine the case study. In some cases, this allowed an assessment to be made about both the export control status of the case and about the technology readiness level involved in the export. It should be noted that these assessments cannot be taken as definitive. There are several reasons for this. This includes the limited amount of information available in the public domain on each case and the fact that researchers might 'undersell' or 'oversell' the policy impact of their work.

The purpose of examining the case studies was to identify lessons for the design and implementation of controls on ITT. In keeping with the conceptual model presented in the last section of this report, it is helpful to explore these issues from the perspective of explicit knowledge and tacit knowledge.

Table 2: Overview of Case Studies

Case study	Type	TRL	Export control status	Description
1.1	Nuclear	1-2	Not listed	Several project between UK Universities and Indian nuclear entities, including the Bhaba Centre for Atomic Research
1.2	Nuclear	7	Not listed	Nuclear fuel evaluation undertaken in Norway on behalf of the Brazilian Navy.
2	Cloud Computing	N/A	N/A	Examination of possible proliferation impact of cloud computing.
2.1	Computing as a service			
2.2	Cloud storage			
3	Additive Manufacture	N/A	N/A	Examination of intangible technology transfer issues associated with additive manufacturing.
4	Research Cooperation	1-4	Not Listed	Several cases involving UK university collaboration with Chinese aerospace entities (some of whom have been linked to ballistic missile programs of concern).
5	Deemed export and public domain information		Listed	An American academic allowed his Chinese student access to export-controlled information and presented findings of export-controlled research in China.
6	Education	N/A	N/A	'Dr Germ', who was educated in the UK before returning to Iraq to work on Iraq's biological weapons programme.

It is helpful to utilise these case studies with reviewing each component of the CAM.

Explicit Knowledge

The principal control on intangible technology according to the definitions of the export control regimes is focused on what would be described as 'explicit knowledge'. Specifically, the export control regime's definition of technology means: "specific information necessary for the development, production or use of goods or software" where the EU control list also includes the following Technical Note: "Information may take forms including, but not limited to: blueprints, plans, diagrams, models, formulae, tables, 'source code', engineering designs and specifications, manuals and instructions written or recorded on other media or devices (e.g., disk, tape, read-only memories); 'source code' (or source language) is a convenient expression of one or more processes which may be turned by a programming system into equipment executable form".[7]

[7] "Export License". UK Government Website. Available online at http://blogs.bis.gov.uk/exportcontrol/files/2015/10/15-176-ogel-access-overseas-military.pdf. (Accessed 26/05/2016).

Based upon these provisions, it is evidently electronic information and printed information that is of principal interest according to the lists of the export control regimes. It is thus helpful to consider what insights the case studies provide in terms of both types of information.

It should also be noted, however, that the export control regimes make certain exemptions, which are relevant in relation to the explicit categories of information. The first concerns information in the public domain. A second concerns 'basic scientific research'. Of the two, it is argued that the public domain formation decontrol is more relevant to explicit knowledge transfer whereas the basic scientific research decontrol is generally more relevant to tacit knowledge transfer.

ITT and Explicit Knowledge

Several of the case studies presented in Part 2 and summarised in table 2 above involve the transfer of knowledge in its explicit form. Examining the case studies highlighted several general observations.

First, from examination of several case studies, it is apparent that explicit knowledge alone is not sufficient to achieve a capability to produce an item of concern. Even in additive manufacturing processes where it could be expected that the need for tacit knowledge of manufacturing processes is less, it was found that tacit knowledge was a vital prerequisite. In that case, tacit knowledge was required both when creating a design and setting up the additive manufacture equipment to produce an item.

Second, while explicit information cannot be used to produce an item in isolation, certain explicit information is of high concern from a proliferation perspective and should be subject to control. Perhaps the most crucial examples include designs for a nuclear weapon. While a design is only a starting point for a would-be proliferator, it is evidently desirable to prevent proliferators from accessing designs. It may also be appropriate to criminalise possession of nuclear weapons designs in a similar way to how some states prohibit possession of information useable in terrorism.

Some might argue that controlling such designs is unnecessary because proliferators could not know for certain whether the designs that they were obtaining were functional (rather than amateur efforts or fabrications). However, there are dangers with this. Proliferators might quickly be able to identify and address flaws with designs based upon either their own tacit knowledge or on tacit knowledge provided through technical assistance from outside the state. Additionally, advancement of computer modelling and simulation might allow for the identification and correction of issues after the fact.

