ARI 69/2019
17 June 2019

What next in export controls? Updating criteria and methodologies in non-proliferation and arms control

Gonzalo de Salazar | Senior Advisor for Strategic Affairs and Sanctions Policy Coordinator at the Spanish Ministry for Foreign Affairs, European Union and Cooperation

Theme

The impact of cumulative innovation in technologies requires policymakers and experts to update the current methodology, concepts and tools for non-proliferation, exports control, restrictive measures, arms control and disarmament mechanisms.

Summary

Military and CBRN technologies are evolving rapidly in a cumulative process of innovation, leading to a growing gap between 20th century military assets and modern systems. The accessibility to conventional and CBRN technologies for non-State actors further adds uncertainties to the spectrum of threats that States are likely to face in the years to come. These facts also raise the question of emerging challenges in arms control and non-proliferation policies, in particular for export controls. In a quest to match trade and security interests, policymakers, diplomats and military/technical experts are confronted with a number of specific challenges in multilateral regimes and initiatives: assessing the impact of new technologies on future military capabilities and WMD programmes; preventing a destabilising proliferation of dual-use technologies with military applications; and addressing the resulting conceptual and material outcomes of such an evolutionary process in the methodology for future arms control, non-proliferation and disarmament negotiations.

Analysis

Cumulative innovation, intensive growth and commercial take-off

Past experience shows that technology usually evolves through a gradual cumulative process, based on a combination of new inventions and innovative uses of existing technologies, rather than revolutionary changes in industrial technology with immediate results. “Cycles of invention – commercial exploitation – innovation” develop gradually and usually take a long time to yield significant results. At an early stage, such innovative technologies have little or no relation with existing operational military equipment, due to a conceptual gap between their original design and their potential use in subsequent designs. The latter use has to be ‘rediscovered’ at a later stage, and many technologies are then gradually adapted to military needs, thus improving operational equipment. Such processes have led in some cases to success, followed by phases of technical progress, or to stagnation and even regression in other cases, eventually becoming commercially irrelevant.

The perception of technological innovation in industrial economies is based on the concept of intensive growth (technology as a factor for improvement) versus extensive growth (labour + capital + resources). The last two decades have already witnessed the emergence of new technologies that have transformed production systems and social habits, leading to important qualitative changes in industrial economies in recent years. Most probably, the take-off phase of an intensive growth based on new technologies is yet to come, but once it starts it is likely to fuel worldwide diffusion of dual-use technologies through global trade and off-shoring, resulting in growing challenges for non-proliferation export controls. One of the major reasons for this spread lies in the necessity for advanced technology firms to write off their often costly research and development (R&D) investments by expanding their markets, which implies promoting exports worldwide. Off-shoring policies help to reduce costs by shifting production, assembly lines or manufacturing of components to factories in countries with lower labour costs. Moreover, foreign direct investments lead to transfers of ownership of firms integrated in the supply chain of important defence contractors. All these factors gradually pave the way for proliferation risks, such as direct access to technology and production processes or ownership of sensitive patents by foreign entities and reverse engineering.

Modern innovation is transforming previously non-listed commercial items into dual-use technologies. In recent history, innovation has mostly been based on new ideas being applied to existing technologies and resources, in a process of gradual improvement over long periods of time. In the Information Age, the cumulative effect of such innovations becomes larger and faster, since each new cycle of innovation delivers a stronger technological impact due to synergies reached in combination with other technologies. Market globalization, intangible technology transfers, and off-shoring policies of private firms are among relevant factors that accelerate technology diffusion worldwide. While these trends are positive in terms of the improvements in productivity, expansion in trade and increase in economic growth, they also represent important challenges for supplier countries, which require adequate regulatory tools to effectively implement export controls.

Such knowledge and technologies may not be listed as controlled items at that stage. However, many dual-use technologies that are not listed as ‘military controlled items’ might be relevant for future WMD or conventional weapons programmes. Export control agencies, through international interaction, determine which weapons, sensitive dual-use technologies, and related materials must be controlled. The same logic is applied to technology-related restrictive measures.[1] But innovation often transforms previous non-listed commercial items into present and future dual-use technologies. Technological change through cumulative innovation outpaces our ability to update lists of controlled items in national and multilateral export control mechanisms. This is particularly important in industries operating in the nuclear, chemical, biological, aerospace and military sectors.

