ARI 37/2024
18 March 2024

Illicit technology transfers to countries of concern: challenges for the international community

Gonzalo de Salazar | Diplomat, PhD in Political Science

Theme

The efficiency of multilateral military and dual-use export control regimes established in the 20th century has been undermined by illicit trafficking networks and gaps in export controls.

Summary

Recent findings concerning the use of Western technology in weapons used by Russia have raised the issue of the effectiveness of sanctions and export control mechanisms established between 1975 and 1995. However, the global scene today is very different from that of the last decades of the 20th century. This paper analyses the need to address the nature of risk-related transactions, identify the gaps and propose upgrading export controls with awareness-raising policies, update the normative framework and provide adequate resources to national implementation agencies.

Analysis

Gaps in current export controls: the state of play

Evidence of Western manufacturers exporting to Russia since its invasion of Ukraine in 2022 sheds light on the extent to which these weapons are reliant on such components.[1] A detailed analysis of the technology used by Russian military systems shows many foreign-made items used by the defence industry.[2] Western technologies have also been found in Iranian military unmanned aerial vehicles (UAVs). It is important to note that in many cases, companies that manufacture such items are not legally responsible for any wrongdoing, especially if the items transferred are not listed in any export control regulation.

[1] The RUSI has identified 450 foreign-made components in its examination of 27 different Russian military systems, including the Kalibr and Iskander missiles. Russia's military modernisation programme has depended on the extensive use of microelectronics manufactured in the West. There is also evidence of counterfeit components used in Russian weapons systems and, therefore, the possibility that the identified entities may not have indeed manufactured components featuring the logos of named entities. James Byrne et al. (2022), 'Silicon lifeline: western electronics at the heart of Russia's war machine', RUSI, August.

[2] Conclusions are based on a dataset of more than 170 individual components that had been found in Russian equipment, with the branding or logo of foreign companies including microchips used to power smartphones and laptops supplied by intermediary countries, though research does not support that transfers violate any international or domestic regulations. See International Partnership for Human Rights (IPHR) & The Independent Anti-Corruption Commission (NAKO) (2023), 'Enabling war crimes? Western-made components in Russia's war against Ukraine'; and 'The chips are down: Putin scrambles for high-tech parts as his arsenal goes up in smoke', Politico, 5/IX/2022.

Certain restrictions on the export to Iran of technologies associated with the nuclear and military sectors, derived from UNSC Resolution 2231 (which endorsed the Joint Comprehensive Plan of Action in 2015) were not considered 'sanctions' at that time, but 'temporary restrictions' to guarantee the success of the agreement. It is also worth mentioning that the UNSC Resolution 2231 imposed trade limitations on nuclear technology, conventional arms transfers, missiles and UAVs.[3] They also prevented UN member states from participating in the supply, sale or transfer to or from Iran of any items, materials, equipment, goods or technologies described in the Missile Technology Control Regime. However, the limits imposed by the UN Security Council on Iran's trade in advanced missiles and UAVs expired on 18 October 2023.[4] Iranian UAVs are now found in Russia's arsenal. Moreover, certain non-state actors (like Hamas, the Houthis and Hezbollah) have the ability to assemble or produce some of these weapons, which could indicate they have foreign assistance and supplies, most probably from Iran.

Sanctions policies are amongst the most widely used non-military instruments of retaliation, pressure and deterrence. Although 'sanctions' and 'restrictive measures' are commonly considered the same concept, in practice there may be restrictive measures without a sanctioning character. In other words, all sanctions are restrictive measures, but not all restrictive measures are sanctions. This is the case for most export control procedures as implemented by multilateral export control regimes (Nuclear Suppliers Group, Australia Group, Missile Technology Control Regime and Wassenaar Arrangement), which were not created as sanctioning bodies but as mechanisms to conciliate legitimate trade interests and international security. However, the technical expertise and items annexes of these regimes have also been used as tools for sanction implementation.