Third, and by extension, information in the public domain can be of proliferation value. Once information is in the public domain, however, it can be inherently difficult to prevent the onward transmission of knowledge. There is thus a strong rationale for the public

domain decontrol. Outreach and enforcement action against individuals who inadvertently or incorrectly put information into the public domain is vital, however, if explicit information is to be controlled. In practice, however, because explicit information is of limited value in its own right, it is valid to focus such actions around technologies of highest concern – at least in the first instance. Moreover, in practice, this might mean focusing on military and single-use technology rather on dual-use goods.

Finally, in some cases, it might be possible to have information removed or hidden from the internet.

Nonetheless, it is evidently desirable to control nuclear weapons designs and other non-electronic information of high proliferation concern. Moreover, electronic information transmitted through physical format is evidently as potentially damaging as information transmitted electronically. Therefore, it seems apparent that some form of graduated scheme is required. One possible scheme is presented below.

	WMD-related	**Single Use**	**Dual-use**
Printed materials (Exempt from public domain decontrol)	X		
Printed materials		X	X
Stored data (i.e. not printed)	X	X	X

This graduated approach would see efforts to keep information that is WMD-related (defined below as TRL 6-9) out of the public domain and the public domain decontrol would not apply. Printed materials would continue to be controlled unless the information was already in the public domain. Controls on electronic data would continue.

Electronic Transfer

Electronic information is evidently difficult to control. While electronic information is a form of explicit knowledge and thus cannot be used to manufacture items on its own, the general trend in society is to have larger datasets and partially automated processes for both design and manufacture. The need for high quality standards for materials and products will continue to limit the usability of 'generative design' technologies for the foreseeable future. Nonetheless, risks that large datasets containing proliferation-sensitive information will only grow unless urgent and systematic action is taken.

Challengingly, the export control dimension of such transfers is only one part of this problem: cyber intrusion and theft might target export controlled information, but it is the remediation against risks which are outside of the usual domain of export controls.

At present, export controls are primarily used to manage intentional transfers by exporters rather than to prevent theft. There are evidently also challenges for export control

authorities as electronic information cannot be readily detected at the border. It is also not typically the role of signal intelligence organisations to monitor export compliance by companies.

A practical solution that could help to manage both challenges relates to information security standards. Presently, there is generally no requirement for companies to implement a set IT security standard for export control reasons outside of key jurisdictions, such as the United States. However, certain standards are commonly adhered to in industry that includes standards related to information security. For example, the Authorised Economic Operator (AEO) standard has an IT security component.[8] Another standard – Payment Card Industry (PCI) – exists and is widely implemented to protect personal information and payment details on the internet. Such standards, if combined with an export control internal compliance program – can go a long way towards ensuring the adequate protection of electronic information against both authorised export and theft. Licensing and enforcement authorities, should, therefore, consider how to encourage firms to take up such measures and should ensure that the measures are appropriately implemented during audits and inspections of the company. A requirement could thus be introduced that firms holding controlled technology in an electronic form must either be AEOs or subject their IT infrastructure to the requirements of AEO. Another possibility would be to leverage tools created to ensure adequate protection of personal data. Presently, any company holding personal data in the UK, for example, must take adequate measures to ensure that it cannot be accessed by unauthorised persons. An industry standard 'PCI' compliance standard has been developed in relation to this requirement.[9] A separate ISO standard - ISO/IEC 27001 - information security management – has also been developed.[10]

Payment Card Industry Data Security Standard – High Level Overview[11]

Build and maintain secure network and system	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system password and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs

[8] World Customs Organisation, 'WCO SAFE Package'. Available online from http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/safe_package.aspx (Accessed 29/01/2016).
[9] PCI Security Standards Council, 'PCI Security'. Available online at: https://www.pcisecuritystandards.org/pci_security/standards_overview (Accessed 29/01/2016).
[10] ISO/IEC 27001 - Information security management, available online at: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (Accessed 01/02/2016).
[11] PCI Data Security Standard: Requirements and security assessment procedures: version 3.1, April 2015

	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

The PCI Data Security Standard is mandatory for all firms handing payment data (i.e. credit card information). In principle, it would seem that this standard could easily be extended to firms handling export controlled information. Another possibility would be to create a customised standard for the handling of technology in an electronic form. This would be a time-consuming process, however, and it is not clear whether the investment required would be worth it, given the relatively few firms that are likely to hold such information. The final approach would be to leave it to companies to demonstrate that adequate measures have been taken. Such checks could be undertaken during compliance audits. In conclusion, therefore, it appears that while questions are raised about the implications of cloud computing for export controls, they are largely not new. The same questions can – and indeed should – be asked with regard to more traditional computer storage mediums. Consideration should therefore be given to setting an information security standard for all firms that hold controlled technology in an electronic form. Such guidance should be applied regardless of storage medium.

