Emerging Technologies and the Challenges of Controlling Intangible Technology Exports

NITISH SURI[1]

Abstract

This article addresses the challenge of controlling emerging technologies in the absence of an objective mechanism that can provide for meaningful parameters to put them under a control list. A model is developed to identify parameters that determine technology controllability and also enable relevant score-based analysis to present decision makers with an assessment criteria of the proliferation risk of the emerging technologies. The Technology Proliferation Risk Score (TPRS) suggested in the article is determined through the parameters scored based on the data collected on relevant technologies from different sources. National governments can incorporate the TRPS model for risk assessment of technologies in their governance mechanisms to determine the controllability of technologies at early stages of emergence. Considering the vast potential of software and emerging technology transfers, it is pertinent that national export policies be ahead of their time to ensure nonproliferation due to export controls on high risk technology.

Keywords

Export controls, emerging technologies, proliferation risk assessment, intangible technology transfers

1 Nitish Suri is Deputy Director General of Foreign Trade. He is an Indian Civil Servant handling Indian export policy while working in Ministry of Commerce and Industry, India. He is from the Indian Trade Service and has several years of experience in implementing and formulating India's trade policy. He is also a U.S. Department of Energy Asian Export Control Fellow, 2019. The research and views expressed in this paper are personal and do not represent views of Government of India.

Introduction

International, multilateral, and regional instruments require countries to regulate the export, brokering, and transit/trans-shipment of military equipment and dual-use items. These regulations, referred to as dual-use and arms export controls, cover a wide range of physical goods, including conventional arms, Weapons of Mass Destruction (WMD) and their delivery systems, and conventional arms and WMD-related parts and components. In addition, they cover different types of software and technology—defined as including both technical data and knowledge and technical assistance—that is specially designed or required for the development, production, or use of controlled items. Controls on transfers of software and technology are generally considered to be an essential aspect of dual-use and arms export controls. Many of the items that are subject to control—particularly more complex and technically advanced conventional weapons—are less effective if the recipient does not have access to relevant software or technical data to enable or enhance their use. Knowledge and technical assistance can also be crucial to the successful production of certain types of WMD.

India has a robust export control system that is managed by the Directorate General of Foreign Trade (DGFT) in the Ministry of Commerce.[2] India is adherent to various international export control treaties and regimes. In particular, India has been a State Party to the Biological and Toxins Weapons Convention (BTWC) since 1974 and State Party to the Chemical Weapons Convention (CWC) since 1996. It is also a founding member of the IAEA and an active participant in nuclear safety and security instruments including safeguards implementation since 1971, under the agreement with the IAEA for the application of safeguards to civilian nuclear facilities (INFCIRC/754). Furthermore, India complies with United Nations Security Council resolution 1540, subscribes to the Hague Code of Conduct in June 2016, and is a member of all main multilateral export control regimes (the Missile Technology Control Regime, the Wassenaar Arrangement, and the Australia Group) with the exemption of the nuclear related ones (the Nuclear Suppliers Group and the Zangger Committee). However, India's export control list is fully harmonized with the control lists of all four multilateral export control regimes.

Export of commercial dual-use commodities, software, and technology is subject to controls as per the export control list of India (SCOMET - Special Chemicals, Organisms, Materials, Equipment, and Technologies). Section III under India's Foreign Trade (Development and Regulation) Act prohibits, restricts, or otherwise regulates the import or export of goods, services, and technology.[3] The DGFT has laid down the policy and procedure for export control for items listed in categories I-V and VIII of the SCOMET list.[4]

India has adopted trade controls for technology transfer under its SCOMET list and considering the volume of technology and software exports from the country, it is relevant for India to

---

2 "Export Control Guidelines – SCOMET Help," Directorate General of Foreign Trade, India, April 24, 2019, <https://dgft.gov.in/sites/default/files/SCOMEThelp24042019-converted.pdf>.

3 "Foreign Trade Development and Regulations Amendment Act," India, 2010, <https://dgft.gov.in/sites/default/files/Foreign_Trade_%28Development_%26_Regulations%29_Amendment_Act%2C_2010.pdf>.

4 Ibid.

have a robust mechanism in place to control intangible technology transfer both to companies and individuals outside India and also foreign nationals within India. The technology can more readily be carried or transmitted across borders especially due to rapid growth of digital connectivity. Emerging technologies pose further challenges to countries for controlling the transfer of intangible technology. There is a need to understand whether and how to control this and in India's context, adopt best and advanced global practices to counter this challenge. These are the questions this article tackles.

The focus on export control of intangible technology and software assumes significance in countries like India that export a huge volume of software products and services to almost all countries in the world. India's IT(Information Technology) and ITeS (Information Technology and enabled Services) industry grew to USD $181 billion in 2018-2019.[5] Exports from the industry increased to USD $137 billion in FY19 and out of that 21.80 percent of the total exports are of Research and Development Software products to around 80 countries.[6] The cloud market in India is expected to grow threefold to USD $7.1 billion by 2022 with the help of increasing adoption of Big Data, analytics, artificial intelligence, and the Internet of Things (IoT).[7] In such a scenario, it is pertinent to develop a robust system to mitigate the risk of proliferation of technology meant for non-civilian purposes.

This article focuses on emerging technologies and the suggested ways and means to control them and includes a broad strategy for technology transfer control to counter the risk of proliferation citing global best practices. Governments' export control policies associated with electronic transfers of technology are still developing.