When it comes to export control mechanisms, we need to ask ourselves if the current multilateral regimes can address today's needs and challenges. The answer is, to some extent, yes. Between 1971 and 1996 several multilateral military and dual-use export control regimes were established. The main objective of these regimes was to balance commercial interests with legitimate security concerns. The export control regimes established during this period were the Zangger Committee (1971), the Nuclear Suppliers Group (NSG) in 1975, the Australia Group (AG) in 1985, the Missile Technology Control Regime (MTCR) in 1987 and the Wassenaar Arrangement (WA) in 1996. Over the years, these regimes have been updated and their membership enlarged.

[3] UNSC Resolution 2231, which was adopted on 20 July 2015, aimed to support JCPOA implementation and imposed limitations that went into effect for 90 days. These applied to all UN member states and could be lifted only with prior approval from the Security Council. The restrictions were time-limited. Restrictions on conventional arms transfers, which included sales or purchases of missiles and armed UAVs, expired in 2020. Those on missiles and UAVs, included in Annex B, paragraphs three and four of the resolution, expired on 18 October 2023. The paragraph-three definitions are understood to apply to the 'Category I' systems as defined by the MTCR (rockets and UAVs with a range of at least 300 km and a payload capacity of at least 500 kg). Paragraph four includes both 'Category I' and 'Category II systems (missiles and UAVs with a payload capacity under 500 kg). Iran was, until 18 October, forbidden from trade related to all guided or unguided rockets and UAVs with a range of 300 km or more. Moreover, limitations on Iran's nuclear activities will expire in October 2025.

[4] The day before, Russia announced that it would no longer observe the limits imposed by UNSCR 2231 and called on European countries to abandon their missile and UAV-related restrictions on Iran, which helped Iran to promote its arms, UAVs and missile exports. Russia has deployed and used Iranian UAVs and missiles in Ukraine together with missiles purchased from the DPRK.

However, the global scene today is very different from that of the last decades of the 20th century, there are growing gaps in export controls and the efficiency of these regimes has been seriously undermined. There are important political and economic reasons behind this trend, but this paper will focus on technical issues.

Risk transactions to countries of concern

This paper begins with a reference to the growing evidence of Western manufacturers exporting to Russia since its invasion of Ukraine in 2022. Researchers have found companies or intermediaries that could have been involved in sanctions evasion-related activities. There is also evidence of counterfeit components used in Russian and Iranian weapons systems and the possibility that some identified entities may not have manufactured the components. This aspect of destabilising transfers is, therefore, linked to illicit trafficking networks and entities in third countries able to produce counterfeit components through reverse engineering.

Most products found in the illicit supply chain are dual-use, though there are many non-listed dual-use items in the chain of supply as well, such as microchips designed for smartphones and laptops. Among the former items are:

- Automated robotic machines and computer numerical control machines.
- Spare parts, coolants, lubricants and software for computer numerical control machines.
- Memory modules for missile satellite navigation and computing units.
- Circuits, microprocessors, switches and oscillators.
- Computer and other electronic components.
- Semiconductor, satellite navigation systems, guidance computers and altimeters.
- Gyroscopes and GLONASS-enabled chips.
- Radio sets.

A second problem is the extent and *modus operandi* of illicit trafficking networks. In addition to new producers of advanced dual-use and military technologies entering the market, parallel clandestine markets have developed through illicit trafficking. Many of the above items reach their destination through countries that are not members of the 'sanctions coalition' and/or do not implement proper export control regulations. Many of the illicit networks operating in these states are supervised by the security services of end-user countries, often ignored or unnoticed by the local authorities.

Weapons and military or dual-use technologies flow beyond the reach of multilateral export control mechanisms. The involvement of illicit trafficking networks in armed conflicts and clandestine supply chains for states under international arms embargo is a major challenge for governments in supplier countries. To some extent, there is a link between organised crime activities and these illicit transfers. Such networks, often linked to organised crime, have contributed to the development of parallel markets for these technologies for clandestine programmes of weapons production or reverse engineering. As new clients find these networks a useful tool and criminal smuggling groups find lucrative opportunities, they may also work for economic gain with state or non-state actors. There are many intermediaries in the supply chain.