Non-Electronic Transfer

The control list definitions extend to information in forms other than electronic (i.e. physical copies of hard-copy blueprints, written reports, CDs, DVDs, and so on). In a computerised age, the importance of this category is likely to be declining. Indeed, it seems likely that the majority of materials printed today would be reprinted for publication and thus will belong to the public domain (and therefore exempt from controls). Despite this, companies might well have printed reports, manuals, and designs that contain export-controlled information for their own purposes. As a result, it is foreseeable that transfers of export controlled information in printed form will continue to take place.

The CAM module suggests that the contribution of any such material to the act of proliferation is likely to be limited. Reading a manual or viewing a blueprint does not provide the tacit knowledge required to produce a part.

Evidently, the measures explored above, while contributing to efforts to prevent proliferation by controlling intangible technology transfer, go beyond the bounds of export

controls into the open dissemination of knowledge. These matters will inevitably raise issues concerning freedom of speech.

Tacit Knowledge

The definition of technology used by the export control regions extends to 'technical assistance', which it states 'may take forms such as instructions, skills, training, working knowledge, and consulting services'. Technical assistance, by this definition, can be considered a mechanism through which to transfer tacit knowledge. Tacit knowledge is viewed in academic literature as being difficult to transfer via impersonal means. Although not impossible, transferring tacit knowledge impersonally, from one person to the next, is often time consuming or expensive. Apprenticeships are usually undertaken over the course of several years, for example, and it can take many more years to achieve mastery of the craft.

The importance of tacit knowledge to proliferation should not be underestimated. A key barrier to capability transfer is the difficulty in acquiring tacit knowledge, as the carbon fibre case study demonstrated. Tacit knowledge can be developed (rather than obtained through transfer), but this can also be a slow process requiring a solid understanding of the basics of a discipline and a process of trial and error to evolve designs and build knowledge.

Technological advancement might lessen the barriers to transferring tacit knowledge. It might be that some tacit knowledge can be transferred by video, for example, and services such as Skype might allow for tacit knowledge transfer where individuals are not physically in the same room. However, there are few signs that the barrier posed by tacit knowledge transfer will disappear. For example, even in relation to additives manufacture technologies, the tacit knowledge requirement is still significant despite the fact that designs can be packaged into digital build files. This is because machine and performance settings must be set, taking into account issues related to the nature of the specific material or alloy being used, environmental issues, and even the actual (rather than theoretical) performance of each specific machine.

Insights on Tacit Knowledge Transfer from the Case Studies

Several of the case studies included in the appendices and summarised in table 2 above involved activities that could result in transfers of tacit knowledge. The separately-published case study on Chinese efforts to indigenise carbon fibre production also demonstrated the use of numerous mechanisms that can result in tacit knowledge transfer.

It should be noted that, in addition to being difficult to transfer, tacit knowledge is also highly context-specific. Applying tacit knowledge from one application to another will generally require an additional phase of learning, perhaps involving experiments or trial and error method. This is important in relation to the types of assistance that might take place. It is helpful to conceptualise these types of transfer as direct (TRL 6-9), indirect (TRL 4-5), and basic (TRL1-3).

Direct

Tacit knowledge transfer that is of direct relevance to WMD proliferation could take place. However, such transfers of tacit knowledge are likely to have certain features, including perhaps involving government-linked (or former) engineers and scientists as it is generally these individuals that would have the context-specific tacit knowledge that is relevant for WMD.

The main policy measures that can mitigate this risk are:

- Centralised controls to ensure that the different apparatuses of the state (i.e. the military or military-linked industrial complex) do not enter into foreign cooperation on WMD-related activities.
- Outreach to current and former scientists involved in WMD-related programs.
- Measures to criminalise citizens when outside the state if they aid another state in acquiring WMD. The UK implements such extraterritoriality, as UK law prohibits aiding another country to acquire enrichment capabilities.