The article is intended to identify the parameters for determining the proliferation risk to control intangible technology transfer with the emergence of new technologies, evaluate risk proliferation factors against each parameter, and identify policy recommendations, especially in the context of countries like India. The article also presents conclusions and recommendations focused on the steps that could be taken by the Indian government, companies, and research institutes to both streamline controls on transfers of software and technology and improve their effectiveness. These suggestions are intended to address some of the challenges and gaps identified by the article as well as steps that could be taken to develop a more harmonized approach on certain issues. Finally, the conclusions look at the need and potential to complement the application of export controls to software and technology with other governance tools, such as risk engines and end-to-end encryption and systems of self-regulation, particularly in the research field and academia. As a result, new national laws and international mechanisms might be required. However, adoption of effective mechanisms is likely to be controversial and therefore a need exists for a risk-based, targeted approach, as well as international cooperation.

---

5 "Key Findings in the Indian IT and ITeS Industry Report," India Brand Equity Foundation, September, 2019, <https://www.ibef.org/industry/information-technology-india.aspx>.

6 Ibid.

7 "Nasscom Cloud: Next Wave of Growth in India," Nasscom, August 2019, <https://www.nasscom.in/knowledge-center/publications/nasscom-cloud-next-wave-growth-india-2019>.

Technology and Nonproliferation Controls

The four major export control regimes all require their members to adopt controls on intangible technologies as well as on goods. The approach taken by the export control regimes has largely been to control the intangibles associated with technologies that are otherwise controlled. The designs for missile propulsion systems, for example, are likely to be considered controlled and thus cannot be exported without a license. Currently, intangible technology is defined by the Wassenaar Arrangement as:

> *"Specific information necessary for the development, production, or use of [controlled] goods or software" where... "information takes the form of technical data or technical assistance;" "Technical data may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories;" "Technical assistance may take forms such as instruction, skills, training, working knowledge, consulting services."*

Technical assistance may involve transfer of technical data as defined by the Wassenaar Arrangement. In India, paragraph 2(m) of the Foreign Trade (Development & Regulations) Amendment Act of 2010 defines technology as "any information (including information embodied in the software), other than information in public domain that is capable of being used in (i) the development, production and use of any goods or software (ii) the development of, or the carrying out of an industrial or commercial activity or the provision of service of any kind."[8] Section 13(2) and 13(3) of the WMD Act of 2005 provide restrictions on the transfer of technology. Section 13(2) clarifies that any transfer of technology of an item whose export is prohibited under the Act is prohibited. Section 13(3) specifies that when any technology is notified under the Act or any other relevant act, as being subject to transfer controls, the transfer of such technology shall be restricted to the extent notified thereunder.

Under SCOMET policy, transfer of any controlled technology is not allowed a) by a person or from a place within India to a person or place outside India; b) by a person or from a place outside India to a person, or a place, which is also outside India (but only where the transfer is by, or within the control of, a person who is a citizen of India, or any person who is a resident in India).[9] Hence, transfer of controlled technology to foreign nationals is barred by any person who is a citizen of India or any person who is a resident in India, even if it happens outside India.

It is mandatory for all companies and their subsidiaries registered in India and all other business entities operating in India and involved in the manufacture, processing, and use of Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) to obtain permission from the Directorate General of Foreign Trade before entering into any

---

8 "Foreign Trade Development and Regulations Amendment Act," India, 2010, <https://dgft.gov.in/sites/default/files/Foreign_Trade_%28Development_%26_Regulations%29_Amendment_Act%2C_2010.pdf>.

9 "Export Control Guidelines – SCOMET Help," Directorate General of Foreign Trade, India, April 24, 2019, <https://dgft.gov.in/sites/default/files/SCOMEThelp24042019-converted.pdf>.

arrangement or understanding that involves an obligation to facilitate or undertake site visits, on-site verification, or access to records/documentation by foreign governments or foreign third parties, either acting directly or through an Indian party or parties.[10] Requests for such permissions are considered in the way requests for export/import licenses are considered.

The Dilemma of Controlling Emerging Technologies

Ensuring control over intangible technology transfer is a challenge. Transfers of software and technology through intangible means can occur through the electronic transfer of data or the oral transmission of information. There are several different means through which technology transfers may take place including:

1. Commercial and government sales
2. Scientist, engineer, student, and academic exchanges
3. Co-development and co-production agreements
4. Commercial proposals and associated business visitors
5. Trade fairs, exhibits, and air shows
6. Sales to third-party nations
7. Multinational corporation transfers
8. International programs (such as fusion, space, and high energy)
9. International meetings and symposiums on advanced technology
10. Dummy corporations
11. Knowledge acquired after mergers and acquisitions

With the emergence of new technologies, the risk of proliferation through the above means and the types of technology transfer have also increased. There is a need to have appropriate controls on the export, re-export, or transfer of emerging technologies. The Bureau of Industry and Security of the U.S. Department of Commerce sought assistance from exporters and other stakeholders to identify emerging technologies with proliferation relevance.

Some of the categories of the emerging technologies with potential risk for proliferation include:

10 Ibid.

- Biotechnology (e.g., nanobiology, synthetic biology, genomic and genetic editing to build viruses, and neuro-tech)
- Artificial intelligence and machine learning technology (e.g. neural networks and deep learning, evolution and genetic computation, computer vision, planning, etc.)
- Navigation, and timing technology
- Microprocessor technology (e.g., systems-on-chip or stacked memory on chip)
- Advanced computing technology (e.g., memory-centric logic)
- Data analytics technology (e.g., visualization, automated analysis algorithms, or context-aware computing)
- Quantum information and sensing technology (e.g., quantum computing, encryption, or sensing)
- Logistics technology (e.g., total asset visibility or distribution-based logistics systems)
- Additive manufacturing (e.g., 3D printing);
- Robotics (e.g., micro-drone and micro-robotic systems. swarming technology, self-assembling robots, and molecular robotics);
- Brain-computer interfaces;
- Hypersonics (e.g., flight control algorithms, propulsion technologies, and specialized materials);
- Advanced materials (e.g., adaptive camouflage, functional textiles, or biomaterials);
- Advanced surveillance technologies (e.g., face-printing and voiceprint technologies);

Policy-makers are faced with the challenge of ensuring that the competitive edge of domestic high-tech companies in the global market will not be damaged if such emerging, cutting-edge technologies are included in the scope of export control lists. Their challenge is to determine which export of emerging technology poses a risk to national security and has a higher proliferation risk. This calculation is necessary for governments intending to regulate the transfer of emerging technologies through export controls.

