THE ROLE OF INTANGIBLE TRANSFER OF TECHNOLOGY IN THE AREA OF BALLISTIC MISSILES – REINFORCING THE HAGUE CODE OF CONDUCT AND THE MTCR

By Arnaud Idiart,
Group French Export Compliance advisor, Airbus

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of the FRS and can under no circumstances be regarded as reflecting the position of the European Union.

Table of Contents

A. CLARIFICATION OF THE TOPIC AND THE MAJOR ASPECTS FOR CONTROLLING PROLIFERATION

WITHDRAWAL OF THE SOVEREIGN CONTROL AUTHORITIES: TRANSFER OF RESPONSIBILITIES TO EXPORTERS AND WEAKNESS OF INDUSTRIALISTS

FOREWORD

This contribution written within the specific framework of improving the fight against the proliferation of weapons of mass destruction, recalls the respective roles of governments and private players as well as the universal general principles of export control.

In its international dimension, **export control as it works today, has gradually developed and is still developing via a process aiming for optimisation and thus compromise. To avoid fracturing the system, any new development must be guided by caution. This paper therefore extensively focuses on analysing the existing situation.**

It indeed seems essential, in a field as complex and as politically and economically sensitive as security, that any proposals for lasting improvements be based on "business" foundations, described as clearly as possible.

These proposals are based on experience. They seek to be pragmatic and primarily reflect the expectations of economic operators. However, with a view to optimising a fundamentally governmental system, the writer hopes that, through this corporate vision, these findings and proposals will give lawmakers the confirmation and operational bases they may be lacking.

PREAMBLE

Export control of sensitive goods is, by nature, a constantly evolving activity. **In terms of guaranteeing the security of nations, export control is no doubt one of the most powerful instruments of foreign policy**, enabling exporting countries[1] to send out strong diplomatic signals of either alliance or disagreement to all nations[2]. For example, in matters of sanctions, sector-specific, partial or general embargoes almost immediately target deliveries of high-tech products

1 cf. SIPRI - "Trends In International Arms Transfers, 2016" by - Aude Fleurant, Pieter D. Wezeman, Siemon T. Wezeman and Nan Tian – (https://www.sipri.org/sites/default/files/Trends-in-international-arms-transfers-2016.pdf) :"*The five biggest exporters in 2012–16 were the USA, Russia, China, France and Germany. Together, they accounted for 74 per cent of the total volume of arms exports*".

2 For memory, in the year 800, the quality of Frankish swords gave the empire real supremacy, so Charlemagne banned the sale of these swords outside his territory. By the Edict de Pistres, in 864, Charles the Bald confirmed this prohibition and even extended it (by banning blacksmiths from working outside the Kingdom) to control of Frankish "high technology" particularly in alloys and quenching!

and weapons, the latter very often being closely linked to the former. To keep up with the internationalisation of production and globalisation of supply that gained speed as of the second half of the 20th century, the centre of gravity of sensitive goods control shifted from finished, turnkey systems, to equipment and then components, and finally to technology. It is indeed the know-how necessary to produce basic parts and particularly the know-how required to design complex systems that gives a country real autonomy, and thus the means to proportionally mitigate the influence of and pressure from its historical suppliers. This industrial redistribution in fact triggered the first changes in control of military goods and high technology. For example, in the 1980s in France, except for combat aircraft, the French arsenals, grouped together in a State industrial sector by the "Délégation Générale pour l'Armement" (DGA), still produced most military equipment and particularly the complex weapon systems necessary to guarantee the nation's total military independence, including in space and nuclear. The various sectors of armament were then gradually privatised and entrusted to industry. Today, the Délégation Générale pour l'Armement (which became the Direction Générale de l'Armement[3] in 2009), has practically no industrial activity. It acts as a contracting agency for the complex structures that French military resources represent. The government has therefore successively lost its competency in industrial production and thus today a substantial part of its research and development resources.

This process has prompted historically arms-producing nations to rethink their approach to export control of sensitive goods. In France and the USA in particular, government activities have been transferred from the State to the private sector, with control of the relevant exports shifting from an exclusively "ex ante" to an "ex post" system.

Regarding technology transfer more particularly, control may be necessary from the first stages of research[4]. To facilitate the self-classification of technologies used to produce defence or dual-use goods, the French control authorities have recently announced that, save exceptions[5], an export licence application is mandatory for technical data relating to controlled products as of level five (laboratory validation of components and/or models) on the TRL (Technology Readiness Level) scale, which defines the nine successive degrees in technology finalisation. **The "ex ante" control** of the exported technology is therefore only **triggered by the exporting manufacturer once it considers that its invention will be used solely for military purposes** or that its diversion for military use is likely.

As we can see, **this approach to control greatly relieves the Government of its responsibility for regulatory compliance in exports**. At the same time, if the situation deteriorates within the receiving country, or if the supplied products or technologies are not used as expected, **it increases the risk, for the EU industrial community** in particular, **of businesses being directly put in issue** by the media, politicians or even by international public opinion. As

3 French Decree no. 2009-1180 of 5 October 2009 establishing the powers and organisation of the Direction Générale de l'Armement. Disappearance starting in 1990 of the Direction des Armements Terrestres (armoured vehicles and artillery), then of the Direction des Constructions Navales (surfaces ships, SSN and SNBN), of the Direction des Constructions Aéronautiques (supervisory authority of DASSAULT AVIATION) and of the Direction des Engins, the supervisory authority of AEROSPATIALE (cargo and training aircraft, military helicopters, ballistic missiles and observation satellites).

4 Just after the observation level or description of fundamental scientific laws.

5 Particularly as regards technologies related to the Proliferation of Weapons of Mass Destruction (Nuclear, Biological or Chemical).

a result, **in a matter of decades, accepting this image risk has become the price that defence industrialists must pay as they face increasingly intense competition** from new entrants whose governments may not be as media-sensitive. This growing trend has been particularly noticeable since the arrival of new entrants on the global market such as Ukraine, China or Turkey[6].

Faced with this situation, the role of international control circles (including the MTCR[7] and The Hague Code of Conduct) is particularly important. Only politically binding adherence, encouraging international dialogue and aiming to enhance collective security, can gradually erase the behavioural differences created by foreign policy excessively centered on national considerations.

1. REMINDERS: CONTEXT AND CHALLENGES OF EXPORT CONTROL

1.1 RESPONSE TO EVOLVING TECHNOLOGICAL RISKS

The 1957 launch of Sputnik by the USSR was a scientific achievement that enabled the public to understand the importance of space. It took place at the heart of the "Cold War" and naturally opened up new prospects for certain military strategists who saw the opportunity for new conquests: the fight to seize new territories, and then defend or at least control them.

Faced with this real risk, in 1959 the United Nations General Assembly set up a "Committee on the Peaceful Uses of Outer Space". This committee is at the root of the UN's five major international treaties[8] which today form the basis of the law of Space, as well as five important UN General Assembly resolutions that complete them[9]. Work on the proliferation of ballistic missiles regulates military use of launchers using outer space and thus completes the general framework defined by these provisions.

6 cf. SIPRI - "Trends in international arms transfers, 2016"; compared to the 2007-2011 period, exports from China, Turkey and Ukraine respectively increased by 74%, 180% and 49%, to the detriment of France -5%, Germany -36% and the Netherlands -11%.

7 Missile Technology Control Regime

8 The five major international treaties are:) the "Outer Space Treaty"; the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (672 *UNTS* 119); the Convention on International Liability for Damage Caused by Space Objects (961 *UNTS* 187); the Convention on Registration of Objects Launched into Outer Space (1023 *UNTS* 15); and the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (18 *ILM* 1434).

9 The five main resolutions are:) the 1962 resolution (XVIII) containing the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space; resolution 37/92 on the Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting; resolution 41/65 on the Principles relating to Remote Sensing of the Earth from Space; resolution 47/68 on the Principles Relevant to the Use of Nuclear Power Sources in Outer Space, adopted on 14 December 1992; resolution 51/122 containing the Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries.

Export control of products has thus followed the ramp-up of the space activities they supply. While launchers were indeed initially employed for scientific purposes, they swiftly found military applications, and gave rise to "ballistic missiles".

In parallel, as of 1968, with The Nuclear Non-Proliferation Treaty (NPT)[10], international institutions legislated on the risks of proliferation of weapons of mass destruction (WMD)[11].

As potential means of delivering these nuclear, bacteriological or chemical "WMD", missiles represent an unsettling threat for peace and security, on both a regional and international scale.

Thus in 1987, a G7 work group (Germany, Canada, France, Italy, Japan, UK and the USA) was tasked with defining rules for the export of equipment and missile technologies that could be used to build nuclear weapon delivery systems[12]. The States integrated weapons of mass destruction and launchers into their national export control lists quite early on, but only later did they set about regulating export control of potential means of delivery of WMD on an international level[13].