Indirect

Indirect cases are less clear cut. The tacit knowledge required will generally be less applicable and therefore is dual-use in nature. Additionally, the number of fora in which such tacit knowledge transfer could take place – as well as the number of mechanisms that could be used - is greater. The case studies included several cases in which contracted research might have led to tacit knowledge transfer. Additionally, the Dr. Germ case study highlights that educational programmes have been used to acquire such indirect tacit knowledge.

The main policy measures that can mitigate the risks of tacit knowledge transfer aiding proliferation in this category are visa vetting schemes, deemed export controls, and technical assistance controls.

Visa vetting schemes

Such schemes involve the systematic or semi-systematic examination of visa applications order to identify potential WMD concerns. Such schemes can be informal in nature. The number of states operating visa vetting schemes is difficult to identify precisely as at least some states are known to operate ‘informal’ schemes. Informal schemes can involve visa processing staff referring on cases when either suspicions are raised or when the application lists individuals or activities of concern (i.e. ‘nuclear’). More formal schemes also exist, such as the UK’s Academic Technology Approval Scheme (ATAS) scheme. The ATAS scheme, which is descried in annex 1 and 2, is one of the most systematic schemes operated by any country. However, the ATAS scheme is limited in scope in that it mainly addresses certain post-graduate courses.

Deemed Export Schemes

Some states – notably the United States – implement so-called 'deemed' export controls. These schemes make transfers of controlled information (including tacit knowledge) controllable to foreign nationals anywhere in the world. For example, if a Brazilian national was to tour a factory making controlled items in the United States, an authorization would be required. Given the importance of tacit knowledge in capability transfer, such schemes can be an important element of a non-proliferation system. However, states have been reluctant to adopt such controls. One reason for this is that administrative burden that the measures imply.

Technical Assistance Controls

Some states have controls on technical assistance. These controls tend to be an extension of the 'catchall principle' in that they are applicable when the exporter knows or has been informed about a WMD end use. Such mechanisms can be helpful in preventing tacit knowledge transfer when information or intelligence comes to light about a true end use. They can thus be a helpful deterrent and an important fallback measure even if the measures tend not to be used often.

Basic Scientific Research

The export control regimes include decontrols for "basic scientific research". As the first case study in part 2 of this report (related to UK/India Nuclear research) highlights , it is critical to have a clear understanding of this term and the scenarios to which it applies. If the term is interpreted too narrowly, it can interfere with low-risk research collaboration. If it is interpreted too broadly, it can allow for the uncontrolled transfer of technology that is relevant to WMD or other applications of concern.

In practice, as the case studies in part 2 demonstrate, implementation of the basic scientific research decontrol appears to lack consistency. A key reason for this inconsistency is that there is a lack of understanding about what constitutes basic scientific research under the prescribed definition. The definition given in the EU control list is relatively vague:

> *'Basic scientific research* [according to the general technology note and the nuclear technology note] *means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.'*[12]

[12] European Commission, ANNEX to the Commission Delegated Regulation amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items, Brussels, 12.10.2015. Available online at: http://ec.europa.eu/transparency/regdoc/rep/3/2015/EN/3-2015-6823-EN-F1-1-ANNEX-3.PDF (Accessed 05/02/2016).

Increasing understanding and consistency of implementation around this definition would be advantageous as it would help to improve the consistency of export control implementation. It may also help to ensure that potentially problematic technical projects are appropriately managed. However, in order to be useful, it is argued that any updated definition must be widely socialised in the academic community and in governments as well as being correctly understood. A prime reason for seeking to integrate TRLs into the CAP is that TRLs meet this criterion: the TRL schema is used widely in industry and has been incorporated into the EU Horizon 2020 programme.

An important limitation to TRLs is that there is no international standard associated with them. As such, the terms and metrics used can vary from one organisation to another. Despite this, the structure of all TRL models tends to be the same. Generally, there are always nine distinct levels in a TRL model. Two examples were set out in table 1 in section 1 of this report.