[1] Some UNSC resolutions on sanctions use the annexes of the Nuclear Suppliers Group and the Missile Technology Control Regime as technical references for the implementation of restrictive measures.

While 'traditional defence sector' companies have always had a solid security culture, based on specific confidentiality regulations, this may not be the case for some commercial firms from the civilian dual-use sector, which may eventually become suppliers to defence prime contractors. Some of these challenges may lead to a proliferation of sensitive and dual-use technologies, including machine-tools. Commercial and market-oriented companies –especially those producing and supplying dual-use technologies– are more exposed to the risk of unintended sensitive transfers to destinations of concern.

In this regard, the production and availability of technologically advanced components and machine-tools is of particular relevance, since they play a primary role in industry, but also in the construction of advanced military platforms. Some examples of this trend are: software and computers; propulsion systems; video technology; robotics; nanotechnology; autonomous vehicles and remote-controlled systems; and technologies associated with space applications.

New materials, such as carbon fibre and graphene, are also essential in modern industry. New production systems, such as additive manufacturing, are used in different sectors of industry, building objects by adding ultra-thin layers of material one by one: plastic prototypes, ultrasound machines, gas turbines, aeronautics, medical implants, etc. The use of these technologies in the production of military platforms is growing, especially in aeronautics.[2] The potential of new technologies in the defence sector is enormous. As a result, the control of all these technologies is becoming not only a commercial advantage for industry, but also a strategic asset.

New technologies, weapons and tools to make weapons: tangible and intangible

Our past experience in arms control, non-proliferation and disarmament methodology has been based on hardware, materials and physical platforms accounting and monitoring. The international agreements negotiated in the 20th century established quantitative ceilings to limit military capabilities and determine the rationale of strategic balances. Examples of this approach are the Treaty of Versailles in 1919 after the end of World War I; the Naval Treaty of Washington, signed in 1922; or, more recently, the Treaty on Conventional Forces in Europe, since 1990. Other treaties in the second half of the past century established non-proliferation principles, where a quantitative approach to tangible assets was the method to determine compliance, based on measurable materials. Such is the case of the Non-Proliferation Treaty and the Chemical Weapons Convention, which rely on a verification and accounting system of safeguards and inspections, implemented by the International Atomic Energy Agency and the Organisation for the Prohibition of Chemical Weapons respectively. The Arms Trade Treaty follows the same philosophy in its information exchange mechanism: reporting on tangible transfers.

[2] New generations of machine-tools function in combination with advanced programming and simulation software to manufacture flat, mild curvature, complex shapes and high-contour aerospace components. Computer-controlled additive manufacturing machines make lighter parts and components in a faster process, reduce production costs, and yield significant fuel savings for aircraft.

However, the impact of new technologies and intangible assets on conventional and WMD capabilities is likely to grow in the years to come. As an example, due to new trends in information technology, the use of cyber weapons against nuclear, chemical and critical infrastructure may become a threat that will be difficult to assess with current conceptual tools. Therefore, given the extensive use of dual-use applications and intangible assets integrated in modern military systems, the quantitative approach may not be sufficient in the future. The same rationale is applicable to export controls, where software, electronics and other non-lethal technologies determine the capabilities, precision and effectiveness of modern weapons systems.

Some of the risks described above also emerge in the form of intangible technology transfers associated with digital transactions: the transfers of technical data in a non-physical form, including available encryption software, email exchanges of documents related to sensitive information, online consulting, access to cloud-based technologies and other procedures in wireless telecommunications networks. Export control authorities in supplier countries face increasing challenges related to sensitive Intangible Technology Transfers (ITT) due to functional symbiosis of industry and academia, the presence of foreign nationals in domestic high-technology sectors, the mobility of qualified personnel or the access to global information technology networks and digital-electronic methods of intangible transfers.

Some of these challenges may be associated with the potential proliferation of sensitive and dual-use technologies, as well as the uncontrolled diffusion of intellectual property rights. For more than three decades, firms and academic institutions have had their own corporate data centres. However, there is an increasing interest and investment in cloud-based technology, an efficient method of managing computer servers, data storage and networking. Access to clouds by unauthorised persons can lead to illicit trafficking of technology through intangible transfers, either with stolen or cracked passwords, or with voluntary cooperation from insiders. There is no physical border in cyberspace, where custom controls are not enforceable. But ITT are transactions between tangible sources and recipients using physical hardware. This should allow a better protection of sensitive intangible asset technologies, as well as prevention and deterrence of illicit ITT in the context of export controls. There is a growing need for an updated legal framework and specialised training for enforcement investigators. New specific policies and best practices for effective enforcement are required to update definitions of what constitutes an ITT export and when an ITT export occurs, in order to specify in national regulations which knowledge and technology transfers must be subjected to export control and what information transfers must not be restricted, eg, because the information is widely publicly available or constitutes harmless basic scientific knowledge.