Finally, **it was not until 2002 that The Hague Code of Conduct Against the Proliferation of Ballistic Missiles**, the "HCOC"[14], **introduced the first multilateral political instrument against the proliferation of ballistic missiles**[15]. And it took until **2004,** with the UN Security

10 729 UNTS 161. https://cil.nus.edu.sg/rp/il/pdf/1968%20Treaty%20on%20the%20Non-Proliferation%20of%20Nuclear%20Weapons-pdf.pdf

11 Since the early 1990s, the range of certain countries' ballistic missiles (excluding nuclear-armed states) such as Iran has swiftly increased, causing concern.

12 In 1992, the scope of application of the MTCR was extended to weapons of mass destruction (WMD). This work resulted in a political arrangement called Missile Technology Control Regime or MTCR.

13 In France, it was not until the order of 20 November 1991 (*JO* of 22 November 1991 – NOR: DEFM9101820A) listing the ordnance and similar equipment subject to a special export procedure. In Europe: Regulation (EC) no. 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology applies to 1) "Missiles" (complete rocket and unmanned air vehicle system capable of delivering at least a 500 kg payload to a range of at least 300 km) and propulsion systems, space vehicles and related equipment: (Category 9a004 space launch vehicles and "spacecraft").

14 http://www.hcoc.at/documents/Hague-Code-of-Conduct-A_57_724-French.pdf. The final text of the Code was adopted in The Hague on 26 November 2002 by 93 States; in June 2016, 138 States were signatories. The HCOC stems from work done by the members of the Missile Technology Control Regime – "MTCR" – introduced in 1987, to combat the proliferation of weapons of mass destruction – "WMD" – (essentially nuclear arms). Indeed, "The members of the MTCR, having acknowledged that export control could not be the only answer to the proliferation of missiles, sought as of the 1999 Noordwijk plenary meeting, to adopt a new instrument to regulate the States' action in this area. Today, the MTCR has 35 member countries: South Africa (1995); Germany (1987); Argentina (1993); Australia (1990); Austria (1991); Belgium (1990); Brazil (1995); Bulgaria (2004); Canada (1987); Denmark (1990); Spain (1990); USA (1987); Finland (1991); France (1987); Greece (1992); Hungary (1993); India (2016); Ireland (1992); Iceland (1993); Italy (1987); Japan (1987); Luxembourg (1990); Norway (1990); New Zealand (1991); Netherlands (1990); Poland (1998); Portugal (1992); Republic of Korea (2001); Czech Republic (1998); United Kingdom (1987); Federation of Russia (1995); Sweden (1991); Switzerland (1992); Turkey (1997); Ukraine (1998)."

15 In the 1950s, the Soviets implemented liquid-propellant missiles resulting from a quite easily copyable technology (Scud type: 300 km range for a payload of approximately 1,000 kg). Since the early 1990s, we have seen the range of ballistic missiles of non-nuclear-armed States (within the meaning of The Nuclear Non-Proliferation Treaty "NPT") swiftly increase. For example, at the end of the 1980s, the Iranians mastered the Shahab-1 missile (Scud-B) with a 300 km range. Supported by North Korea, they initially increased the range to 500 km and produced the Shahab-2 (Scud-C). Then, as of 1998, they performed multiple tests on a missile now assumed to be operational, the Shahab-3 (with an estimated range of 1,300 km) and worked on developing new versions with the aim of reaching a 2,000 km

Council **resolution 1540**[16], for the provisions defining WMD to include the terms "***and their means of delivery***".

The HCOC contains three fundamental commitments: 1) a general commitment to exercising restraint in the development, testing and deployment of ballistic missiles and not to contribute to proliferation; 2) a strong political commitment aiming to implement and comply with transparency measures (such as the annual declaration of ballistic and space programmes or pre-launch notifications of ballistic missile and space launch vehicle launches) and, 3) recognition that the States must not be deprived of the use of Space for peaceful purposes (but without space programmes serving to conceal military ballistic programmes). In practice, as a precaution, most exporting nations today classify and control rockets and space launch vehicles as military products[17].

1.2 CONSTANT INTERNATIONAL REINFORCEMENT

Furthermore, with a view to improving harmonisation of export control practices, and to restrict the stockpiling of conventional weapons but also to reinforce control over the non-proliferation of WMD, on 25 May 1998, the Council of the European Union adopted a new text entitled: "European Union Code of Conduct on Arms Exports". This Code sets out various principles and criteria for granting export licences, common to all Member States, in the area of arms exports. It also seeks to improve transparency and the States' responsibility for arms transfers to third countries to tend towards an increasingly common policy on exportation of war equipment out of the EU. The twenty-seven Member States of 2008 were then prompted, particularly by the European Parliament, to enshrine the principles of the Conduct of Conduct in a "Common Position"; thus on 13 December 2008, the European Council Common Position 2008/944/CFSP of 8 December 2008 was adopted[18].

Although it was legally reinforced by this "Common Position", the Code of Conduct is above all a politically binding instrument for Member States. While this text could possibly be considered legally binding, the likelihood of one of the 28 EU Member States making a formal complaint to the European Court of Justice, and of a penalty being imposed, is practically inexistent.

---

range *(Cf.* the very detailed study: SAMORE, G. (dir.), *Iran's Strategic Weapons Programmes – A Net Assessment*, International Institute for Strategic Studies, London, 2005). An international framework was therefore urgently needed to meet the rampant threat of the proliferation of WDM delivery systems…

16 On 28 April 2004, the Security Council unanimously adopted resolution 1540 (2004) pursuant to Chapter VII of the United Nations Charter, wherein it confirmed that the proliferation of nuclear, chemical and biological weapons and their means of delivery constituted a threat to international peace and security and decided that the States should, *inter alia*, refrain from supporting by any means non-State actors from developing, acquiring, manufacturing, possessing, transporting, transferring or using nuclear, chemical or biological weapons and their delivery systems. http://www.un.org/fr/sc/1540/about-1540-committee/general-information.shtml.

17 cf. Wassenaar Arrangement (41 countries): category 9.A.4.: "Space launch vehicles, "spacecraft", "spacecraft buses", "spacecraft payloads", "spacecraft" on-board systems or equipment, and terrestrial equipment, etc."

18 OJEU L335/99 of 13 December 2008. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:335:0099:0103:fr:PDF).

However, despite this legal weakness (which is regularly criticised by certain lobbies for political purposes), the Code is in fact very effective. By making exporting governments solely responsible for their decision to follow the criteria of the Common Position or not, it does not undermine the fundamental principle of national sovereignty. **In practice therefore, the absence of a judge in a system based on voluntary adherence naturally leads each partner to practice "responsible" self-censorship.** Any occasional breach would inevitably oblige the perpetrator to, in turn, reciprocally accept another partner's transaction, even though it would rather condemn it.

1.3 DIFFICULTIES AND LIMITS CONTROLS

First, it should be noted that **a great many consumer products can be diverted to military or illegitimate uses**. This is even truer of any "sensitive" product initially controlled as a military or dual-use item, but which is not or is no longer covered by control lists due either to its obsolete design, or to its inferior performance compared to new generations. To combat such diversions, a system relying on the collective vigilance of both exporters and government agencies has thus been introduced. It is known, and officially established by the EU Regulation on dual-use items, as the Catch All clause[19].

This issue of the potential diversion of equipment or components naturally arises in respect of the information and know-how that give rise to the finished goods. Understandably, introducing a general system of control by all countries, for the possession and trade of all products, is not a reasonable option. **The grounds for implementing the "catch all" clause are therefore limited in practice (at least for now[20]) to the risk of military diversion by countries under arms embargo and to the proliferation** of nuclear, bacteriological and chemical weapons (WMD).

Faced with the complexity and variety of products, experience has shown that control is ensured with optimal efficiency if it is concentrated and specialised by area of application[21].

To best ensure their national security, mutually and reciprocally, and thus contribute to greater international security, States today agree to control, firstly, products specially designed or modified for military use (classification by nature) and secondly, products that are not military by nature but

19 CF. Articles 4 and 8 of EC Regulation 428/2009 of 5 May 2009.

20 The draft reform of the current EU Regulation on dual-use items (EC 428/2009) provides for an extension to risks of human rights violations and terrorism. We can naturally only welcome this drive to promote moral standards and to reinforce security. However, the lawmaker plans to make the operators responsible for this vigilance, overlooking the fact these two new criteria are essentially political by nature and that companies have neither the legitimacy nor the resources (human and financial) to substitute for these truly governmental functions.

21 In this vein, the Wassenaar Arrangement control lists include items detailed by other international regimes such as the MTCR or the NSG. It therefore contributes to informing exporters of the sensitive nature of products. Operators that are aware of the origins of controls can better define the possible reasons for diversion and therefore monitor particular risks of use or end users.

Thanks to a meaningful codification, each entry in the Arrangement list consists of at least 5 digits, the third of which indicates the origin of the controls: 0 = Conventional arms; 1 = MTCR; 2 = NSG; 3= Australia Group; 4 = CWC;

whose performances could bestow a certain superiority on anyone possessing or using them (classification by purpose).