Examining the definitions of 'basic scientific research' and the TRLs together highlights the following issue: while TRLs are intended to capture the readiness of a technology for a specific end use, the definition of basic scientific research, applies only where the basic scientific research is 'not primarily directed towards a specific practical aim or objective'.[13] It could thus be argued that, by the current definition of basic scientific research, research at any TRL level relevant to a controlled item could itself be considered subject to control. However, given the low direct utility of TRLs at, for example, levels 1 to 3, this would likely result in the control threshold being set too low in a majority of cases.

An alternative approach would be to change the definition of basic scientific research to indicate that it applied only when the TRL level in relation to controlled technology was below a certain TRL level, thus ensuring that concept development was not subject to control, whereas prototyping and complete systems would be subject to control. Non-proliferation purists might find this approach problematic, as it could enable programmes of concern to draw upon researchers for concept development.

This in turn raises the question of at what TRL level would the basic scientific research decontrol stop applying. In general, it could be argued that TRL 4 should not be exempt because it involves 'technology validation' – i.e. steps to ensure that the capability being produced would be suitable for the envisioned end-use. Another argument would be that TRL 5 should not be exempt, as this would involve validation of the technology in a relevant environment.

For single-use technologies, such as nuclear weapons, it is apparent that TRL 3 - 'proof of concept validation' - should be subject to control. It could thus be argued that for a defined list of technologies, an even lower TRL threshold should be set – perhaps at TRL 3.

---

[13] "Export control legislation for UK academics and legislators", UK Government Website. Available online at https://www.gov.uk/guidance/export-control-legislation-for-uk-academics-and-researchers. (Accessed 26/05/2016).

A key question in relation to the application of TRLs for export control purposes would be: technological readiness … for what? As they are traditionally applied, TRLs are used to indicate the level of readiness of a technology for a specific application. For example, TRLs could be used to indicate the readiness of a composite/resin system to be used in the construction of a rocket wing. In the export control context, it could be argued that TRLs should be assessed against all items on the control list. However, this might be very burdensome for industry and academia as it would require researchers to understand how their work could contribute to technology on the whole of the control list. An alternative would be to say that the assessment should be made against only the intended end-use or where a WMD end-use is known or suspected. This approach might be particularly appropriate given that higher technology readiness levels must intrinsically be related to only a very specific intended application.

The question of at what TRL the control threshold should be set is both a policy and a political question, in addition to being a technical one. Therefore, the goal of this paper is to inform a debate about at what level – if any – the control threshold should be set rather than presenting a specific position or solution.

Section 3: Policy Recommendations

In the preceding section's analysis of the case studies in the context of the capability acquisition model, how different types of control measure can contribute to controlling proliferation through intangible technology transfer is highlighted. Given the factors of globalisation, it is apparent that no system of control can be fool proof. Instead, the goal of this study has been to identify risk-based control mechanisms.

The use of the capability acquisition model and technological readiness levels has proven to be a helpful tool in the course of this review. Indeed, the utility of the TRL concept in reviewing the case studies suggests that the TRL framework is a useful tool for evaluating what is meant by 'basic scientific research. One recommendation resulting from this study, therefore, is that the TRL model be used as one tool when considering whether the basic scientific research de-control applies. It would be for each country to decide what TRL might act as a threshold, but the author is of the view that TRL 4/5 is appropriate.

A. Towards a broader Strategy

Having examined the issue of proliferation through intangible technology transfer as well as the main controls that can be used on ITT, it is apparent that many of the potential policy tools do not fall within what is traditionally thought of as the export control toolkit. Instead, a broader toolset is required if ITT is to be effectively managed. This implies that the export control regimes might not be the optimum forum through which to address the ITT issue and raises the question of whether some other forum exists that is better suited (or at least complementary to) the regimes in relation to ITT.

A principle forum might be the UNSCR 1540 mechanism. Resolution 1540 of 2004 is binding on all states and has export control provisions. However, it also requires states to take other measures to prevent proliferation of WMD to states and terrorists, including with regards to domestic transfer (as opposed simply to export). A comprehensive review of 1540 is currently underway. Consideration should thus be given to how 1540 can be leveraged to control proliferation through ITT. In practice, it is likely that the regimes will also play a role – hence the need for a broader strategy on managing proliferation through ITT.