Framework for Analysis

The author analyzed the work of the Nonaka Innovation Cycle Model on the knowledge transfer and conceptual models like the Capability Acquisition Model (CAM) for transfer of intangible technology to suggest a standard model to evolve the concept of identifying parameters that

take into account controllability while judging what needs to be controlled.[11,12]

Gorman has identified several types of knowledge, including declarative (what), procedural (how), judgemental (when), and wisdom (why), suggesting that each type of knowledge had both tacit and explicit elements.[13] Nonaka's innovation cycle models knowledge transfer as a spiral process and each type of knowledge can be transferred in a different way.[14] He states that tacit knowledge is subjective and experience-based and cannot be expressed in words, sentences, numbers, or formulas, often because it is context specific. This also includes cognitive skills such as beliefs, images, intuition, and mental models as well as technical skills such as craft and knowhow. Explicit knowledge is objective and rational knowledge that can be expressed in words, sentences, numbers, or formulas (context free). It includes theoretical approaches, problem solving, manuals and databases.

Adapted Capability Acquisition Model

To understand the transfer of intangible technology, Ian J Stewart suggested the Capability Acquisition Model. He studied the process of capability indigenization which more often involves the acquisition or emulation of a capability that already exists elsewhere in the world rather than creating new ideas.

The model suggests that in order to achieve the target capability, the acquirer of technology can progress iteratively inwards as their possession of tacit knowledge increases. This inward progression allows them to utilize explicit knowledge, materials, and equipment more fully in reaching their target capability.[15] Both tacit and explicit knowledge are required for capability acquisition to be successful. Tacit knowledge acquisition is a prerequisite to acquisition of capability. It is suggested in the model that it is the progression of tacit knowledge that allows progress to be made towards realizing a capability, thus implying that acquisition of equipment or materials and availability of explicit information alone would not result in successful capability acquisition.

A further refinement of this model involved the integration of the "technology readiness levels" (TRL) model. A key reason for integrating TRLs into the CAM model is that it allows the model to consider the contribution of research and development to the acquisition of a capability.[16] This is particularly important in relation to intangible technology controls, as research and development can fall within the scope of controls but the nature and scope of these controls is generally poorly understood.

---

11 Ikujiro Nonaka and Takeuchi Hirotaka, "The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation (New York: Oxford University Press, 1995).

12 Ian J. Stewart, "The Contribution of Intangible Technology Controls in Controlling the Spread of Strategic Technologies," *Strategic Trade Review,* Vol. 1, Issue 1 (Autumn 2015), pp 48-55.

13 Michael E. Gorman, "Types of Knowledge and Their Roles in Technology Transfer,"*Journal of Technology Transfer* Vol. 27, No. 3 (2002), pp. 219-231.

14 Ibid, p. 12

15 Ibid.

16 Ian J Stewart, "Examining Intangible Controls," Project Alpha, Kings College, Vol 1, June 2016, pp 2-8.

Emerging Technologies – Technology Proliferation Risk Score (TPRS) Model

Forecasting emerging technologies and their impact, especially in the security field rather than just from an economic perspective, is inherently difficult and to some extent elusive. However, if dialogue with both exporters and researchers can provide information about a technology early on, predictions, risk identification, and the development of adequate standards and parameters could be streamlined. The approach to assessing emerging technologies and to distinguishing between basic and applied research — therefore understanding when export control exemptions may apply — often differs significantly between scientists and authorities. Some authorities have started supporting the use of so-called technology readiness levels (TRLs), a scale originally developed by the National Aeronautics and Space Agency (NASA), to establish common general standards for technological development.[17]

The proposed Technology Proliferation Risk Score takes inspiration from the adapted CAM and utilizes the TRL suggested in the model to determine the risk assessment of emerging technologies.[18] It measures proliferation risk and provides the TPR score from one to ten, on the basis of proliferation risk criteria. Proliferation risk is the likelihood of a state or non-state actor obtaining sensitive technology within a given time period. Proliferation risk criteria are the reference points against which the significance of risk is evaluated and measured.

The Adapted Capability Acquisition Model fails to identify the proliferation risk associated with the technologies. There is a need to develop new tools and approaches for understanding, limiting, and managing the risks posed by the proliferation of intangible technologies. This article focuses on the risk assessment of new emerging technologies and the methodology to be applied to score these technologies based on their proliferation capability.

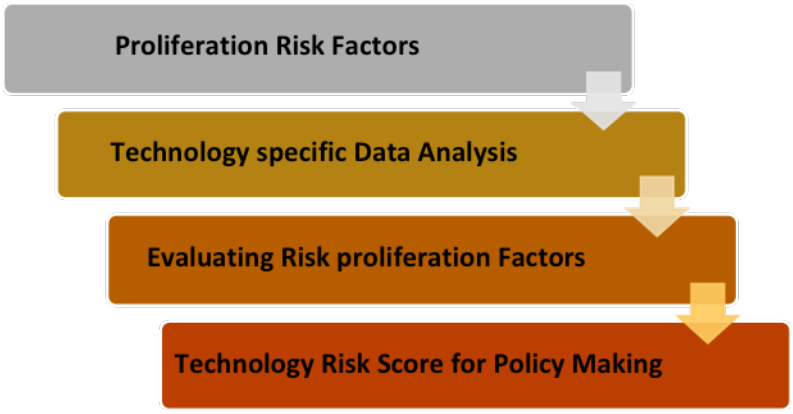

Image 1. Framework for analyzing and calculating proliferation risk score

17 "Technology Readiness Level," National Aeronautics and Space Administration, October 29, 2012, updated on August 7, 2017, <https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html>.

