Commentary

To Share or Not to Share?: The Challenge of Controlled Technologies in Research and Development (R&D)

RUDI DU BOIS, JULIA BELL, DRIES BERTRAND[1]

Abstract

Globalization of world trade has not only led to an increase in the trade of goods but also to technology transfers on a global scale. In the wrong hands, advanced and sensitive technologies can pose serious compliance risks. Export controls have been implemented to impede the proliferation of advanced technology through the control of dual-use items to sensitive end-uses and end-users. However, technology acquisition and transfer is hard for governments to monitor and control. Many governmental regulatory authorities currently lack the skills and resources to counter the growing threat of diversion of advanced technological items. Public-private cooperation should help in this respect. From their side, companies and R&D institutions that act as exporter have the legal responsibility to comply with export regulations and should therefore establish a robust compliance program in order to prevent dissemination of sensitive technologies. Non-compliance has legal consequences, including significant fines, the loss of export privileges, as well as reputational damage.

1 Rudi du Bois is a Senior Advisor at Deloitte Belgium. He is an expert in export controls and sanctions with more than 30 years of experience in developing and implementing trade compliance programs, conducting risk assessments, and commodity classifications. Julia Bell leads Deloitte's Global Export Controls & Sanctions team in London. She has led compliance-enhancing projects for a number of years in a variety of industries, including financial services, consumer products, oil and gas, aerospace & defence, manufacturing and the technology, media and telecommunications industries. She is a specialist in U.S., EU, UK, French, German and other EU Member State military, dual-use, and sanctions regulations. Dries Bertrand is a partner in Deloitte Belgium's Global Trade Advisory practice, based in Brussels. He has over 15 years of experience in the area of global trade and worked for various international companies providing global trade strategy, import / export compliance and global trade automation advice.

Keywords

Research and development, sensitive technologies, export controls, diversion, export compliance, penalties

A Digital World

Barriers that once impeded the flow of information and technology have been progressively eroded. In a world where computing costs are plummeting, connectivity is becoming ubiquitous, and information flows freely, previously cost prohibitive tasks and business models are becoming more available to a larger amount of players. However, companies must effectively manage the balance between providing the access and agility to run their business while ensuring that data is secure and that the organization is compliant with governmental regulatory requirements.

This risk is compounded by an increase in the development of more sensitive technologies based on microchips and related products. This kind of technology has the capacity to substantially improve the accuracy and effectiveness of weapons at relatively low cost.

The Role of Western Technology

The current Russian aggression in Ukraine provides some useful lessons. The effective use of Western weapons by the Ukrainians- from the long range High-Mobility Artillery Rocket System (HIMARS) from the United States to the Anglo-Swedish Next Generation Light Anti-Tank Weapon (NLAW) - is now well known. More significant from the point of view of this commentary, however, is the role of "Western" (including from U.S. allies like Japan) microprocessor-type components incorporated into Russian equipment.

A study by the Royal United Services Institute (RUSI) in conjunction with Reuters revealed that in Russian equipment that had fallen into Ukrainian hands, there were no less than 450 such components, with 318 from the United States, followed by 34 from Japan, and 30 from Taiwan.[2] This took place despite strict Western sanctions since the Russian occupation of Crimea in 2014. A study of Iranian equipment sold to Russia showed a similar picture.[3]

This illustrates the key problems of control of such technology:

- First, that this technology is dual-use and not unequivocally military, and thus harder to identify;

---

2 James Byrne, Gary Somerville, Joe Byrne, Dr Jack Watling , Nick Reynolds, and Jane Baker, "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," RUSI, August 8, 2022, <https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine>.

3 "Dissecting Iranian Drones Used by Russia in Ukraine," Conflict Armament Research, November 2022, <https://storymaps.arcgis.com/stories/7a394153c87947d8a602c3927609f572>.

- Second, the items are small and easily concealed, especially in the flood of microchips used for a plethora of civil applications;

- Third, even if designed in the United States, and to a lesser extent in Europe, much of this technology is manufactured in factories (fabs) in East and Southeast Asia, thus making diversion easier.

Export Controls

Export controls have been implemented to impede the proliferation of advanced technology through the control of dual-use items to sensitive end-uses and end-users. The legal consequences of non-compliance with national export control regulations can be substantial, including significant fines, the loss of export privileges, as well harming a company's reputation.

One example of how high fines might be in the case of violation is the case of Société Internationale de Télécommunications Aéronautiques SCRL (SITA), in which this Swiss company reached a USD $7.8 million settlement with the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) in 2020.[4] SITA is a global IT service provider that serves the commercial aviation industry. The company breached U.S. sanctions several times by providing services to Iranian and Syrian airline operators. SITA was under the jurisdiction of U.S. sanctions because the company's server was located in the United States, the software provided for its clients was U.S.-origin and finally, the messaging services of the company were located in Atlanta, Georgia.