B. Export Control Actions

i. Scope and Definition

The capability acquisition model and the case studies highlights that the traditional concept of export controls as measures to prevent the physical transfer of goods is increasingly outmoded. Controls on physical transfer continue to be an important component of the non-proliferation regime. However, globalisation and technological advancement mean that effectively controlling intangibles – explicit and tacit knowledge – is as important as

controlling physical goods. Challengingly, however, the traditional view of export controls is not particularly compatible with the objective of controlling intangibles as intangibles are not exported in the traditional sense.

ii. List-based export controls

The case studies included activities of possible proliferation concern that were not expressly listed on the lists of the export control regime. Surprisingly, this includes 'technology' (i.e. designs) for nuclear weapons and stainless steel nuclear fuel cladding technology. While it might seem redundant to include nuclear weapons on the lists of the export control regimes, such an inclusion is potentially important. Should a nuclear weapons design ever be leaked, for example, a control on 'technology' associated with design would provide a legal instrument to take remedial action against individuals if this design transferred from the country. Another issue highlighted in the case study was in relation to stainless steel nuclear fuel cladding. Such fuel cladding is typically used in submarine reactors. As stainless steel cladding is not listed on the list of the NSG, 'technology' related to fuel cladding for nuclear submarines might fall outside the scope of control.

These issues are evidently partly a result of the list-based approach taken by the export control regimes. The lists for various reasons can never be complete. However, in relation to 'technology', the effect of omissions might be more pronounced because of the loss of control associated with explicit and tacit knowledge. This is particularly important in the context of electronic transfer and technical assistance.

iii. Electronic Transfer

Electronic data transfer is perhaps the most rapidly evolving topic to be examined in this paper. It is evidently the case that export-controlled information in electronic form can be transferred more rapidly today it could have even 10 years ago. Additionally, the risks of proliferation of electronic information appear to be increasing as the threat of cyber intrusion increases. Additionally, as was highlighted in the previous section, however, the term 'export' is becoming outmoded when it comes to electronic information, as information is vulnerable whether it is stored on servers outside of the country or within the country.

As a result of these factors, it is argued that states should require companies to meet certain basic information security standards when storing export controlled information in electronic form – whether or not it is subject to export.

Additionally, to deter individuals from deliberately putting export controlled information into the public domain in an effort to evade export controls, states should adopt laws that could penalise this if it is shown that the individual acted willfully or negligently.

iv. Technical Assistance Controls

While potentially beyond the scope of export controls in the traditional sense, consideration should also be given to creating a 'WMD technical assistance control' that would state that

it should be expressly stated that 'technology for design, development and use of nuclear weapons is subject to control' prohibit citizens from providing assistance to WMD programs anywhere in the world. The extraterritorial nature of such a control would be difficult to enforce. However, this would plug a clear gap in the non-proliferation regime.

If controls continue on A4 goods, consideration should be given to whether authorisation is required before EU and Non-EU citizens can access the technology

C. Visa Vetting Schemes and Deemed Export Controls

There is a clear need for states to have in place a scheme to identify any known proliferation concerns with persons entering their jurisdictions. This is a binding requirement of certain UN Security Council resolutions. It is also one way in which states can implement controls on technical assistance in relation to tacit knowledge transfer in the state's territory.

The variability and lack of harmonisation between states on vetting schemes is a potential gap in the non-proliferation regime. As the coordinate implementation of a vetting scheme has counter terrorism as well as counter proliferation virtues, this would appear to be an area in which progress could be made in the current global climate. There are key challenges that might frustrate more complete implementation of vetting schemes, however, including the variation in legal basis and the fact that, at present, organisations responsible for export licensing often have no responsibilities in regards to visas.

At the very least, measures should be in place to control technology transfer when a WMD end-use is known or suspected

- Ability to refuse / cancel visas
- States should be required to have in place processes to review visa applications for possible WMD / sanctions violations and should notify partner countries when visas are refused / revoked
- Consideration should be given to a standardised approach across the EU
- Universities and companies should ensure that staff, students, and visitors have valid visas before allowing them access to export controlled information

D. Guidance for Enterprise

In the course of this review, it has become apparent that enterprise (industry, business and academia) face a difficult task in remaining compliant with intangible technology controls. In some areas, there is a need for authorities to clarify issues related to definition and scope. However, even with increased clarity around key issues, implementation of controls on ITT in enterprise will remain a challenging topic. It is therefore vital that authorities work with

enterprise to develop guidance that is both in line with legal requirements and practical to implement. Ideally, any such national guidance should be discussed in the appropriate international forums with a view to coordinating national guidance at the international level.