Once illicit trafficking networks are established, their low profile, high mobility and clandestine nature place them *de facto* out of reach of sanctions and export control mechanisms, making them attractive to countries of concern, terrorists and armed groups. The smaller these transport networks are, the more difficult they are for police forces to detect. However, such transfers also take place in countries where sanctions and export control regulations are not applicable, thus becoming a 'grey zone' where illicit transfers are not in contradiction with existing law and enforcement procedures. Intangible technology transfers make enforcing export and customs control regulations even more difficult. There is a growing need for an updated legal framework and specialised training for enforcement investigators, as well as prevention and deterrence of illicit intangible technology transfers in export controls.

According to the available open sources, some features are frequently present in illicit supply chains:

- In many cases, components reach their destination via a transnational network of subsidiaries and distributors operated by countries of concern to procure goods using front companies. Sometimes they are one-day front companies that can evade any inclusion in sanctions lists. Third-country transshipment hubs and clandestine networks work to build routes to secure access to Western microelectronics.

- They use fraudulent end-user certificates. These are documents used in international transfers involving the sale and supply of arms and dual-use technologies. Its purpose is to identify the final recipient of such materials and certify that the latter does not intend to make a subsequent transfer to third parties. The certificate is used to specify the details of the final destination of the goods and their use (company or entity, address, country of destination and intended use –civilian or military–). End-user certificates can be forged for fraudulent use.

- Sometimes, the end users are real, but they engage in reverse engineering projects for unknown clients. The stated end-user company can dismantle the equipment, copy the system's components and design a replica or a derivative. The latter is sold to another client, who is unknown to the exporter of the original product.

- Customs data in the shipment documents either provide a general description of the products or include inaccurate information. Sometimes they do not include the name of the goods.

- Recipients use different payment methods: cash or bank transfers and also the barter of goods (oil or raw materials), gold and cryptocurrencies. They make transfers of local currency (roubles, yuan, etc) to bank accounts within their countries (not committed to export restrictions) or to foreign banks accepting these currencies. The funds are then transferred and converted into other international currencies (US dollars, euros, etc) to pay the supplier.

Transfers of sensitive but not restricted dual-use products

Many of the technologies concerned are mass-produced industrial goods that are not subject to dual-use controls, but freely available on the market. Transfers of such products to countries of concern are a sensitive issue, but they are not illegal.

Moreover, supplier companies may be based in a country bound by sanctions and export control regulations, but their production is also located in third countries where local branches have access to the original technology but are not subject to the export regulations of the country where the headquarters is based.[5] They can also export sensitive but not regulated items to third countries, which do not impose sanctions on targeted countries of concern, therefore entering a transnational 'grey zone'.

Most international restrictive measures have been imposed by Western states through sanctions regimes and embargoes based on national or multilateral legislation. Less than 40 like-minded states are willing to implement such measures worldwide, while the rest of the international community remains in a 'grey zone', where only restrictive measures adopted by the UNSC are officially enforced. Transfers of listed items from suppliers to these states require an end-user's certificate. However, these markets –nearly 150 countries– offer opportunities for re-transfers to third countries, either due to a weak control of listed items –which contravenes the terms of the contract with the supplier– or to the free trade of non-listed technologies. There are four main reasons for this behaviour:

1. Many states do not share the view that restrictive measures other than UNSC resolutions are legitimate.
2. Even if they do, they may not have the legal, technical and enforcement tools to implement such controls.
3. There are limits in the existing legal tools to intervene or prevent exports of sensitive but non-listed dual-use technologies.
4. Some states depend on 'countries of concern' as arms, technology or energy suppliers, and the assurance of those supplies remains critical to their national security. For these countries, a loss of access to equipment, components or energy supplies constitutes a security threat. This may encourage such countries to facilitate the evasion of sanctions. In many cases, business-oriented policies prevail, creating an alternative chain of supply.