Traditionally, the classification of sensitive products is thus based on two key concepts: performance and specificity. In practice therefore, it is necessary to determine 1) whether the product is "*specially designed or modified for military use*" and**, if it is not 2) what additional power the product in question can give someone that has it**. The first question aims to combat the potentially destabilising stockpiling of conventional weapons and equipment. In addition, trade and possession of military firearms are, for reasons of internal security, subject to extra "ad hoc" controls both on the national territory and when exported. Once the effective military or non-military nature established, the second question attempts to anticipate and manage risks of diversion. To do so, the focus is placed on the product's performances and intrinsic capabilities. For example, Iran has recently been found procuring commercial gyroscopes, available via the Internet, to build armed drones[22]. Thus, **control of "dual-use items by nature" is done "by purpose"** and takes into account two complementary risk factors: 1) is the end user considered "suitable" by the exporting government, and its allies and partners? 2) Is the end use of the exported product legitimate, having regard for international criteria? Products must not serve illegitimate interests, be it for purely civil or specifically military purposes. But, although some products are "non-military" by nature, there is a real risk that they might be used for potentially illegitimate purposes, such as the "Proliferation" of weapons of mass destruction.

With a view to making recommendations to improve export control, reinforcing product classification is no doubt one of the means to be favoured.

1.4 PRODUCT CLASSIFICATION

For reasons of both cost and efficiency, the following two principles should be applied.

Define simple criteria and only subject product categories to a special regime where this is unquestionably warranted. The highly pragmatic approach taken by the Obama administration in the USA for the control reform initiated in august 2010 could serve as inspiration here. This reform provides a good example of the advantage of selecting products by family and sub-family ("semi-generic" rather than product reference by product reference), as it reduces the administrative burdens while guaranteeing good quality control.

In practice, such an analysis relies on introducing two criteria: firstly, "**the commonness of supply**", representing the reality of supply on the international market; and secondly, the performance of each function that the product fulfils, i.e. its technical-operational nature.

In this way, the analysis and classification of defence-related products retain their logical basis of an approach by nature: "*specially designed or modified for military use*". But above all, this functional

22 Since the start of the conflict in Yemen, Ansar Allah 'Houthi' forces, and those aligned with former President Ali Abdullah Saleh, have deployed increasingly sophisticated weaponry. This includes Iranian 'Kamikaze' drones (Qasef-1 of the Ababil-II family manufactured by "Aircraft Manufacturing Industrial Company (HESA - Head office No. 107, Sepahbod Gharany Ave., Teheran), used to attack the Saudi-led Coalition's Patriot anti-missile defence system. http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwj64Yb5ruLTAhVM0xoKHduTBjUQFggrMAE&url=http%3A%2F%2Fwww.conflictarm.com%2Fdownload-file%2F%3Freport_id%3D2465%26file_id%3D2467&usg=AFQjCNGcU8qZbcpKucKeVq96YeA7MgdKrA

logic requires the necessary pragmatism to deal with an increasingly diverse supply: "*Few products to control for improved control*". **Today, some investigations are indeed still done out of pure technocratic "necessity", justified by concern to fully comply with regulations but ultimately ineffective in terms of combating diversion**; these obsolete relics from another age are costly for both industry and government.

Control of intangible transfers should be linked to that of physical items.

The dichotomy that still prevailed in the 1990s between technologically advanced, arms-producing countries (a tiny minority) and a very large majority of finished-product-consuming countries is gradually disappearing. Yesterday's customers are progressively becoming subcontractors, then co-contractors and finally partners or even competitors that cannot be ignored. **New entrants are now only rarely interested in "turnkey" products; today, they mainly want to acquire the know-how they need to develop their own production.**

Countries naturally shift from consumer to producer status as their national economy develops. To guarantee their independence and national sovereignty, they must have control over strategic production capacities. In parallel, achieving this autonomy comes with increasing wealth and the need to protect it, just like the territory. Today therefore, control of "technologies" encompasses control over knowledge and know-how. It covers the questions of developing, retaining and protecting increasingly complex national competencies requiring all-round stakeholder involvement, i.e. governments, researchers and industrial exporters. As stated, the identification and classification of products to be controlled is a vital condition to ensure the right level of control. Simple rules are therefore necessary so that all the players actively contribute to the process. **To objectify the sensitive nature of intangible knowledge transfers, one good rule consists in classifying product information in the same way as the product itself, by establishing the following principle: "*all information that could be used to reproduce the equipment or impair its efficiency is controlled*".**

Once product classification has been mastered, overall improvement of export control involves, in practice, examining two other decisive aspects for granting licences.

1.5 PRODUCT NATURE AND PURPOSE: TWO DECISIVE LICENCE CRITERIA

Firstly, the public or private nature of the final destination of exported products is a decisive factor for granting export licences or authorisations. Secondly, it is important to bear in mind that all major exporting countries more or less follow the eight criteria laid down by the "EU Code of Conduct on arms export control"[23]. Moreover, other more technical and operational considerations complete the authorities' analysis when they examine export applications[24]. And, depending on the

23 Common Position 2008/244 adopted on 13 December 2008. Cf. "IRANIAN TECHNOLOGY TRANSFERS TO YEMEN First published in March 2017 by, www.conflictarm.com - "Conflict Armament Research. © Conflict Armament Research Ltd., London, 2017.

24 Criteria taken into account for granting military export licences.

Reminder of the 8 criteria of the Code of Conduct:

1) Respect for international commitments; 2) Respect for human rights in the country of final destination. 3) Internal situation in the country of final destination; 4) Preservation of regional peace, security and stability; 5) Security of the

products supplied (complete systems, equipment; major sub-assemblies; components, accessories, support equipment, tools, documentation, etc.), the risk of diversion and thus the related control requirements differ both by their nature and their severity.

We know that fundamentally, but for exceptions, **knowledge transferred by exporters in most high-tech fields is intrinsically dual use**. Furthermore, the identification and assessment of the threshold beyond which disclosure of technical information justifies control cannot reasonably be judged out of context and in a totally rational manner. Even in nuclear or space, all the fundamental laws of physics and most theoretical knowledge are common to purely civil and resolutely military achievements.

Other criteria must therefore be used for control, such as "end user" or "end use". A technology initially acquired for fully legitimate and perfectly commendable reasons and sold as such by an exporter, could nonetheless ultimately be used to serve much less worthy ambitions.

The table below providing a comparison of military and civil goods shows that the need to control products depends both on their purpose and their potential.

POTENTIAL CHARACTERISTICS	TECHNOLOGY or MILITARY ITEM	TECHNOLOGY or DUAL-USE ITEM
Possible uses	Obvious	No certainty
Use for military purposes	Immediate	Deferred (years, etc.)
Foreign policy message	Yes; strong.	Not necessarily
Capacity supplied	Clear and directly proportional to the functions, performances and quantities delivered.	Independent of the area of use justifying the initial acquisition and the quantities supplied
Long-term effects	Decreasing capacity (obsolescence)	IRREVERSIBLE capacity Several small contributions can lead to very significant advances

Member States and their allies; 6) Behaviour of the buyer country with regard to the international community; 7) Existence of a risk that the military technology or equipment will be diverted or re-exported; 8) Compatibility with the technical and economic capacity of the recipient country.

2) Additional criteria:

a) Extent to which the equipment belongs to the civil world (military specificities/functions of the product); b) Technological standard of the equipment; c) Contribution of the product to the operational performances of the system to which it belongs; d) Product criticality in terms of supply chain and DTIB; e) Criticality of the system to which the product belongs (nuclear, biological, chemical, ballistic, related means of delivery, etc.); f) Level of "classification", protection of Defence secrets; g) Share of government funding of the technologies.

Easiness with which the exporter can anticipate the consequences of the export	Quite significant Depends mainly on its intelligence department	More limited as it must be able to analyse technological progress in several sectors in parallel

As the general aim is particularly to anticipate risks of diversion, **in the specific case of technology exports, a double difficulty is faced: firstly, 1) the essentially dual-use nature and, secondly, 2) the intangible nature.** These two factors considerably reduce the effectiveness of "ex ante control" since only the end result of the knowledge transfer will be visible. And this result will only be seen in the more or less long term and most often no backtracking will be possible! This has prompted control authorities to define the following three points of doctrine:

- **The sensitivity of the export is greater for the technology than for the product** to which it relates**;**

- **The technical design**, development and production **documentation** and documents required for maintenance (levels 2 and 3) as well as testing means and dedicated test benches (or specific general-purpose test bench interfacing modules) are **classified at a level at least equal to that of the equipment**.

- **The technical documents used for promotion** (trade fairs, advertising, etc.) and "user documentation", assembly and maintenance manuals (level 1**) are not controlled**[25]**.**

Thus, for export licence issuance, the appropriate chronology emerges quite naturally. First, the evaluation of potential military applications determines the product classification. For the analysis, a systemic approach identifies the degree of military specificity of the complete product's functions (platform), its main items of equipment, their sub-assemblies and key components or even of specific services necessary for optimal use. Detailed knowledge of this tree structure is the only thorough way of establishing the targeted controls necessary to keep both human and financial resources to a minimum.