The guidance document for UK Higher Education Institutions on Export Controls and the ATAS Student Vetting Scheme is an example of the type of document that could be produced by national authorities.

States should be prepared to respond to requests from industry and academia about ITT classification

It should be recognized that universities have a different structure than companies:

- It should be recognized that, in an academic environment, the responsibility of the University is to inform its staff about the export compliance obligation.
- It is the responsibility of the academic, with the support of the university, to apply for authorisations as necessary.

Companies contracting research institutes to conduct research on controlled technology have a responsibility to:

- Inform the research institute of the control requirement
- Include appropriate language in the contract to ensure that the technology is appropriately managed

Conclusions

Part 1 of this report has thematically examined the case studies contained in part 2 using the adapted capability acquisition model. From this examination, it is apparent that export controls as currently constituted are poorly suited to the task of managing intangible technology transfer.

Given the importance of intangible technology transfer in proliferation, it is desirable to address the limitations of the current approach. It is recognised, however, that any strategy to do so much be both risk based and targeted given the ever increasing movement of information and people that is being witnessed as a result of globalisation. A risk based and targeted approach is also required to balance the need for control with the imperatives of free speech, freedom of movement and so forth.

The issues raised in this report go beyond the competence of the export control community. As such, any such strategy would have to engage a plethora of stakeholders. One forum that might be well suited to this task is the UNSCR 1540 mechanism. Resolution 1540 does require states to adopt appropriate and effective measures to prevent WMD proliferation through intangible technology transfers. Given the dual-mandate of the resolution in preventing WMD proliferation and preventing WMD terrorism, and given the fact that the resolution is binding on all states, adoption of measures through the 1540 mechanism could go a long way to setting international standards in relation to ITT issues. It is timely to consider reinforcing the mandate of the 1540 committee in relation to intangible technology transfer given that a 'comprehensive review' of the resolution's implementation is taking place over the course of 2016.

Even if a forum for a broader strategy can be identified, certain additional measures that the export control community could take in order to address ITT issues have been identified. While some of these issues are for national authorities to consider rather than for the export control regimes per se, the nature of intangible technology transfer issues means that close cooperation at the international level is required if any national measure is to be effective. Consideration should thus be given to having a dedicated discussion on ITT issues in each of the regimes.

Annex 1: Overview of the UK's Academic Technology Approval Scheme (ATAS)

The Foreign and Commonwealth Office (FCO) operates the Academic Technology Approval Scheme. This is a scheme that is designed to help prevent the spread of knowledge and skills that could be used in the proliferation of WMD and their means of delivery. Similar schemes are operated by other governments worldwide.

The ATAS is designed to ensure that people who are applying for postgraduate study in certain subjects in the UK do not have already existing links to WMD programmes. The scheme requires that a student applying for particular subjects of study in the UK are required to apply for an ATAS certificate before applying for a student visa or extension.

Students who are not nationals of the UK, EEA or Switzerland (called ATAS-eligible students herein) may need to apply for ATAS certificates when studying towards any of the courses listed below.

It is the responsibility of universities to ensure that no student is enrolled on any course listed below unless they have received an ATAS certificate from the FCO for the specified course or verified that the student is exempt by inspecting documents that prove nationality. Failure to do so could result in the university's loss of ability to sponsor visas.

How does the process work?

The UK Border Agency will not issue visas for students to study on eligible courses until an ATAS certificate has been issued. Students must therefore apply for an ATAS certificate after receiving offers for a place at university and before making arrangements to travel to the UK (including application for a visa). The FCO aims to process ATAS applications within 20 working days.

What is the role of universities?

- Correctly assign the appropriate Joint Academic Coding System (JACS) code to all courses[14]
- Inform students of the ATAS certificate requirement when sending offer letters, and include on the offer letter the following information:
    - Course title and list of compulsory or optional modules
    - JACS Code
    - Instructions for ATAS application
- Verify that an ATAS Certificate is held before enrolling an ATAS-eligible student on any course that follows
- Ensure that a new certificate has been issued should the student decide change course

Implementation in practice

[14] JACS codes are used by the Higher Education Statistics Agency (HESA) and the Universities and Colleges Admissions Service (UCAS) to classify academic courses.