There is no international consensus on what a 'destabilising transfer' or a 'destabilising supply chain' is. Such a disagreement on the definition of a 'destabilising transfer' reflects the nature of the international system, the dynamics of strategic competition as well as different –or opposing– perceptions of regional or international security. For instance, Russia, Iran and the DPRK consider that supply chains that strengthen their own security and the sustainability of their military operations –even at the expense of international security and the territorial integrity of other states– are a 'stabilising factor'. However, this

[5] Many countries participate in multilateral export control regimes with common guidelines and regulations for international trade of weapons and dual-use technologies. Offshore branches of relevant companies in third countries can have access to sensitive technology to produce certain goods and legally export them if they are not subject to the same regulations.

issue is central to geopolitical controversies and cannot be addressed with success in multilateral export control regimes, although it can be a matter of discussion in outreach activities.

The existence of a 'grey zone' of states that formally comply with UNSC resolutions, but do not comply with other restrictive measures (implemented by G-7, EU and like-minded states) or export control guidelines, makes possible the activity of profit-oriented trafficking networks –not necessarily illegal– that exploit the gaps in international sanctions regimes. Countries formally adhering to restrictive measures and export control guidelines but without the necessary legal tools and technical expertise also belong to this 'grey zone'.

Global trade is the setting of transactions of concern, which spread to countries that are not committed to export controls, have different and divergent political views, or do not have the right tools and legislation to address illicit supply chains in their territories. Expanding restrictions or sanctions to third countries in the 'grey zone' would imply establishing restrictions in a market that accounts for half of the world's GDP, seriously distorting international trade.

Both issues –risk-related transactions in transnational illicit trafficking networks and technology transfers in the 'grey zone'– deserve more attention from multilateral export control regimes in the current international scene. Outreach strategies should address these issues, seeking a source of legitimacy for sanctions and export controls, enhancing capacity building and offering alternative chains of supply of critical technologies.

Other challenges for effective export controls: dual-use technologies, derivatives and intangible technology transfers

When addressing the challenges for effective technology-related restrictive measures, some additional factors should be taken into account:

- The growing demand for dual-use technologies. It is important to emphasise that many of these components have a civil purpose and are not included in export control or sanctions lists, since they are of common use in industry and present even in small household appliances.

- Addressing non-listed dual-use technologies is problematic since it affects the legal framework of business activities. National export control agencies do not have legal tools to act against this trade, which falls beyond the current scope of export control regulations. Export controls have relied so far on the use of 'catch-all clauses', which allow national authorities to control any product not listed, but in which exports are considered to go against non-proliferation principles (taking into account factors such as the identity of the importer, the country of destination and a new potential use of the product). However, the frequent use of these clauses for non-listed items is controversial.

- Such non-listed dual-use technologies can be used to upgrade existing military systems with new applications or to manufacture new ones. An importer seeks in the market available technologies able to perform a functional role that has been

previously identified as a need by the end user. Many weapons used by state and non-state actors in asymmetric warfare are the result of 'reverse engineering' and 'reverse designing' derivatives. The acquisition path of sensitive technologies undertaken by state and non-state actors under sanctions frequently starts with commercially available items purchased off the shelf or on the black market. These items are later disassembled to produce replicas, or redesigned and upgraded with other available technologies to produce derivatives adapted to their needs and resources. The products may be of a lower technology standard and performance compared with the original system, but they play a similar functional role.

- The use of intangible technology transfers (ITT). Some of the risks described above also emerge in the form of intangible technology transfers associated with digital transactions, and transfers of technical data in a non-physical form. Export control authorities in supplier countries face legal and procedural challenges related to sensitive intangible transfers.[6]

Direct investments

Direct investments in strategic sectors may result in transfers of technologies integrated into the supply chain of major defence and dual-use contractors. This can occur either through a foreign investment for the acquisition of a domestic company, or through a domestic investment abroad to offshore industrial activity in third countries, not subject to the same export control rules that the parent company must respect. These investments open the way to risks of technological proliferation. This implies the need to have an inventory of such companies and to create an adequate legal framework to scrutinise proposals for take-overs by foreign entities or the relocation of industrial activities abroad. In any case, it is not easy to control emerging technologies in these processes, as their development is mainly driven by the private sector and evolves at a faster pace than the legislative development in strategic investments, sometimes escaping governmental control. These control limitations are further complicated because a large part of these technologies is digital information that can be transferred intangibly. Some international coordination will be needed among like-minded countries.