Particular difficulties with information and knowledge transfers.

By nature, the sensitivity of a technology transfer is complex to assess, since its consequences can generally only be seen some time after the event. Furthermore, there is no general method for strictly and universally measuring and reporting the sensitivity of a given transfer. The table below draws on industrial experience and could serve as a practical guide to help operators and their

25 cf. Directive (EU) 2017/433 of the Commission, of 7 March 2017, amending Directive 2009/43/EC of the European Parliament and of the Council as regards the list of defence-related products. ML22: "*Note 2: Point ML22 does not apply to:*

a. **"Technology"** that is the **minimum** necessary for the installation, operation, maintenance (checking) or repair, of those items which are not controlled or whose export has been authorised;

b. "Technology" that is "in the public domain", "basic scientific research" or the minimum necessary information for patent applications;

c. "Technology" for magnetic induction for continuous propulsion of civil transport devices."

control authorities agree on the categories of information that should be controlled, on a case-by-case basis, based on each company's particular business.

This table is therefore designed as an operational contribution for more appropriate control of technologies (technical data, know-how or services); it can be used to draw up a fairly comprehensive list of potential materials for these knowledge transfers, by person/entity involved.

PRACTICAL TYPOLOGY OF THE DIFFERENT OPERATIONS REQUIRING KNOWLEDGE TRANSFERS
FOR PRODUCT USERS
TECHNICAL DOCUMENTS: Product and environment technical specifications; Results of simulations; tests; product qualification; acceptance procedures; acceptance reports; test reports, etc.
TECHNICAL ASSISTANCE: Platform integration; system takeover; assistance upon product delivery; installation; test bench implementation and calibration; operating support; training in trouble-shooting.
TRAINING: User training for use and routine maintenance (level 1)
SUPPORT DOCUMENTS: User documents; Training materials; Service bulletins or equivalent; Handling of technical events; Computer Based Training; Appraisal report; Calibration report; Technical repair report; Meeting reports where they contain "military" technical information; photos of equipment or sub-assemblies, specific tools; Mission preparation documents, mission reports; Infrastructure guide and plans; Document updates following error correction; Document updates following changes to procedures;
SOFTWARE: Application software for real system or test bench computer, installation/test means; Source code / Object code / Executable code; Application software such as: Mission Preparation/Reference Model; Mission Preparation and Target Modelling; Release note; Mission Data Files; Software Acceptance Certificates; Mission data file editing tools; Test reports; Software Interface Specifications; Change Requests; Test datasets, etc.
OTHER: Replies to technical questions by message.

FOR INDUSTRIALISTS, MANUFACTURERS, INTEGRATORS, REPAIRERS, etc.
Subcontracting; Production transfer; manufacturing licence transfer.

TECHNICAL DOCUMENTS: Technical requirement specification; Product and environment technical specifications; Sub-system performance allocation; Design documents (including mechanical and electrical plans); Design justification file; Manufacturing and control file; Study reports; Appraisal reports; Simulation reports;
OTHER DOCUMENTS; Tests; Production transfer; Technical development assistance; Transfer of design skills; Test plans; Test procedures; General qualification plan; Qualification report; Design documents; Approval documents; Mechanical interfaces; Electrical interfaces; Drawings, Wiring diagrams; Nomenclature; Photos of equipment or sub-assemblies and specific tools; Mechanical or thermal simulation reports; EMC simulation reports; Approval programme; Approval report; Logistics data.
SOFTWARE: Application software for system computer; test bench; firing installation; test means; Source code / Object code / Executable code; Thermal modelling; Aerodynamic models; Mechanical models; Algorithms; Libraries of Mission Preparation and Target Modelling software version documents; Release notes; Mission data files; Acceptance certificates; Mission data file editing tools; Test reports; Software interfacing specifications; Change requests; Test datasets.
OTHER: emails conveying information about technical questions.

This inventory is vital as it determines the most appropriate organisations and procedures for the exported products and their related services.

1.6 EXPORT QUALITY ASSUSRANCE: INTERNAL CONTROL PLAN – I.C.P.

As the aim is to optimally organise the company's internal procedures, the trends that have been emerging in recent years for export control and technology export control in particular should be recalled.

- Providing assurance of compliance with export licences for both sensitive and dual-use products demands very well-managed traceability; the export control organisation, resources and specialised processes must be covered by an internal control plan (ICP) tailored to the size of the company and the complexity of its products.

- To successfully integrate export control procedures into the company, they should be incorporated into the Quality Baseline. This is vital to guarantee their flawless interaction with the information system and particularly with processes relating to programme or contract management and performance. In return, this integration enables full advantage to be taken of the Quality methodology and the related certification audits.

1.7 PARTICULARITIES AND DIFFICULTIES RELATING TO THE END RECIPIENT

To simplify, two main categories of "consumers" can be distinguished. Industry, which manufactures, integrates and consumes basic parts; and operators that use systems for their functions and performances.

Furthermore, when assessing the risk of diversion of products "deemed" sensitive (whether they are purely civil, military or dual-use), control authorities use the commercial channel as a basis, from the exporter to the end user via all the possible variations that involve a diversity of intermediaries.

The number, but also the clarity, of operations and above all the capacity of the people involved, should inform reflection on the changes to be made to control systems.

1.7.1 Temporary (short-term) holders of the product "as built" for transformation or resale

In addition to the operational users of military or dual-use classified systems, who are controlled as "end users", three major groups of professionals may be involved in the trade, transformation, handling or temporary possession of controlled products:

Industrialists that "consume" system components (manufacturers, integrators, subcontractors); traders (wholesalers, retailers and intermediaries/brokers); and service providers (advertising/ promotion agents and sales representatives, forwarders, carriers, etc.).

For the products procured by these three groups, the risks of the product ultimately being used for a purpose other than the one declared or initially planned are slight. On a more technical level, owing to questions of process qualification, optimisation and streamlining, industrialists only rarely change the initially declared use of products, as they procure them for clearly established functions and specific performances.

In the event of a breach, these operators are immediately sanctioned, and directly so by the markets. Their company's image and durability are at stake, as they face risks of being boycotted both by customers but also by suppliers keen to safeguard their reputation as "cautious and responsible operators" among national and international control authorities.

As a result, **systematically demanding non-re-export commitments from well-established manufacturers or integrators** for the sub-assemblies and components they integrate into their production **is a burdensome administrative requirement.** Not only is it costly in terms of management, traceability, reporting and filing procedures, **but it has practically no impact on reducing diversion risks and is therefore of little added value for export control.** For these operators, at the very most, providing **a simple integration declaration should be sufficient** and still help to reduce the risk of possible diversions. However, the effects of technology transfers are potentially permanent, including transfers to members of a same Group for example or from a prime contractor to its subcontractors, and even transfers of manufacturing rights.

1.7.2 Long-term product holders / users

Military products are used for themselves, to enable government forces to fulfil their operational functions. Thus, for military end users, the problem of spares is the trickiest one to control. These

exports mainly concern **physical finished products, with controlled technology transfers being occasional and limited to maintenance manuals at the most**.

If the end use proves to be different to the one initially intended, it is generally justified by diplomatic circumstances and thus by considerations of foreign policy which fluctuate by definition and depend directly on external national or international issues. These considerations and the related responsibilities can obviously not be delegated to private companies, as they have neither the legitimacy nor the resources that governments have to assume the consequences. To increase the reliability and effectiveness of export control within the framework of non-proliferation in particular, it is therefore more difficult to make practical or general recommendations; as each country has its own sovereignty, **only politically (but not legally) binding inter-governmental agreements would appear to be appropriate instruments**.

1.7.3 The special case of government corporations

The problem may nonetheless arise for the control of high-tech industrial goods and military-classified products supplied to government corporations, such as arsenals, research centres and institutes, etc.

In this case, the production is initially intended for the creation or build-up of government forces. Export sales of products derived from national production are therefore an additional source of revenue that above all reduces acquisition and ownership costs for national forces. **Supplying products, and especially sub-systems or know-how, may therefore be authorised to meet the specific needs and development of a given country of final destination in the short term, but with the longer-term, more organisational prospect of supporting economic development, the cornerstone of foreign policy to increase national diplomatic influence**.

Thus, for the country supplying sub-systems and components, confidence and respect for national sovereignty are pushed to the maximum as regards the re-export of its products, subsequently transformed or integrated into local productions (or even of products "as built", re-exported as spares, without any modification or integration).

In this approach, the exporting country must naturally obtain all possible guarantees, in advance and sometimes through inter-governmental agreements. Because once the national programme completed, it can be tricky objecting to a "friendly" country selling on locally manufactured equipment to its own allies. Any such ban would run counter to customary international diplomatic doctrine known as "non-interference". Only the United States, for their most sensitive military products (covered by the US Military List) and by "taking advantage" of the dominant position the dollar gives them, today depart openly from this rule by imposing the extraterritoriality of ITAR[26], despite regular "protests" from all their allies.