At the same time, it is necessary to identify industry, research centres, universities and individuals that have access to sensitive technology in order to undertake targeted outreach efforts and, if possible, also promote self-regulation, based on cooperation with export control agencies, including by designing and implementing internal compliance programmes, encouraging appointment of export control points of contact and enhancing codes of conduct. Such measures supplement risk analysis procedures in visa-vetting methods, including profiles following the model used in granting licences for transferring defence and dual-use material, and sensitive areas which could make ITT possible or

facilitate them. Furthermore, raising awareness and self-regulation in sensitive suppliers enables them to become the 'first line of defence', controlling sensitive technology at the source. This is already being done in many countries through 'compliance programmes' and 'know-your-customer' policies, but only when such companies are active in supply chains and exports that are already declared sensitive. Finally, these challenges require new tools for enforcement agencies, including national legal frameworks for special investigative techniques in the web in order to monitor electronic transfers of sensitive information, under judicial supervision, in accordance with national legislation.

Innovation and new applications of existing technologies: the conceptual gap

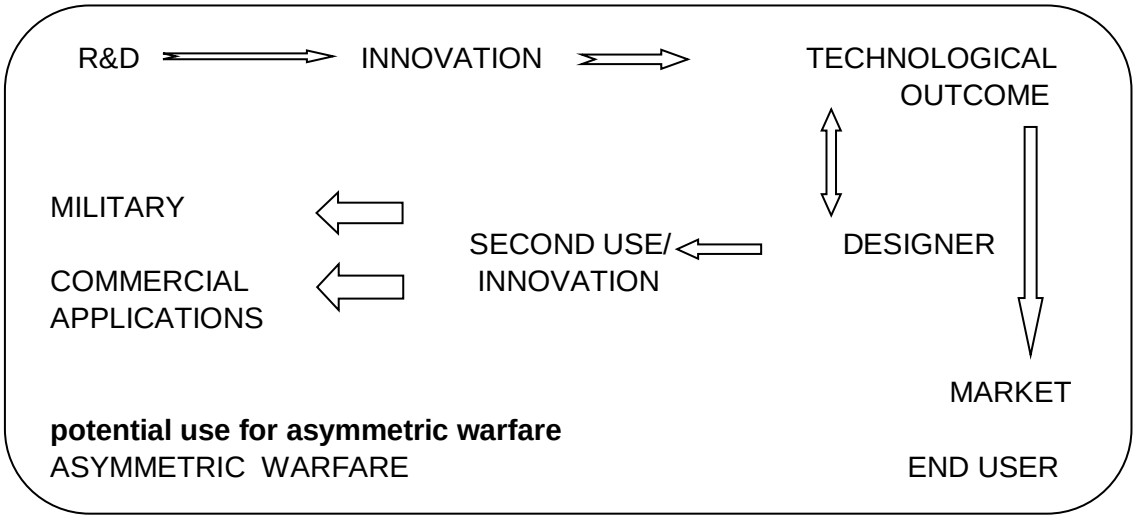
Throughout history there have been cases in which the original design and intended purpose of innovative technologies were used for specific applications, which were entirely different from their use in differing subsequent designs or systems. The latter use had to be 'rediscovered' at a later stage, and many of these technologies were gradually adapted both to commercial and military needs, thus improving operational equipment and commercial technologies. In the 18th century the steam engine was initially designed for the textile industry, but it was successfully adapted to trains and vessels in the 19th century. The GPS was designed for military purposes, and a few decades later became commercially available and widely used for civilian applications. Cell phones, specifically designed for wireless communications, have been used as remote-controlled detonators of improvised explosive devices in terrorist attacks. Between the original design and purpose of innovative technologies and their potential 'rediscovered uses' there is a conceptual gap,[3] due to lack of awareness or purpose to use them in new and different applications.