Existing student records systems provide the basis for ATAS implementation provided that academic departments correctly assign JACS codes to all courses. Student records systems should highlight to admissions staff all applications by ATAS-eligible students to ATAS-related courses. The system should prevent course registration until confirmation that an ATAS certificate has been linked to the student's record.

Which courses are ATAS eligible?

The boxes below list all ATAS relevant courses and their associated JACS codes.

<table>
<tr><td colspan="2">Taught Courses
Engineering and Sciences, with JACS codes beginning:
F2 – Materials Science
F3 – Physics (including Nuclear Physics)
H3 – Mechanical Engineering
H4 – Aerospace Engineering
H8 – Chemical, Process and Energy Engineering
J5 – Materials Technology not otherwise specified.</td></tr>
<tr><td colspan="2">Research Based Courses</td></tr>
<tr><td>Subjects allied to Medicine with JACS codes beginning:
B1 – Anatomy, Physiology and Pathology
B2 – Pharmacology, Toxicology and Pharmacy
B9 – Others in subjects allied to Medicine</td><td>Biological Sciences with JACS codes beginning:
C1 – Biology
C2 – Botany
C4 – Genetics
C5 – Microbiology
C7 – Molecular Biology, Biophysics and Biochemistry
C9 – Others in Biological Sciences</td></tr>
<tr><td>Veterinary sciences, agriculture and related subjects with JACS codes beginning:

D3 – Animal Science
D9 – Others in Veterinary Sciences, Agriculture and related subjects</td><td>Physical Sciences with JACS codes beginning:
F1 – Chemistry
F2 – Materials Science
F3 – Physics
F5 – Astronomy
F8 – Physical Geographical Sciences
F9 – Others in Physical Sciences</td></tr>
<tr><td>Mathematical and Computer Sciences with JACS codes beginning:

G0 – Mathematical and Computer Sciences
G1 – Mathematics
G2 – Operational Research
G4 – Computer Science
G7 – Artificial Intelligence
G9 – Others in Mathematical and Computing Sciences</td><td>Engineering with JACS codes beginning:
H1 – General Engineering
H2 – Civil Engineering
H3 – Mechanical Engineering
H4 – Aerospace Engineering
H5 – Naval Architecture
H6 – Electronic and Electrical Engineering
H7 – Production and Manufacturing Engineering
H8 – Chemical, Process and Energy Engineering
H9 – Others in Engineering</td></tr>
<tr><td>Computer Sciences with JACS codes beginning:
I1 – Computer Science
I4 – Artificial Intelligence
I9 – Others in Computer Science</td><td>Technologies with JACS codes beginning:
J2 – Metallurgy
J4 – Polymers and Textiles
J5 – Materials Technology not otherwise specified
J7 – Industrial Biotechnology
J9 – Others in Technology</td></tr>
</table>

Annex 2: Implementation of non-proliferation controls in universities

Note: this is an extract from a guide developed by King's College London and the Association of University legal Practitioners in partnership with the Department of Business, Innovation and Skills and the Foreign and commonwealth office. The guide is aimed at UK universities. This section is reproduced here as the guide might be relevant in other countries.

Universities must implement compliance systematically if ATAS and export control requirements are to be met.

Universities should implement a compliance system which adheres to the following good practices:

- Publish clear guidance on academic websites and intranets any existing ethical or legal policy or good practice on research and academic study. As a minimum, this could include:
    - The Export Control Decision Tree;
    - Links to this guidance document;
    - Links to the export control pages on the Businesslink website: http://www.businesslink.gov.uk/exportcontrol
- Incorporate export compliance considerations in all research ethics processes;
- Include reference to export control regulations in any training or induction of researchers and academic staff, and academic support teams or technology transfer teams in relevant academic disciplines
- Have a clearly published policy statement made by the university Principal or a Vice Chancellor on export controls and non-proliferation;
- Sign up to receive the Export Control Organisation's Notices to Exporters email, Twitter or RSS Feed notifications and the FCO's quarterly ATAS update;
- Provide a clear point of contact either within the legal department and/or other appropriate teams for export control queries and within the admissions hierarchy regarding the ATAS process;
- Provide a clear point of contact within the admissions / student records hierarchy for any ATAS-related enquiries;
- Ensure that academic departments apply the appropriate JACS code to both taught courses and postgraduate research.

All license applications should be made online via SPIRE, the ECO's export licensing database available at: https://www.spire.bis.gov.uk

www.projectalpha.eu