1.7.4 Particularities of space products, Ballistic Missiles and commercial launch vehicles

The term launch vehicle encompasses systems with wide-ranging missions. It thus includes rockets capable of placing a telecommunications satellite into geostationary orbit at 36,000 km, or

26 International Traffic in Arms Regulations;

an observation satellite into low Earth orbit at 300 km. Other launch vehicles are configured to send space probes into interplanetary space. In all cases, the earth's atmosphere must be cleared[27].

In any event, a launch vehicle is a complex machine involving a great number of technologies in very varied fields such as metallurgy, chemistry, optronics and electronics. **All launch vehicles are export controlled, as is their equipment, because they demand outstanding performances, particularly in terms of reliability and service life**. The upper stage of a launch vehicle always carries an "equipment bay". This major sub-system contains everything the rocket or ballistic missile needs to function throughout the flight. It controls the perfect chronological sequence of the various flight programme phases, particularly **to guarantee the precision, navigation and attitude control (by means of inertial surveying systems for flight guidance and steering and star sighters for their resetting)**. An on-board computer manages the entire system, particularly the payload (civil satellite or warhead), but also the power supply for example. This "equipment bay" is obviously also present on ballistic missiles, cruise missiles and other unmanned aerial vehicles (UAVs).

Export control applies to these four categories of system (*ballistic missiles, launchers, cruise missiles and other UAVs),* as well as their components, accessories, support equipment, specifically designed tools and the technical data and relevant know-how that could be used to reproduce them or impair their efficiency. The lists[28] group these products together by category (propulsion, components and equipment; propellants, etc.), the main ones being listed in the simplified table below[29].

27 To do so, the payload must be accelerated to approximately 8 km/s and a height of approximately 200 km reached to clear the dense layers of the atmosphere.

28 Cf. MTCR/TEM/ 2016 /Annex 20th October 2016 - http://mtcr.info/mtcr-annex (in English only). In particular: production facilities for energy chemical compounds; production of structural composites, pyrolitic deposition and densification and structural materials; navigation, direction finding and flight control instruments; avionics; launch facilities; computers, analogue-to-digital converters; test facilities and modelling and simulation, design and integration equipment; stealth; nuclear effects protection.

29 Cf. MTCR/TEM/ 2016 /Annex 20th October 2016 - http://mtcr.info/mtcr-annex (in English only).

For Ballistic Missiles	complete missiles	
	their payload (atmosphere re-entry vehicle)	
	their equipment:	navigation, flight guidance and control countermeasures
	their explosive or non-explosive munitions	their deployment structures and mechanisms their security systems their firing systems
For launchers	complete launch vehicles	
	payloads including satellites	
	dispensers,	
	manoeuvre thrusters	
	separation systems.	
For sounding rockets	complete rockets	
	mission-specific equipment, particularly	databases; recording instruments; emitters
	removable recovery equipment	
For cruise missiles	complete devices	
	their explosive or non-explosive warhead	
	their removable delivery and release systems,	
	their security systems	
	firing systems,	
	their removable signature reduction systems	
	their removable countermeasure systems,	
For other UAVs	the UAVs themselves	
	their payload such as cruise missiles	their munitions and related devices, their countermeasures; their mission equipment such as recording instruments, databases, etc. and recovery systems

2. B. ANALYSIS OF WEAKNESSES; DISCUSSION AND PROPOSAL FOR REASONABLE, PRAGMATIC ACTION

The first part of this paper focused on the key factors to guarantee export control of sensitive products and specified what the international political "Arrangement", known as the Missile Technology Control Regime (MTCR), today particularly covers.

As stated above, the MTCR aims especially to restrict the proliferation of means of delivery of Weapons of Mass Destruction and their technology. To achieve this, its 37 members ensure a permanent watch over transfers of missile equipment and the related materials and technologies that could be used in systems capable of carrying WMD.

Seeking to better identify the aspects of control that need improving, the study continues to examine **how far and in which conditions it would be possible to enhance this 30-year-old system** that has been carefully honed with the passing of time, technological developments and crises.

2.1 PRIVATE INDUSTRY TAKES OVER FROM GOVERNMENT ARSENALS

One great difficulty in implementing and improving export control lies in the low resources that are devoted to it. To cope with the reduction in Defence budgets, which was particularly significant at the end of the 1960s, European governments began to develop a new strategy, **transferring the industrial workload of arsenals to private industry. At the same time, a policy was developed to encourage cooperation and export, particularly to reduce by economies of scale the fixed costs of designing and producing new national arms systems** that were too high for a single country. This transfer gradually moved up the production chain. Today, innovation in the civil sector is the main source of inspiration of military developments. Furthermore, the cost of military innovations is substantially reduced, provided it is limited to the development of additional functions or to improving the performances or features of existing products (resistance to temperature, pressure, vibrations, electromagnetic radiation, etc.).

In parallel, with the development of "Certifications" and "Quality" (in the Japanese sense) in companies, we saw a shift from permanent governmental control of products, performed "in situ" directly on production lines, to a process of certifying industrial design and production methods.

As a result, State expertise was transferred out of the industrial sites to gradually only remain in the design offices. And the human resources, diminishing due to natural ageing, i.e. the government workers and skilled tradesmen, were progressively replaced by Quality experts having only overall knowledge of standards rather than "know-how". Then, when the first industrial arms establishments were privatised in the early 1990s, in turn these Quality technicians left the arsenals' production lines, and were henceforth involved solely in approving the organisation and methods defined by the private sector for its factories and workshops.

In France, the DGA gradually abandoned its status as "prime contractor" to initially retain that of "designer principal" and then eventually that of a "mere" specifier.

Furthermore, the more complex and sophisticated weapons systems became, the more this evolution gained speed and intensity. For example, French fighter aircraft have always been produced by Dassault; and France's nuclear deterrent force – initially handled by Aerospatiale, a company wholly controlled by the State – ended up being entrusted to Airbus of which 74% of the capital is today floated on the stock market.

Thus, private enterprises gradually became the only ones to have in-depth knowledge of the products and their manufacturing complexity and, hence, the expertise required to judge their real specificity compared to international supply – the factor that ultimately determines their degree of sensitivity for export.

2.2 HOWEVER, EXPORT CONTROL CAN BUT REMAIN A PURELY GOVERNMENTAL ACTIVITY

In practical terms, the performance of export control hinges on the overall quality of numerous factors, the standard of which must be as consistent as possible to guarantee optimal quality of the system as a whole.

This long list of sovereign functions includes the development of principles and rules for: production classification, the application of penalties, canvassing of new customers, contract negotiation or order acceptance. Or going further, the choice of decision criteria for: granting or refusing export licences, filing licence applications, implementing these licences, the conditions of delivery relating to equipment performances, the verification of information provided, etc. And finally, the conditions to be met for: technical assistance, trouble-shooting, supplying spares and repairing delivered products, etc.

All these aspects can have a direct and critical impact on the quality of service expected and even increasingly demanded by the customer; they are therefore also all competitive advantages on the international market. Unfortunately, the openings and efforts made by the authorities to improve flexibility on all these points evolve very slowly. In addition, very often, the rare changes are only minor and remain subject to interpretation, making it difficult for operators to truly deploy and integrate self-verifications into their internal control systems. These operators continue to feel "insecure" and are not reassured by any message of tolerance that would nonetheless bring the flexibility needed to trigger a virtuous circle. **From this perspective, effective recognition of companies (at least "certified" companies) as true partners in the fight against proliferation would no doubt be an improvement**.

2.3 IMPROVING CONTROLS REQUIRES A METHODOLOGICAL APPROACH

Any attempt to improve the performance of export control requires a methodology based **on the three fundamental and universal pillars in this area: Product Performance, End User and End Use**.

The first of these pillars requires a functional understanding of the product and its detailed characteristics, to ensure it is correctly classified.

This point, which demands in-depth technical knowledge, is always very difficult to master, in particular for new technologies. Indeed, anticipating future applications or imagining new needs swiftly takes us into the realm of R&D.

This explains, at least partly, the overcautious attitude often taken by the classification authorities which, "out of precaution" or fear of being criticised by their peers, choose to ignore or underestimate the reality of international supply. Firstly, this inevitably distorts competition on the export market to the detriment of operators. And secondly, **an excessive "principle of precaution" culture results in the authorities mobilising resources (to cover all transactions and all products) on insignificant operations, despite their scarcity. And those same resources are then lacking for truly sensitive cases.** In the end, the results in terms of combating proliferation are very minor, since the "over-controlled" products are ultimately often available on parallel markets.

The second and third pillars concern the assessment of the end user's capacity (country and the entity in it) and whether the end use of the supplied products is legitimate; this latter aspect of control is no doubt the most difficult to guarantee

Because while geopolitical analysis and expertise in international relations can be relied on to gauge the "end user", only assumptions based most often on essentially political declarations of appropriateness are available to assess the "legitimacy of the end use". In any case, these "guarantees" are always influenced, for supplies to States, by subjective considerations of territorial security or national sovereignty. In addition, such reasons naturally and in essence vary in time and space; they are very difficult to verify and even more complicated to contest, if necessary.