This conceptual gap can be identified when innovation is not intended or focused on a particular goal at a given time and is conceived by a designer/developer unaware of its full potential. The analysis of a conceptual gap requires an assessment of the innovation process to compare the original purpose of the technology with other potential uses of the same technology as reflected in Figure 1. The need to expand markets and recover R&D investments leads to the search for new applications and functions of existing technologies. In this process, the interaction between designers and end users is essential, since it is often demand from the latter which leads to new findings. In this regard, innovation plays a role in two parallel functions:

(a) Existing and new dual-use technologies are used to upgrade existing platforms and systems with new applications. The latter play the role of enablers.
(b) New designs of technologies for innovative applications are used to construct new platforms and systems.

[3] Gonzalo de Salazar Serantes (2018), *Crimen y conflicto armado*, MAEC, Madrid, p.199-201.

Figure 1. The development of conceptual gaps



The conceptual gap is bridged with a deductive and functional approach: a designer or researcher seeks existing technology that is able to perform a functional role that has been previously identified as a need by the end user. In this process there is an issue of particular relevance concerning capabilities for asymmetric warfare. While cases of "reverse engineering" of military and dual-use technologies by state-sponsored entities are widely known in the context of "technology flows" leading to industrial production, the acquisition path of sensitive technologies undertaken by non-state actors usually starts with commercially available items purchased off-the shelf or on the black market. These items are later redesigned and upgraded with other available technologies to produce derivatives – not replicas – adapted to their needs and resources. This product may be of a lower technology standard and performance compared to the original system, but it plays a similar functional role. Many weapons used by non-state actors in asymmetric warfare and terrorism are the result of "reverse designing" derivatives[4].

In the context of asymmetric threats, the existence of such conceptual gaps in chemical, biological, radiological and nuclear (CBRN) systems requires a specific approach. Often associated, rightly or not, to weapons of mass destruction, CBRN materials are part of a more complex system with production facilities, means of delivery, CBR agents, nuclear devices, explosives, detonators, guidance systems and particular vulnerabilities, eg, to sabotage through cyber-attacks. The outcome of innovative processes is diverted and integrated into existing CBRN devices, in which CBRN materials are part of a more complex system. The complexity of CBRN systems and their enhancement through integration of dual-use conventional technologies are usually ignored when the two – conventional and non-conventional technologies– are defined as separate categories.

[4] An example of this process is the ability of some guerrillas to transform commercial UAVs and use them on the battlefield, surface-to-air missiles adapted to surface-to-surface functions or portable rocket launchers based on modified models of self-propelled grenades, built with plastic components using injection moulding machinery, steel and aluminium.

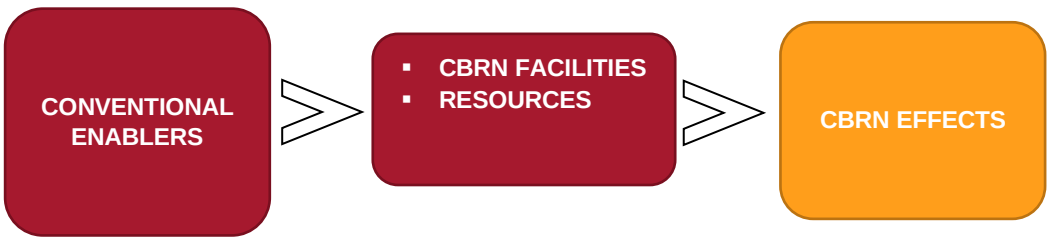
Moreover, risk management –based on the safety/security standards implemented in a CBRN facility– is also a relevant factor in export control. If they are not protected, these technologies and materials can be stolen at the facility, diverted to other purposes or used against the receiving State or other countries (including the supplier country). As a result, two elements can be identified as characterising conceptual gaps in CBRN.

First, and from a technological perspective, CBRN systems cannot be conceived as an isolated category. They are integrated in a complex spectrum of technologies, ranging from conventional to CBRN elements, including dual-use technologies. CBRN systems differentiate conceptually from conventional systems due to their fallout and consequences, the legal framework in which they are categorised as well as certain ethical considerations, due to their usual association with WMD. But they are, in effect, integrated in a complex and comprehensive continuum of diverse technologies, where conventional and non-conventional technologies are blended and only then possibly formed into a CBRN weapon. Therefore, controlling the spread of CBRN materials is insufficient for achieving non-proliferation, since complementing conventional or dual-use technologies usable for the weaponisation of these materials need to be regulated, too.