18 Ian J. Stewart, "The Contribution of Intangible Technology Controls in Controlling the Spread of Strategic Technologies," *Strategic Trade Review,* Vol. 1, Issue 1 (Autumn 2015), pp 48-55.

This analytical/predictive tool for comprehensive proliferation risk assessments will provide important information for discussions and decisions regarding export control options for controlling intangible technology transfers.

These assessments will:[19]

- Exploit approaches for analysing difficult-to-quantify proliferation risk factors or indicators (e.g. potential to proliferate, accessibility, and level of damage);
- Evaluate diverse risk proliferation factors by analyzing the data for technologies to understand the trade-offs and potential risk of proliferation;
- Apply these tools to score technologies and display the results in a useful format for decision makers to control these technologies.

Technology Risk Proliferation Score Criteria

Fred A. Manuele is the first to use the term "risk scoring system" for operational risk assessments.[20] He states that two-dimensional risk assessment matrices using likelihood (L) of event occurrence and severity of consequence (S) have been commonly used in risk assessment exercises. However, as risk scoring systems with three or four risk factors are becoming more common, adding a third or fourth factor such as failure detectability, control effectiveness, and vulnerability or other can be useful.

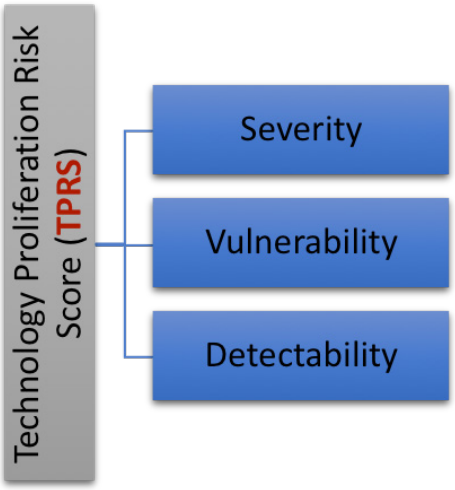

Image 2. Technology proliferation risk parameters

19 "The Objective of the NEET's Proliferation and Terrorism Risk Assessment (PTRA) Subprogram," United States Office of Nuclear Energy, <https://www.energy.gov/ne/nuclear-energy-enabling-technologies/proliferation-and-terrorism-risk-assessment>.

20 Fred A Manuele, "Risk Assessment and Hierarchies of Control – Professional Safety," May 2005, pp 38-39 <https://aeasseincludes.assp.org/professionalsafety/pastissues/050/05/030505as.pdf>.

This article analyzes the technology proliferation risks by determining the parameters for assessing the proliferation risk of technologies. The parameters include: the ***severity*** in terms of the possible consequence or impact of the technology if transferred outside the country and into the hands of the non-state actors or high risk countries and the ***vulnerability*** of a specific technology which is the exposure of a particular technology and measures the capability of the non-state actors to access a particular technology. The detectability factor is the degree to which a specific technology transfer to a non-state actor or high risk countries is detected by the enforcement agencies.

Severity (S)

Severity is a measure of the possible consequence of a technology transfer to a non-state actor or enemy state. Severity associated with a risk is normally assigned a score, level, or rating. This will be measured on a rating of one to ten. A one rating relates to the remote possibility of causing minor severity harm, a ten rating being a risk with very likely probability of causing catastrophic harm. The severity assessment matrix ranks two items: the probability of occurrence of harm and the severity of that harm due to technology proliferation.

Severity Score (Severity harm from Technology Proliferation)				
Probability of Proliferation	**Catastrophic**	**Serious**	**Moderate**	**Minor**
Very Likely	10	9	8	7
Likely	9	8	7	6
Unlikely	6	6	5	4
Remote	4	3	2	1

Table 1. Severity assessment matrix

Vulnerability (V)

Vulnerability is a measure of the degree to which a particular technology or the system associated with it is likely to be used for proliferation, manufacturing of a WMD, or exposed globally. The vulnerability will be measured on the basis of the scoring of the following factors:

Vulnerability Score			
S.No.	**Vulnerability Factor**	**High/Yes**	**Low/No**
1	Capability to reverse engineer technology	1	0
2	Ability to substitute for conventional manufacturing/ processes	1	0
3	Cost of acquisition of emerging technology	0	1

4	Barrier of entry to acquire or learn technology	0	1
5	Design–Build–Test cycle of Technology (Short -1, Long – 0)	1	0
6	Existing Self-Regulating Instrument/ Regulatory Framework	1	0
7	Cyberattack Vulnerability (Technology transfer through Cloud computing or insecure servers)	1	0
8	Dual-use Capability (Applicability in developing WMDs)	1	0
9	Development of Standards to transfer technology	0	1
10	Technology Readiness Level (More than 6) *	1	0
	Vulnerability Score	Max - 10, Min - 0	

Table 2. Vulnerability scoring matrix[21]

The various vulnerability factors to be analyzed in scoring the emerging technologies include the following:

- **Capability to reverse engineer technology** – The Institute of Electrical and Electronics Engineers (IEEE) defines reverse engineering as "the process of analyzing a subject system to identify the system's components and their interrelationships, and to create representations of the system in another form or at a higher level of abstraction," where the "subject system" is the end product of software development.[22] Reverse engineering is a process of examination only: the software system under consideration is not modified (which would make it re-engineering or restructuring). Reverse engineering can be performed from any stage of the product cycle, not necessarily from the functional end product. The capability to re-engineer an emerging technology raises the risk of proliferation of that technology. The high probability of reverse engineering an emerging technology will raise the vulnerability risk;

21 The TRL Score as suggested by the Adapted Capability Model from Ian J Stewart. See Ian J Stewart, "Examining Intangible Controls," Project Alpha, Kings College, Vol 1, June 2016, pp 2-8.