This intrinsic difficulty creates uncertainty, for the exporting country, about the long-term compliance with the commitments initially made at the time the order is placed. Yet, the ability to avoid any diversion at any stage in performance of the contract, and the image and international credibility of the exporting Government are at stake.

Risks also exist for companies, right from the start of manufacturing through to the transfer of product ownership. Diversions are always possible, including during subcontracting and delivery, particularly as third-party intermediaries must be involved for industrial or logistics requirements.

2.4 THE TWO INTERPRETATIONS OF END-USE AND END-USER

The rules in this area are neither very clear nor consistent over time or in space. Not only does this complicate the operators' position and render control processes more complex, but it also generates additional human and financial costs for industry.

2.4.1 First approach: extraterritoriality of national controls

As mentioned above, in the years 2000, this was still exclusive to America[30]. **Today, this approach would appear to be developing and, even within the European community** (where

30 This "dictatorship", which is contrary to international law, relies "de facto" but therefore not "de jure" firstly, on the commercial hegemony created by the dollar which is still almost exclusively used as the exchange currency for exports, and secondly, on exorbitant financial penalties in the event of a breach, reinforced by the publication of

export control rules are nonetheless harmonised), multilateral transactions can become problematic.

For example, at present, for its national equipment manufacturers, the German control authority[31] makes export licences contingent upon their European integrator partners producing "end user" declarations and possibly "non-re-export" undertakings, signed by the end-user foreign government for which the finished products leaving the EU are destined. **This one-sided attitude is a manifest infringement on the national sovereignty of States, and they ultimately shoulder responsibility for the exportation outside the Community nonetheless**.

Yet, today, none of the EU Member State governments seem to really take offence. On the contrary (to the exporting industrialists' dismay), no doubt out of reciprocity and maybe also to avoid confronting the USA head on, this practice is becoming more widespread in Europe: this is already the case in Italy and the UK. But, if it became general practice, the consequences of this kind of technocratic measure are easy to imagine, as is the complexity of the export control file if the integrator had to obtain "end-use/end-user certificates" from its end customer for each foreign component its product contains.

2.4.2 The traditional approach of France and most exporting nations today

France traditionally leaves it to the government of the foreign integrator to judge, alone (in return for the same treatment), the appropriateness of exporting products containing French components to its export customers.

Contrary to the American logic, France thus considers that the components lose their original nationality when they are integrated into the product giving rise to the contract with the end user. At that time, they take the nationality of the integrator's country, such that **the exported system is controlled rather than each of its basic components and the exporting country alone is responsible for the transaction to the international community**.

This French approach is obviously more pragmatic, both from an industrial and a commercial standpoint; it takes place as if the government of the integrating industrialist ensured, **simultaneously in a single operation, 1) for itself, the full compliance of the export of the complete product delivered and, 2) on behalf of its component-producing partner countries, the export control of the integrated parts they supplied.**

Finally, it can be noted that the "risk" of the integrated components being "diverted" to uses other than those declared is often mentioned to justify applications for end-user/end-use certificates concerning basic parts.

However, this historical practice is no longer adapted to the technical reality of the high-tech equipment and components market.

---

blacklists banning, in practice, recourse to US suppliers and restricting foreign contracts to those not afraid of seeing their relations with the USA impaired.

31 The Federal Office of Economics and Export Control: Bundesamt für Wirtschaft und Ausfuhrkontrolle – BAFA -.

This is because for high-tech basic parts much sought-after by "proliferators", the risk of diversion has become almost inexistent. Both integration and miniaturisation are today pushed to extremes and the functional specialisation of basic parts has made them almost impossible to use outside their original environment.

Accordingly, in addition to the prohibitive cost of recovery operations, for reverse engineering for instance, it is now almost impossible to dismantle products to retrieve their components without causing unavoidable and irremediable damage.

2.5 OTHER SOLUTIONS ARE POSSIBLE TO INCREASE "END USE" AND "END USER" CONTROL

Regarding the end user (the country and the entity from it), it would seem that, in practice, this point can only be controlled by a clear attitude and unambiguous communication on the exporting country's foreign policy.

Understandably, for numerous political and diplomatic reasons, it would be unreasonable to expect total transparency. However, publishing lists of countries and persons, as the USA has traditionally done but also as is now more frequently the case in Europe (for sanctions and embargoes), would no doubt bring an improvement.

Information exchanges about "high-risk parties" are currently limited to government agencies, which prevents exporters from anticipating and avoiding contacts and situations that could eventually prove difficult to manage.

Even if these lists were not a condition preventing exportation, they would certainly be a diplomatic means of sending out a strong signal of solidarity to partner States. And from the exporters' point of view, on a commercial level this official sign would allow them to objectively explain refusals to sell. Lastly, it shall be noted that when faced with listed parties (countries and persons), exporting States would be in a relatively comfortable position personally, as none of them could be specifically designated as the source of the sanction since the list results from a consensus within international circles of control.

In practice, three categories of lists can be considered.

- Negative lists of countries; adopted within the framework of embargoes with varying degrees of severity (natural and legal persons, product categories, economic and financial sectors, etc. through to total embargo) when converging information and evidence of reprehensible attitudes or illegitimate uses are held and confirmed by the partners' intelligence agencies.

- Grey lists of countries or users; (like the US “unverified entity list”) indicating a certain level of suspicion on the part of most intelligence agencies concerning potential or actual illegitimate doings.

- Positive lists of countries; they may contain preferred destinations, be linked to specific licences and naturally vary with the products exported. This kind of list is already used (particularly by Britain and Germany) for their general national military

licences and for European general licences (EU GEA[32]) applying to Dual-Use products.

Even though they often deplore the restricted scope of general licences, this system is nonetheless greatly welcomed and extensively used by industrialists, due to its transparency and ease of implementation.

2.6 RISKS RELATING TO LEGITIMACY AND END USE ARE PARTICULARLY LINKED TO HUMAN RIGHTS AND TERRORISM

Concerning the third fundamental pillar of control (legitimacy of end use), human rights violation and terrorism are effectively the two main areas of risk. In fact, the questions of ethics and of the recipient country's social development[33] can be linked to the question of human rights. Similarly, the proliferation of weapons of mass destruction can be regarded as an aggravating factor of the terrorist threat.

Given its subjective nature, directly related to philosophic and social considerations, end use legitimacy is a very difficult aspect of export control to address and no doubt the most complex to guarantee. It is true that only assumptions and more or less official declarations can be used, and their veracity and permanence are not always indisputable. To assess this aspect properly, the only pragmatic way would appear to be an analytical approach based on evidence found and convictions established by cross-checking and confirming multiples sources of information.

As intelligence is a highly confidential and essentially governmental activity, it can only be done by specialised government agencies, even if industrialists are a valuable source of information for them.

This empirical method also implies accepting a certain risk of error, the extent of which can only legitimately be defined by governments having regard for the potential impact on their image, their international reputation and their politico-diplomatic positioning.

For example, in the early phase of a country's legitimate military development, when it is initially equipping its troops or building up its arsenals, the exporting weapons industry can naturally play its preventive role to the full by helping to guarantee that the products supplied correspond to the customer country's Defence requirements and its effective resources. This action concretely supports government measures taken to comply with criteria two[34] and eight[35] of the European

32 EU General Export Authorisation; cf. Marion Ringot, in "*Export Control Law And Regulations Handbook*, *third edition* (p.232 to 236); (– published by Yann Aubin and Arnaud Idiart on 06/28/2016 at Kluwer Law International). https://lrus.wolterskluwer.com/store/products/export-control-law-regulations-handbook-third-prod-9041154434/hardcover-item-1-9041154434.

33 Criterion no. 8 of the EU Code of Conduct on arms exports (cf. Common Position EC 944/2008).

34 "Criterion Two of the EU Code of Conduct on arms exports: Respect for human rights in the country of final destination as well as respect by that country of international humanitarian law."; cf.:(http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:335:0099:0103:en:PDF; Council Common Position 2008/944/CFSP of 8/12/2008, defining common rules governing control of exports of military technology and equipment:

35 "Criterion Eight: Compatibility of the exports of the military technology or equipment with the technical and economic capacity of the recipient country, taking into account the desirability that states should meet their legitimate

Union Code of Conduct. However, practicing international relations is not an exact science and to enable any fruitful public-private rapprochement in this diplomatic sphere, errors would have to be prevented and any defaults mutually accepted. To combat ill-managed transfers of sensitive information and technology in particular, the model of cooperation between intelligence agencies (implemented and developed by International Circles, notably those of the Wassenaar Arrangement[36] or the MTCR[37]) would no doubt gain from being extended to companies to derive greater benefit from their local presence and experience.

Thus, given the highly subjective nature and confidentiality of intelligence, plus its isolated way of functioning, exporter contact with government agencies and diplomatic missions is no doubt insufficient today.

Yet, in the practice of "certifying" companies[38], as regards examining and implementing export licence applications, the transfer of responsibility from Governments to exporting businesses is a growing trend. On-site, ex-ante control, both on production lines and in logistics, customs and export departments, is gradually giving way to upstream audits, ex-post document controls and inspections.