Another example of violations of technology-related export controls is the U.S. company NewTek, Inc. This company, located in Texas, sold video production technology and services to third-country distributors which were then resold to companies and individuals in Iran. Newtek provided software updates, reseller training, and other support to customers in Iran. OFAC and NewTek, Inc. agreed that NewTek would pay USD $189,483 in penalty. However, if NewTek had not voluntarily disclosed its violations, OFAC would have imposed a penalty of over USD $15 million.[5]

However, technology acquisition and transfer is hard for governments to monitor and control.[6] A case in point, as mentioned above, are the high-tech components and technology that still finds their way to Russia through the use of shell companies, academic and research institutions,

---

4 Eric Sandberg-Zakian, "Insight: OFAC $7,8M Settlement with Swiss Company Expands Tech Enforcement," Bloomberg Law, April 16, 2020, <https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-ofac-7-8m-settlement-with-swiss-company-expands-tech-enforcement>.

5 "Know Your Customer: OFAC, BIS Penalize Companies for Sales of "EAR99" Items and Services to Prohibited Parties Through Distributors," JD Supra, September 22, 2021.

6 Andrea Viski, "Advanced Conventional Weapons and Emerging Technologies: Recognizing and Preempting Proliferation Threats," 2022, <https://strategictraderesearch.org/wp-content/uploads/2022/02/Advanced-Conventional-Weapons-and-Emerging-Technologies.pdf>.

third- country distributors, or espionage.[7]

Evaluating Your Export Activity

As exporters, researchers and companies have the ultimate responsibility for complying with export controls and sanctions. There are four principal ways in which an export can be controlled, and each must be evaluated to confirm that the activity is compliant with export control regulations:

1. Item controls: Item controls are restrictions on the trade, provision and/or movement, of both tangible and intangible items that meet defined specifications. These can be inclusive of complete systems, equipment, components, materials, software, technical data, and services.

2. End-use controls: If an item is not listed on the relevant control lists, it may still require a licence to be exported under end-use controls. Historically, end-use controls were implemented to counteract Weapons of Mass Destruction (WMD) development and use, but they can also be applied in connection with prohibited military applications and other protective matters (e.g., internal repression of human rights, environmental protection, etc.).

3. End-user controls: The final recipient (end-user) of an item can also trigger the need for an export licence. End-user controls apply to certain entities or persons who have been added to a denied and/or restricted parties list (e.g., the U.S. Entity List, Denied Persons List, Unverified List, etc.) or specified within the applicable regulation.

4. Destination controls: Trade sanctions and embargoes are tools to implement trade restrictions against target countries for national security and/or other domestic interests, and may also serve as punitive measures. An example of this could be United Nation sanctions on a target country for upsetting international peace and security or internal human rights violations. Sanctions and embargoes can be unilateral or multilateral, and can be comprehensive (e.g, broad item and financial controls applicable to the entire country and its nationals, such as the DPRK) or targeted (e.g., limited to specific items and/or to specific entities affiliated with the country, such as the Russia Sectoral Sanctions).

What to Do?

Many governmental regulatory authorities currently lack the skills and resources to counter the growing threat of diversion of advanced technological items. Viski (2022) recommends that governments develop a strategy in order to raise awareness, enforce compliance, and build

7 James Byrne, Gary Somerville, Joe Byrne, Dr Jack Watling , Nick Reynolds, and Jane Baker, "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," RUSI, August 8, 2022, <https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine>.

public-private cooperation.[8]

It is the responsibility of the exporter to use the correct export classification and to determine if an export license is required. The exporter is also responsible for ensuring that the export is not destined to restricted end-uses, end-users, or destinations without an appropriate authorization in place. Therefore, companies and R&D institutions should raise awareness about the potential dangers of sharing research results and about the need to implement appropriate prevention and control measures such as export control classification and sanctioned party list screening. R&D institutions should also consider additional security measures such as physical security measures, limiting the dissemination of sensitive information with security recommendation by publishing only part of the research results, as well as requiring security clearances for individuals involved in high risk projects.[9]

A robust internal compliance program (ICP) is required not only to respond to the complexity of these challenges in today's current environment, but also the challenges that will emerge as the regulatory environment evolves— which it will.

8 Andrea Viski, "Advanced Conventional Weapons and Emerging Technologies: Recognizing and Preempting Proliferation Threats," 2022, <https://strategictraderesearch.org/wp-content/uploads/2022/02/Advanced-Conventional-Weapons-and-Emerging-Technologies.pdf>.

9 "Guidance Note: Potential Misuse of Research," European Comission, 2021, <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf>.