Figure 2. From CBRN material to non-conventional systems

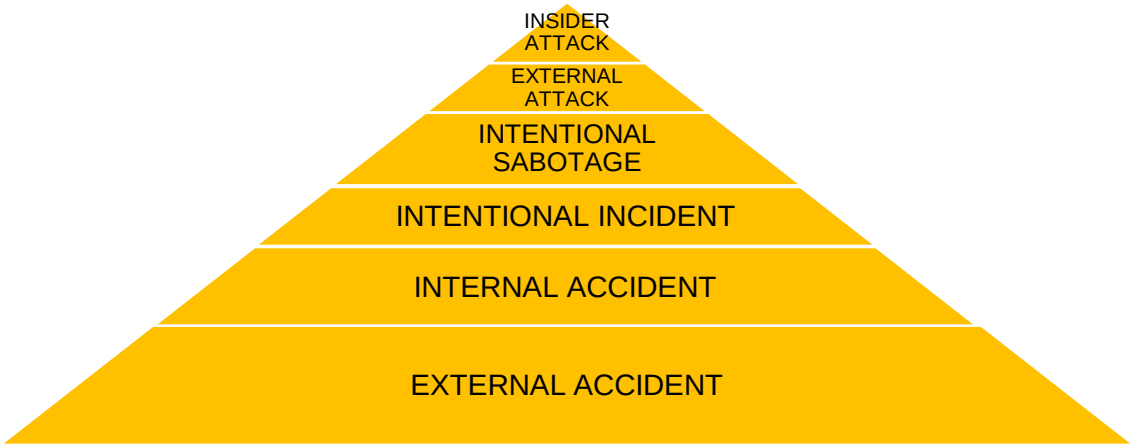
Secondly, CBRN outcomes can also be achieved by state or non-state actors with conventional enablers and without themselves owning CBRN material, by attacking CBRN facilities and infrastructure.

Figure 3. From conventional enablers to CBRN effects



This perspective is particularly important when dealing not only with terrorist threats but also in a hybrid war context: insiders, militia-type agitators and hackers can all use conventional systems to achieve harmful CBRN outcomes as shown in Figure 4.

Figure 4. Risk management in CBRN facilities



Coordination and assessment of information through national prevention-defence-resilience hubs is important for monitoring critical infrastructure and improving situational awareness, enhancing the ability to connect seemingly unrelated events which might be symptoms of a hybrid attack.

Conclusion

The way ahead: measuring intangible assets and anticipating technologies' potential outcomes

Weapons systems, dual use technologies, technical production systems and their different applications bear not only the legacy of knowledge, but also the traces of evolution in human behaviour. In this regard, the process is characterised by a tempo marked by relevant inventions and industrial highlights, as well as a long-term perspective of evolution where elements of a technical-industrial legacy find new roles assigned by human creativity. In summary, the time is ripe for considering a gradual update of the methodology for non-proliferation, exports control, restrictive measures, arms control and disarmament mechanisms. New concepts and tools will be required to assess the relevance of technologies and capabilities, both conventional and non-conventional, based on tangible and intangible factors.

The impact of cumulative innovation in technologies with potential use in CBRN and conventional weapons programmes, including manufacturing systems, has become a major challenge for policymakers and experts in the security, non-proliferation and disarmament community. In particular, export control authorities and military experts will need to assess the consequences of future innovation on existing controlled platforms.

At the same time, enforcement agencies will need to assess the parameters of compliance in an intangible space. Intangible technology transfers –where traditional customs and enforcement controls cannot be implemented– require a new approach to address new challenges for export controls, such as information transactions where the concept of national boundary either is blurred or simply disappears.

This intellectual exercise will also require a methodology to define the conceptual gaps between the 20th-century designed operational weapons systems and an innovative use of new technological resources or dual-use applications for military purposes. This implies reflecting on possible mechanisms to assess and identify the potential dual use of commercial technologies, which may not be integrated in existing controlled systems at present but might be relevant for future weapon designs and programmes.

Technological observatories, qualitative indicators of capacities based on innovative technologies, as well as new conceptual and impact evaluation models, would be useful regulative tools in this context. Further efforts in this area could include not only an assessment of the transfers to be monitored and the gaps to be bridged, but also a deeper analysis of relevant factors in technological proliferation.