Governments cannot offload their responsibilities onto companies, particularly for monitoring and controlling the undertakings made by foreign operators signing the certificates and other non-re-export, end use or end user commitments. These steps can only be taken by representatives of the exporting government present on location and, where applicable, of its allies, which conduct local intelligence activities, whether openly or otherwise. However, governments would undoubtedly gain from sharing their resources and giving exporters more direct access to their national intelligence agencies (and via them, possibly those of their partner countries).

This lead could therefore bring significant progress in improving controls.

security and defence needs with the least diversion of human and economic resources for armaments". (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:335:0099:0103:en:PDF; Council Common Position 2008/944/CFSP of 8/12/2008, defining common rules governing control of exports of military technology and equipment.

36 Cf. "Best practices for effective export control enforcement" (agreed at the 2000 Plenary and amended at the 2016 Plenary) - http://www.wassenaar.org/wp-content/uploads/2016/12/Best-Practices-for-Effective-Export-Control-Enforcement-1.pdf

37 Annual meeting of the "information exchange" group in parallel to the plenary meeting.

38 The status of Authorised Economic Operator (Regulation no. 1875/2006 of 18 December 2006) provides that starting 1 January 2008, the provisions relative to AEO will come into force, i.e. that all Member States must be in a position to process applications made by authorised operators. Since July 2009, international trade operators have been required to submit in advance a summary entry and exit declaration containing data considered necessary to do a "security" risk analysis. This status of AEO, which is valid throughout the European Union, distinguishes the most reliable community operators, as part of a Quality recognition process. In parallel, the status of "Certified Company" recommended by European Directive EC 43/2009, entitles suppliers from all Member States to deliver numerous Defence-related products to integrator industrialists in the EU, without the need to first apply for an intra-community transfer licence, the reliability of these integrators and the Quality of their export control system being certified to the Community by their respective governments.

2.7 SPECIFIC RECOMMENDATIONS CONCERNING TECHNICAL DATA AND ITS MANAGEMENT

As the United Nations Security Council has unanimously reaffirmed in several resolutions, the proliferation of weapons of mass destruction – nuclear, biological and chemical – and their means of delivery[39] constitutes "*a threat to international peace and security*". Proliferation has a particularly significant destabilising effect on international security as the phenomenon is developing in areas of tension. Furthermore, proliferation-related crises and the increasing range of ballistic missiles held by sensitive countries are threatening the security of France and Europe. Then there is the risk of nuclear or radiological machines, and biological or chemical agents being used for terrorism.

Combating proliferation requires reinforcement of the international non-proliferation regime, and close operational cooperation to prevent unlawful sensitive transfers and to counter illegal networks. To do so, governments have launched measures, on a national, European and international scale[40].

---

39 Missiles, rockets or other unmanned systems capable of carrying nuclear, chemical or biological weapons to their target and specially designed for that use (cf. resolution 1540 of the United Nations Security Council of 2004).

40 Example in France: Instruction no. "14 /SGDN/AIST of 24 March 2009 on action to combat the proliferation of weapons of mass destruction and their delivery systems. It requires good inter-ministerial coordination and strong mobilisation of all the relevant ministries. ***"Four focuses of EU action against proliferation"****, are identified:*

improve our knowledge of proliferation; efforts in research and use of intelligence and a pool of experts to provide decision-makers with a fair and independent assessment of risks and threats; developed and extended, in particular, to financial supervisory authorities

reinforce the efficiency of Government action to combat proliferation; raise awareness among scientific, academic and economic stakeholders.

improve prevention and protection; the relevant ministries will contribute to the effort to raise awareness of the importance of proliferation in economic (industrial and commercial companies, professional federations, financial institutions and banks), scientific and academic spheres (researchers, teaching staff, students) …

prevent financing of proliferation. Prevention and repression of proliferation financing, resulting particularly from our international obligations, require determined action by the ministries. The Ministry of the Economy should more particularly contribute, with the Ministry of Foreign and European Affairs, to reinforcing international and European cooperation and instruments in order to define rules and practices to more effectively combat proliferation financing;

• in conjunction with the other relevant ministries, make particular efforts along these lines within the Financial Action Task Force (FATF);

• improve cooperation between administrative authorities, financial supervisory authorities and the financial intelligence unit, particularly by developing, in conjunction with the other relevant ministries, a typology of financial channels

Strengthen the European and international system. Within its remit, each ministry will encourage its European counterparts to step up their anti-proliferation efforts and measures to harmonise laws and procedures specific to this area. To complete and update a European analysis of the risks and threats of proliferation, the relevant ministries will reinforce their cooperation with the European Union situation centre (SITCEN), in accordance with the exchange channels in place and practices in force. The Ministry of Foreign and European Affairs, in conjunction with the relevant ministries, shall promote a European anti-proliferation network and encourage the implementation of training for Member States' and EU officers. Together with the competent ministries, it shall pursue its action to reinforce international instruments and achieve the adoption of international rules improving the control of dual-use goods and

The British experience shows that **most non-controlled technology transfers occur during international travel and missions of defence company staff.** However, nothing new or very operational is currently planned at a regulatory level. Can we be surprised or even complain when we know that, firstly, the control authorities admit that they do not have the resources to control intangible transfers and, secondly, **the Government particularly hopes to rely on companies since it is in their best interests to fully protect their technologies and the competitive advantage they represent**?

2.7.1 Even for Governments, still today, full control of intangible transfers is impossible

Attempting to discover all unlawful technology transfers would, in any case, be unrealistic. But it is above all very difficult, not to say impossible, to prove a suspected or even detected breach, and thus prosecute and punish the offender.

To improve measures to combat the spread of weapons of mass destruction more particularly, **one first and rapid measure (requiring only a small investment) would consist in reinforcing or extending measures and instruments already used**. Very often, the accumulation of new rules, new instruments or allegedly new facilities, results in poor enforcement of existing systems, and even simply a lack of understanding or consistent interpretation. New requirements, stemming from inevitable changes in the environment or technologies, could very often be incorporated into the body of regulations by simple explanatory notes. Data transferred by intangible channels is available in physical form when it is developed and upon its arrival for use by the recipient. **Therefore, outside the transport phase, all export control practices and procedures that exist for physical goods can apply to information.**

Furthermore, this control proves to be quite different depending on the country. This disparity no doubt stems from real difficulties with implementation, both for the authorities and the exporting manufacturers[41].

Although in export control the sending of information is often considered to be the act of transfer or export that is subject to licence (not the receipt), in some countries, it is the actual receiving of information abroad (on an electronic medium without a licence) that constitutes a violation of export control rules.

2.7.2 Companies do not currently have the tools they need to control intangibles

In practice, conservatory measures are therefore adopted. For instance, cell phone functions for receiving email attachments abroad can be disabled and employees sent on missions carry computers with limited network and intranet access. To truly have a chance of controlling exports of intangibles, the company's laptops would have to be equipped with "spyware" to block

intangible transfers of technologies, and the introduction of effective measures in brokerage, transit and transhipment. It shall also promote the reinforcement of legal means of curbing acts of proliferation on an international scale.

41 "*Pratiques communautaires internes de contrôle des exportations et des transferts intracommunautaires de produits de défense"* by Fabio Liberti, Sylvie Matelly and Jean-Pierre Maulny - Etude finale - October 2010.

http://www.defense.gouv.fr/content/download/104465/1019134/file/EPS2009_pratiques_communautaires.pdf.

unauthorised information and data flows based, for example, on key words and sender/receiver communication controls.

However, use of such software is contrary, at least in Europe (but not currently in China for example), to laws on the protection of privacy and civil liberties. So far in France, the CNIL[42] has responded negatively when questioned in this respect.

Consequently, the introduction of **an ex-post control, requiring the company to be more active and the public authorities to regularly audit exporters, could be seen as the most appropriate measure for controlling intangible transfers**. In this context, prevention and training are more effective measures than systematic, exhaustive controls. Logically, a realistic approach requires implementing more preventive than repressive measures.

With a view to collaborative action, information meetings and discussions should be organised between public authorities and companies (including via sectional professional groupings). And official joint Industry/Administration groups could be formed to monitor, identify and prevent potential risks. Such **joint working groups could particularly draft concrete operational guidelines such as the practical measures operators should take for their technology transfers by intangible channels.**

2.7.3 Information and data identification and marking

Another tricky point on which cooperation between industry and government agencies would no doubt be beneficial is the identification and marking of information and data to be controlled.

For the control of technologies and their transfer, especially by intangible channels, marking is a decisive factor. In this area once again, pragmatism calls for accepting a system that restricts risks of diversion as far as possible, but without being able to rule them out completely.

Regarding knowledge transfers, it would be unrealistic to aim for total control of information, apart from banning all unauthorised exchanges. Communications within the scientific community, the necessary exchanges within and between companies and their customers, and governmental and industrial cooperation inevitably result in access to sensitive data being unintentionally granted to unauthorised people, either accidentally or more or less lawfully.