Following the European Commission Joint Communication on a European Economic Security Strategy (2023),[7] the EC White Paper on Outbound Investments (2024) includes non-binding proposals to prevent the leakage of strategic technologies.[8] In the same way, and under the US Executive Order on Investments in Certain National Security Technologies and Products in Countries of Concern (2023), investors must exercise greater caution when investing in specific foreign countries. The US government now regulates outbound investments in China, and it has a particular focus on safeguarding important technologies that are critical to the country's national security. As part of this effort, the US Treasury Department and other agencies will be

[6] Cloud-based technology has been gaining more interest and investment due to its efficiency in managing computer servers, data storage and networking. However, unauthorised access to these clouds can result in illegally transferring technology through intangible means. This can happen either through stolen or cracked passwords or voluntary cooperation from insiders. It is important to note that cyberspace has no physical borders and customs controls are not enforceable in this realm.
[7] Joint Communication JOIN (2023) 20 final on 'European Economic Security Strategy', 20/VI/2023.
[8] Communication COM (2024) 24 final on 'WHITE PAPER on Outbound Investments', 24/I/2024.

implementing regulations that restrict investments in certain key sectors of China's economy.[9]

Conclusions

So far, efforts to improve export controls have focused on very important tasks, such as following up technology trends, engaging industry and academia, outreaching to non-members and fighting illicit trafficking. The challenges described above have been for many years on the agenda of governments implementing export control regulations and international sanctions. Some elements of a common strategy to improve their effectiveness are: awareness raising in industry and academia to transform them into the 'first line of defence'; addressing gaps in domestic legal tools; increasing the resources of relevant national agencies; and enhancing international cooperation.

Awareness raising in industry and academia

Relations between government export control agencies, industry and academia should evolve towards a cooperative approach. Raising awareness and promoting self-regulation in suppliers of sensitive technologies and technical knowledge will enable them to become part of the 'first line of defence' of national security. Firms and research centres must enhance their 'know your customer' policy and end-user surveillance to ensure their products are not being used in ways that do not align with their ethical and legal commitments, addressing gaps in domestic legislation. Non-listed dual-use items falling in the category of 'sensitive technologies' are usually controlled with catch-all clauses, originally designed for exceptional cases, but frequently used to cover a 'grey area' of international transactions, with a risk of creating legal uncertainties among supplying companies. There is a need for an updated legal framework, including an extensive approach to dual-use technologies and new transactional concepts, as well as specialised training for enforcement investigators. Updated legislation to address non-listed technologies with relevant security or military implications is also necessary, including the conditions of offshore production and supply chains. Legislators and enforcement agencies will also need to assess the parameters of compliance in an intangible space, where traditional customs and enforcement controls cannot be implemented. Intangible technology transfers require a new approach to address new challenges for export controls, such as transactions of sensitive information, where the concept of national boundary is either blurred or simply disappears.

Increasing resources of relevant national agencies

In many cases, export control-related administrative bodies in supplier countries do not have resources adapted to the complexity of sanctions regimes and the growing number of sensitive transactions. The work volume of these transactions constantly increases, just as the number of potentially sensitive technologies, spreading out of the original legal scope of administrative bodies of these agencies, due to a growing demand for dual-use items. However, the human and financial resources of such agencies do not increase at the same pace. These challenges require new tools and more resources for export control and enforcement agencies, including national legal frameworks for special

[9] These sectors include semiconductors and microelectronics, quantum information technologies and technologies that are involved with artificial intelligence. See The White House (2023), 'Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern', Washington DC, 9/VIII/2023.

investigative techniques on the web in order to monitor electronic transfers of sensitive information, under judicial supervision, and in accordance with national legislation.

International cooperation

Finally, the geographic spread of transnational transactions and the growing complexity of illicit trafficking networks in the 'grey zone' require a review and assessment of membership, outreach and engagement policies in multilateral export control regimes, as well as better international cooperation amongst like-minded governments. Such an idea leads to another fundamental issue in this domain: the engagement of non-members in export control policies.