22 E.J Chikofsky and J.H Cross, "Reverse Engineering and Design Recovery: A Taxonomy," *IEEE Software,* Vol. 7 (January 1990), pp. 13–17.

- **Ability to substitute for conventional manufacturing/processes**: The ability of an emerging technology to be a potential substitute for conventional processes or manufacturing increases the possibility of wide adoption of such a technology. The higher the adoption rate of the technology, the higher the risk to control it. Therefore, a high adoption rate signifies high vulnerability of the emerging technology;

- **Cost of acquisition:** The cost of acquiring an emerging technology is a determining factor. Cheap technology products have higher probability of proliferation as compared to technologies that have high cost to acquire. Higher cost of acquisition will signify lower vulnerability;

- **Barrier of entry to acquire or learn technology:** Barriers to entry are the obstacles or hindrances that make it difficult for new companies to enter a given market. These may include technology challenges, government regulations, patents, costs or education, and licensing requirements. High barrier to entry of an emerging technology will signify low vulnerability;

- **Design–build–test cycle of technology:** Also known as the application development life-cycle in Information Technology, it is a process for planning, creating, testing, and deploying an information system. The systems development life cycle concept applies to a range of hardware and software configurations. There are usually six stages in this cycle: requirement analysis, design, development and testing, implementation, documentation, and evaluation. The shorter the cycle to develop a new technology system, the higher the vulnerability of that technology to proliferate;

- **Existing self-regulating instrument/regulatory framework:** This includes international and regional agreements, national laws and regulations, policies and guidelines, codes of conduct, terms and conditions of funding instruments, and education and awareness-raising exercises covering the emerging technology. Any existing self-regulating instrument/ regulatory framework will reduce the risk of proliferation of the emerging technology. The higher the regulatory framework, the lower the vulnerability;

- **Cyberattack vulnerability (technology transfer through cloud computing or insecure servers):** The vulnerability of an emerging technology to be the target of cyberattacks raises the proliferation risk significantly. This especially applies in the case of cloud computing and transfer of technology through online services. While cloud computing models are full of advantages compared to on-site models, they are still susceptible to both inside and outside attacks. Therefore, cloud developers need to take security measures to protect their users' sensitive data from cyber-attacks. Any emerging technology that can be easily hosted in the cloud or transferred through online services is at higher risk of cyber-attack and therefore more vulnerable to proliferation;

- **Dual-use capability (applicability in developing WMDs)**: This refers to the trade in dual-use items – goods, software, and technology that can be used for both civilian and military applications and/or can contribute to the proliferation of WMD. Many emerging technologies have high dual-use potential signifying their higher proliferation risk;

- **Development of standards to transfer technology:** Developing standards for data privacy related to technology at the international level could enable a more level playing field for companies. At the same time, they could also moderate possible future risks that could result from the exploitation of data sets using machine learning and artificial intelligence. The likelihood of cyber-security standards and codes being effective is considerably higher if they are developed by or in conjunction with the scientific community through a continuous process of review and exchange that is able to respond to rapid scientific developments and public opinion. Development of such standards lowers the vulnerability of the technology;

- **Emerging technology readiness level(TRL):** To gauge the maturity of technology acquisition, it is useful to measure emerging technologies against Technology Readiness Levels(TRL). Following initial development by NASA, industries have widely accepted the TRL scale as a way of measuring the maturity of the application of technology. Ian Stewart has applied the TRL scale in his Additive CAM model. The use of TRLs enables consistent, uniform discussions of technical maturity across different technologies.

The TRL Scale includes the following levels:

Technology Readiness Level[1]	Description
TRL 1	Basic principles observed
TRL 2	Technology concept formulated
TRL 3	Experimental proof of concept
TRL 4	Technology validated in lab
TRL 5	Technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 6	Technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 7	System prototype demonstration in operational environment
TRL 8	System complete and qualified
TRL 9	Actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

Table 3. Technology readiness level

A TRL six indicates that the technology's capability has been determined. A TRL six technology has a fully functional prototype or representational model. A TRL seven technology requires that the working model or prototype be demonstrated in a working environment. A TRL eight technology has been tested and is ready for implementation into an already existing technology or technology system. A TRL score of six and above signifies a mature stage of technology acquisition and is a factor in determining the potential proliferation vulnerability of the technology.

Detectability (D)

Detectability is the ability to detect technology exposure to a non-state actor before it causes harm. The purpose of considering detection is to ensure that potential or actual transfer of technology can be identified with enough time to take action before the harm is caused.

It is determined on the basis of the technology regulations currently in place other than the export controls. It can be determined on the basis of the availability of a specific technology. If the technology is available with only a few companies within a country, it is to be determined whether these companies have internal compliance programmes to ensure that an unwanted technology transfer is reported. Detectability is scored from zero to ten (zero being high detectability and ten low detectability).

Detectability Score				
S. No.	**Detectability Factor**	**High**	**Medium**	**Low**
	Industry Compliance Program	0	1	2
	Degree of digitization	2	1	0
	Government Regulations	0	1	2
	Specific Targeting capability	2	1	0
	Do It Yourself(DIY) Capability	2	1	0
Detectability		**High Detectability – 0, Low Detectability - 10**		

Table 4. Detectability scoring matrix

- **Compliance program:** An effective export control compliance program where technologies are being developed or implemented is important to lower the risk of their proliferation. This also ensures effective detection of any proliferation;

- **Degree of digitization:** This determines the degree to which the technology has been digitized by exporters. A higher degree of digitization will make it difficult for the proliferation to be detected;

- **Government regulations:** Active regulatory frameworks to audit emerging technologies and a mechanism to generate intelligence from exporters to determine the proliferation capability of an emerging technology is a critical factor in detecting risk of its proliferation;

- **Specific targeting capability:** The higher targeting capacity of proliferation of a technology in a limited region or specific set of industry reduces the ability to detect it. The lower the specific targeting capability, the lower the detectability in case of proliferation;

- **Do It Yourself(DIY) capability:** The DIY capability of a technology depends on the ability

to commonly exchange information in order to build it in the DIY community. This may provide an attractive option for non-state actors to easily adapt to the new technology. The higher the DIY capability of a technology, the lower the probability of detecting its proliferation.

Calculating Risk of Emerging Technologies

The various risk factors under the three parameters of severity, vulnerability, and detectability are evaluated and a score for each of the parameters is used to calculate the overall TPRS score as below:

Image 3. Calculating TRPS

The Technology Proliferation Risk Score may be analyzed by decision makers to control the export of emerging technologies. An indicative matrix to analyze the TPR Score is shown below:

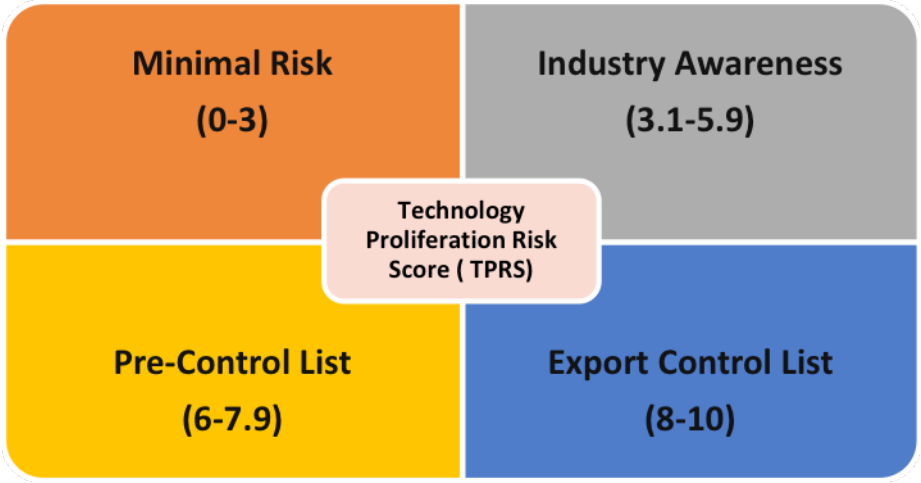

Image 4. TPRS score matrix

The TPRS may be calculated for the emerging technologies by the governments to analyze the risk associated with their transfer and if the risk is high, decision makers can initiate steps to put these technologies in control lists and regulate their transfer. A high risk score signifies high severity, high vulnerability, and low detectability. The following outcomes based on the TPRS are included in the Score Matrix:

- **Minimal risk:** Technologies with TPRS score with low severity, low vulnerability, and high detectability risk do not need focus from the export control perspective;

- **Industry awareness:** Technologies with TPRS score from 3.1 to 5.9 signify lower risk of proliferation but exporter awareness may be introduced for these technologies as a preventive measure;

- **Pre-export control list:** Technologies with TPRS score relatively higher and between six to 7.9 may be included in a "pre export control" list that may function as a watch list for emerging risk of future proliferation if exporter compliance is not checked;

- **Export control list:** A high risk score signifies technologies with high severity and impact if exported in wrong hands, high vulnerability to proliferation and low detectability risk. Such technologies may be included on a country's control list with the requirement of obtaining export license.

Case Study: Additive Manufacturing and Biotechnology[23]

Additive manufacturing (AM) is a rapidly emerging technology with growing relevance for WMD proliferation. The rapid pace of AM development makes it increasingly difficult to keep track of its potential impact on proliferation pathways. More recently, the convergence of biotechnology with emerging technologies, including additive manufacturing, has become a particular focus since these technologies hold tremendous promise but also increase the possibilities for misuse of biotechnology and the proliferation of biological weapons. They could also provide new possibilities for biological weapon use and increase the exposure of digitized biological data and operating parameters to cyberattacks.

Additive manufacturing and biological use of this technology has been applied as a case study of an emerging technology to determine its proliferation risk using the TPRS Model as a test case. While determining the TPRS score, the following methodology has been used after analysing the proliferation factors and risk parameters for this emerging technology with a limited scope of indicating the proliferation risk.

- **Severity:** Additive manufacturing describes a broad category of advanced automated manufacturing techniques. It can produce objects of virtually any shape or form by depositing layer upon layer of material and fusing them together using a variety of techniques, such as liquefied extrusion, inkjet printing, stereolithography, sintering, and laser, or electron beam melting. In a biological weapon, bio-printing a suitable pathogen can infect the target and cause illness or death after dissemination without being affected by environmental conditions or being significantly mitigated by medical treatment and biodefence measures.

The severity of proliferation of such biological weapons in the hands of non-state

23 Kolja Brockmann, Sibylle Bauer, Vincent Boulanin, "Arms Control and the Convergence of Biology and Emerging Technologies" SIPRI, March 2019.

actors is catastrophic while the probability of this occurring is likely. Therefore, the severity score is nine per the Severity Scoring Matrix.

- **Vulnerability:** Additive manufacturing machines rely on digital build files, initially in the form of computer-aided design (CAD) files or similar formats, which can encode the dimensions of the desired object and subsequently in machine-specific formats that include the operating parameters and commands that the AM machine needs to execute in order to produce the object's desired performance characteristics. The digitization of the blueprints and commands—the information that is necessary for the production of an item—allows for easy transferability of the technology using electronic media (e.g. email) or decentralized information-sharing platforms (e.g. cloud storage). Additive manufacturing has already been adopted by the biomedical sector for a variety of applications. The main advantage that many of the applications seek to exploit is the ability of AM machines to produce individualized items without the need to produce new moulds each time, to reconfigure machine tools, or to draw on extensive manual manufacturing skills. AM is established as a production technology for customized biomedical implants or prostheses, such as hip and dental implants.The Vulnerability Matrix for AM and biotechnology is specified in the Table below:

Vulnerability Scoring Table: Additive Manufacturing and Biotechnology			
S.No.	**Vulnerability Factor**	**High/Yes**	**Low/No**
1	Capability to reverse engineer technology	**1**	
2	Ability to substitute for conventional manufacturing/ processes		**0**
3	Cost of acquisition of emerging technology		**1**
4	Barrier of entry to acquire or learn technology	**0**	
5	Design–Build–Test cycle of Technology (Short -1, Long – 0)		**0**
6	Existing Self-Regulating Instrument/ Regulatory Framework	**1**	
7	Cyberattack Vulnerability (Technology transfer through Cloud computing or insecure servers)	**1**	
8	Dual-use Capability (Applicability in developing WMDs)	**1**	

9	Development of Standards to transfer technology		**1**
10	Technology Readiness Level (More than 6)	**1**	
	Vulnerability Score	**7**	

Table 5. The vulnerability score of additive manufacturing and biotechnology is 7

- **Detectability**: The use of bio-printing is less mature, but a variety of applications are in the developmental phase or in the early stages of commercialization. While the ability to print fully functional donor organs that can be implanted and sustained in a human body is probably decades away, the production of different kinds of tissue for medical research and testing is more advanced. AM technology provides a multipurpose manufacturing capability that can potentially substitute for other, controlled production equipment. In addition, the digitization in build files with much of the information required for the production of a controlled product means that it can now be more readily transferred—whether electronically, without having to pass through customs in a material form, or through the travel of a person with the necessary expertise. Advances in AM could thus have a significant impact on the effectiveness of export control as a nonproliferation tool as it could increase the reliance on transfers of data, which are assumed to be more difficult to track and control by licensing and enforcement agencies. The detectability score as per the TPRS model is shown in the table below:

Detectability				
S. No.	**Detectability Factor**	**High**	**Medium**	**Low**
	Industry Compliance Program			**2**
	Degree of digitization		**1**	
	Government Regulations		**1**	
	Specific Targeting capability	**2**		
	Do It Yourself(DIY) Capability		**1**	
Detectability(Additive Manufacturing and Biotechnology)		**7**		

Table 6: The detectability score for AM and biotechnology is seven

TPRS Score: The technology Proliferation Risk Score for additive manufacturing and biotechnology as per the model detailed above is:

Severity (9) + Vulnerability (7) + Detectability (7)/3 = TPRS Score (7.6)

The TPRS Score of 7.6 indicates that the emerging technology of AM and biotechnology falls under the category of a "pre export control" list that may function as a watch list for emerging risk of proliferation in future, if exporter compliance is not checked.

Policy Recommendations for Intangible Technology Transfer Control

The government and exporters can adopt specific strategies to deal with the emerging technologies based on technology's risk score including assisting exporters to put in place strict compliance for technologies that are in pre-control list stage with a relatively high risk of proliferation. The author has detailed the policy recommendations for intangible technology transfers in the context of reforms in export control policies of developing countries like India. The TPRS model has been constructed with the intent to be used by policy-makers when assessing the proliferation risk of the technologies. In this context, the author has suggested the following policy recommendations:

1. Emerging technologies under the export control regimes

The Wassenaar Arrangement recognizes that the implementation of controls on software and technology represents an important aspect of participating states' export control systems.[24] A Statement of Understanding attached to the General Technology Note states that participating states have agreed to treat controlled technology "with vigilance in accordance with national policies and the aims of this regime." The policies of different member states differ when it comes to putting the technologies into their control lists. This is more of an issue in the field of dual-use export controls than military goods given that the latter are more clearly defined and understood. Moreover, it is also particularly relevant in the field of technology controls where establishing what is and is not subject to control can be a difficult process that is open to interpretation.

In such a scenario, the export control regimes should develop a mechanism to objectively determine the emerging dual-use technologies which needed to be controlled. Lists of such dual-use technologies with a high proliferation risk score (with high vulnerability, high severity, and low detectability) should be maintained by the export control regimes to assist member states in putting emerging technologies into their national export control list.

2. Controlling emerging technologies under export control lists in various countries

Various governments including the Government of India should evolve a mechanism to identify the emerging technologies that have high proliferation risk and include them in the export control lists under the controlled category. An emerging technology advisory committee

24 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," The Wassenaar Arrangement, 2013, <http://www.wassenaar.org/controllists/index.html>.

may be created to advise the government on proliferation risk of emerging technologies in close coordination with exporters. The process should involve collecting and analyzing data on the emerging technology in close coordination with exporters and identifying the severity, vulnerability, and detectability of the emerging technology based on the suggested TRPS model to put it into the control list.

3. Technology checker tool

Governments should create a checker tool that is designed to identify export license requirements for export of controlled items to certain destinations. The OGEL checker tool as developed by the Department of International Trade in the United Kingdom is specific to the export of controlled goods.[25] It is recommended that a similar checker tools be developed within various export control regimes to help exporters identify export license requirements for both goods and technology.

4. Government-industry outreach

Various governments actively engage exporters in technology export control compliance programs. Governments in countries like India may assist exporters in implementing strategic trade management compliance through an outreach program. It is recommended that a system for exporter outreach be institutionalized in the form of a *technology transfer compliance outreach program*. The program should focus on export control compliance-related awareness campaigns specifically for technology companies. The government should come up with detailed technology transfer compliance guidelines and provide export compliance training to companies and their staff as part of the program. Further, this should help in gathering relevant data for the TPRS model.

5. Exporter compliance best practices

A robust technology transfer compliance program for exporters can help organizations dealing with the export of dual-use emerging technologies to avoid being regulated. In the TPRS model, the emerging technologies falling under the pre-control list stage in the proliferation risk score assessment can avoid moving to the next stage of proliferation risk if exporters demonstrate efficient export control compliance. The technology proliferation risk score can provide these exporters with an opportunity to work on their internal compliance.

Intangible technology transfers are still a challenge for many medium and small enterprises in developing countries. The author studied best practices followed globally by technology companies and the following best practices are recommended for protecting technologies that are already in the control lists, or even conforming to provisions set in export control laws or falling under the pre-control list category of the TPRS model:

---

25 "Open General Export License (OGEL) Checker Tool," Export Control Organization, Department of International Trade, UK Government, <https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/OGEL_GOODS_CHECKER_LANDING_PAGE/new>.

i. Export risk engine

To provide efficient and effective risk assessment of online activities, technology exporters use risk engine tools. The risk engine can be utilized to analyze a range of indicators associated with an activity to determine the probability that the activity is fraudulent especially in cases where the technology or information is controlled. Used today by leading banks, credit and debit card issuers, and other organizations worldwide, the risk engine detects, analyzes, scores, and manages online activity for the purpose of consumer protection. It reduces the risks of privacy and compliance exposure, lowers the level of fraud, detects possible impersonators, and identifies new fraud trends as they develop to protect any proliferation. Companies should integrate their systems with the risk engine to provide efficient and effective risk detection of online activities of its employees handling sensitive information. The engine monitors the end users' activity and ensures detection of any activity online in secure official environment.

ii. End-to-end data encryption

Software and Technology companies should have cryptographic protection of data such that the data are not in unencrypted form between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary), and the means of decryption are not provided to any third party. The originator and the recipient may be the same person.

iii. Strengthening data storage in cloud computing

The Bureau of Industry and Security of the U.S. Department of Commerce issued specific guidelines for end-to-end encryption of data and data storage over the cloud environment for U.S companies.[26] The governments of other countries should also issue specific guidelines for cloud storage and end-to-end encryption of data for companies located outside U.S.

iv. Technology specific export control study groups in industries

Exporters should be encouraged to dedicate resources for export control compliance and technology and software exporters specifically should create in-house export control study groups that classify the technologies and software being developed. This screening should be mandatory before the technology is transferred or the software is released. The export control study group should assist the company in the process of getting an export license in case the technology is controlled. The group should be responsible for training the staff and making them aware of the export control compliance.

26 "Emerging Technology and National Security Policy," Bureau of Industry and Security, U.S. Department of Commerce, <https://www.bis.doc.gov/documents/bis-annual-conference-2018/2239-cloudy-with-a-chance-of-technology-transfer-breakout-rev-13may2018/file>

v. Technology exporters should strengthen cybersecurity

Cyber security is relevant in the current scenario where non-state actors are increasingly making attempts to hack systems and servers to steal sensitive data. Export control in organizations handling sensitive information and data is about securing their systems from the unauthorized access of hackers. The exporters must design more secure systems, compartmentalized software or information, focus on air gapping networks (network segmentation) and provide limited access to computers with controlled information. Awareness and vulnerability training must be provided to the employees vulnerable to cyber-attacks. The 2FA verification with hardware key access can be provided to prevent phishing attacks and the companies must install network intrusion detection systems especially where the controlled information is stored.

Conclusion

Emerging technologies pose a radical challenge for export controls and demand a new approach. It has been difficult for countries and export control regimes to keep up with the pace of new technologies. It has also been difficult to come to a consensus on why a certain technology should be controlled and thereby establishing the proliferation relevance of an emerging technology is a key challenge that often requires a long consultation process. In the case of emerging technologies, nations are particularly cautious not to compromise new industries and limit the potential of their development and competitiveness globally. The impact and applicability of emerging technologies is often limited and their ultimate potential can be somewhat ambiguous. For emerging technologies, there is no objective mechanism yet that can provide for meaningful parameters to put them under a control list. Therefore, introduction of controls in the absence of such mechanism is complicated.

In this article, the author has attempted to identify parameters that determine technology controllability, evaluate the risk factors under each parameter, and enable relevant score-based analysis to present decision-makers with an objective assessment of the proliferation risk of emerging technologies. The Technology Proliferation Risk Score suggested in the article is determined through the parameters scored based on the data collected on relevant technology for which the proliferation risk score is to be calculated. The TPRS model has a limitation and dependence on the detailed technology dataset before the parameters can be scored. However, the model provides a framework for risk assessment for the emerging technologies and a test case has been studied at a macro level to analyze and score the proliferation risk of additive manufacturing and biotechnology.

Governments can incorporate the TRPS model for risk assessment of technologies in their governance mechanisms to determine the controllability of technologies. Various policy recommendations for the government have been suggested to bring the policies up-to-date with the risk of proliferation of emerging technologies. Recommendations include global best practices that can be adopted to strengthen export control compliance by exporters. This finds more relevance in the context of developing countries like India's where intangible technology transfer is still in an evolving phase and its export control is based on voluntary disclosure. Considering vast potential of software and technology exports globally, it is pertinent that

national export policies are ahead of their time to ensure nonproliferation due to export controls on high risk technology.

Future Research

The risk proliferation factors required for each parameter to score vulnerability, severity, and detectability can be further expanded as per the requirements of the technology. The model can also be detailed for a particular group of emerging technologies like quantum technologies since it may require specific parameters to assess risk. In the next stage, the potential controllability of a technology can be analyzed as a parameter along with severity, detectability, and vulnerability for assessing proliferation risk of emerging technologies under the TPRS Model.