Faced with this situation, **we must accept that full control can only be applied to information that truly warrants it.** Marking and therefore management and control can be done at three different levels of detail: marking of documents (the information media), marking of information (description of ideas and concepts or the key elements of a concept), and marking of the elementary data (values and figures) that make up the information contained in documents. **This is obviously a fundamental point since it directly determines the volume of data to be processed, the size and organisation of the system and the resources needed to implement**

42 The Commission nationale de l'informatique et des libertés (CNIL) in France, the French data protection authority, is an independent administrative authority. The CNIL is responsible for ensuring that computer technology serves citizens and does not infringe upon human identity, Human Rights, or privacy, or individual or civil liberties. It fulfils its missions in accordance with law no. 78-17 of 6 January 1978 amended on 6 August 2004. Cf.: https://www.cnil.fr/

it, and finally the initial investment as well as, in the longer time, the operating and maintenance costs.

This initial strategic choice also requires extremely clear rules governing the marking of documents, information and data, for those who produce or modify information and its media (whether physical or otherwise). However, it is very difficult to generalise on this point[43]. In most cases, the sensitivity of a concept, document, information or datum depends on factors external to the company, such as competition, national industrial priorities or even a country's security or sovereignty. **Furthermore, to be fully understood and therefore correctly applied, these measures should naturally be supported by an initial and continuous training programme**; overlooking this point would run the risk (inevitably and more or less long term) of inflationary drifts that would be disastrous for the entire information system.

2.7.4 Two main categories of information

In practice, companies are required to manage two main categories of information.

- Classified information, which is all covered by more or less stringent, specific protections; depending on its sensitivity, including on the national territory, it is controlled more when it is exported and is therefore subject to regulations specific to the type of information (military, nuclear, cryptology, etc.). Classified information[44] must be processed in

43 In practice, inspiration could be drawn from a guide drafted by the US Department of Defense no. 5200.45, April 2, 2013, designed to provide assistance with writing classification guidance (Manual for the development of security classification guidance cf.: http://www.dtic.mil/whs/directives/corres/pdf/520045m.pdf

44 Classified information: French definition taken from the General Instruction No. 1300/SGDSN/PSE/PSD of 30 November 2011.

"Articles R. 2311-2 and R. 2311-3 of the Defence Code define three levels of classification:

- Très Secret Défense (Top Secret Defence), reserved for information and materials concerning government priorities in matters of national defence and security the disclosure of which could be very seriously detrimental to national defence;

- Secret Défense (Secret Defence), reserved for information and materials the disclosure of which could be seriously detrimental to national defence;

- Confidentiel Défense (Confidential Defence), reserved for information and materials the disclosure of which could be detrimental to national defence or could result in the discovery of a secret classified at one of the above two levels"

NB: "The Restricted marking may be affixed on information and materials where the issuer wishes to restrict its circulation. Contrary to certain foreign regulations, it does not correspond to a level of classification but aims to draw the user's attention to the need to exercise discretion in handling this information. It indicates that the information must not be made public and must only be communicated on a need-to-know-basis to the relevant persons.

Protected information (or materials) issued by foreign governments or within the framework of international organisations, when a security agreement exists, is only covered by protection measures if it bears a national classification marking corresponding to one of the three levels defined by Articles R. 2311-2 and R. 2311-3 of the Defence Code (supra), or an equivalent marking defined for example by the EU (circular of 5 May 2002), NATO, OCCAr, the WEU or Euratom (pursuant to the decree of 25 February 1994 published in the JO of 1 March 1994)".

For memory: US definition of classified information: Any information (or material), regardless of its physical form or characteristics, that is owned by the US government as defined by the *Executive Order No. 12958 -- Classified National*

compliance, firstly, with inter-governmental security agreements[45] and, within this framework, with the respective national rules of the parties to the agreement. In addition, to be "authorised" to hold classified information, companies must introduce internal rules and procedures to guarantee its protection. These internal rules must therefore also be complied with, along with any measures expressly specified in contracts to guarantee industrial and commercial security. **Security regulations do not replace but come on top of national laws and regulations on export compliance.**

- Unclassified information, which may or may not be export controlled. All companies that handle very high-tech products must protect and correctly manage a great deal of unclassified but controlled information. Regarding such sensitive information, the principles and methods applied to guarantee proper management of classified information apply, but on a less demanding level since the information does not involve a risk for national security.

NB: in order to track truly sensitive "export-controlled unclassified" information, companies that also manage classified information would ultimately only need to adapt the organisation, procedures and means already in place to protect Defence secrets.

"Controlled unclassified" information is treated in accordance with international security agreements, national laws and regulations[46], any security directives specific to the company, foreign laws and regulations applicable for export compliance and any specific contract clauses.

Any information corresponding to the following definition of technical data is controlled, either as "classified information", or as "controlled unclassified information": *"Information required for the design, development, manufacturing, assembly, operation, repair, testing, maintenance,*

Security Information; April 17, 1995 -- or other provisions imposing rules of protection against any unauthorised disclosure.

45 Mainly bilateral and established to guarantee identical reciprocal protection, by both countries, of information that could very seriously or seriously be detrimental to their respective national security.

46 For example in France, the system for protecting the nation's scientific and technical potential based on the Penal Code is organised principally around a decree of the Prime Minister en Conseil d'Etat: Decree no. 2011-1425 of 2 November 2011 implementing Article 413-7 of the Penal Code and relative to the protection of the nation's scientific and technical potential (http://www.sgdsn.gouv.fr/missions/protection-du-potentiel-scientifique-et-technique-de-la-nation/le-dispositif-de-protection-du-potentiel-scientifique-et-technique-de-la-nation-faq/#_ftnref1); on an order by the Prime Minister: Order of 3 July 2012 on the protection of the nation's scientific and technical potential (http://www.sgdsn.gouv.fr/missions/protection-du-potentiel-scientifique-et-technique-de-la-nation/le-dispositif-de-protection-du-potentiel-scientifique-et-technique-de-la-nation-faq/#_ftnref2); and on an inter-ministerial circular by the Prime Minister: Inter-ministerial Circular of 7 November 2012 on implementation of the system for protecting the nation's scientific and technical potential (http://www.sgdsn.gouv.fr/missions/protection-du-potentiel-scientifique-et-technique-de-la-nation/le-dispositif-de-protection-du-potentiel-scientifique-et-technique-de-la-nation-faq/#_ftnref3).

It aims to protect access to the most "sensitive" knowledge, know-how and technologies of public and private organisations, the diversion or capture of which could: be detrimental to the nation's economic interests; strengthen foreign military arsenals or weaken the nation's defence capacities; contribute to the proliferation of weapons of mass destruction and their delivery systems; be used for terrorist purposes on the national territory or abroad. Each Ministry adapts the methods of implementing the system for protecting the nation's scientific and technical potential according to the specificities of its scope of jurisdiction (various ministerial directives have been drafted to this effect).

or modification of a defence-related product[47]*; "Technical data" may particularly take the form of diagrams, drawings, graphs, models, formulas, charts, technical concepts and characteristics, written manuals and instructions or those recorded on other media or devices such as disks, magnetic tapes, non-rewritable memories, etc.".*

Other information (for example information concerning the management, sales and marketing of programmes, etc.) is identified and protected by private non-disclosure agreements;

Any question relative to the classification of unclassified information must be put to the company's export manager.

Where there is no specific Programme Security Instruction or equivalent ad hoc document, "controlled unclassified information" may only be transferred or made available to expressly authorised persons. However, the following persons are deemed authorised:

- Any national natural person (e.g. French) employed by a French person[48];
- Any national natural person employed by a national of a third country, provided that natural person has signed a "Recognition of Obligations concerning Controlled Unclassified Information" of which it will have knowledge[49]
- Any foreign natural person to whom the transfer of controlled unclassified information has been authorised by law, regulation, licence or any other valid authorisation of the government or legitimate foreign governmental authority. Where the person is employed by a subsidiary of the company, the latter signs a "Recognition of Obligations concerning Controlled Unclassified Information" of which its employee will have knowledge.
- When controlled unclassified information is not used, it must be locked in a desk, a cabinet, or a room or protected by any equivalent means prohibiting all unauthorised access.
- The information must be destroyed such that it cannot easily be reconstituted (paper copies must be shredded or torn up several times before being thrown away in a bin; computer disks must be erased and reformatted before being transferred to another office, or demagnetised or damaged before being discarded).
- Controlled unclassified information may be sent by normal post or by courier without a "courier certificate"[50].

47 "Defence Article" means any weapon, weapon system, ammunition, aircraft, vessel, vehicle, boat, or any other war material and any part or component thereof or related documentation.

"Document" means any recorded information, regardless of its physical form or characteristics, for example, written or printed (letter, diagram, plan), computer storage media (hard drive, floppy disk, electronic chip, magnetic tape, CD), photo and video recording, optical or electronic reproduction of these defence articles.

48 The term "person" includes natural and legal persons.

49 NB: foreign persons may only have access to controlled information if it is covered by an export licence. In France, a foreign person hired by a French national company may access controlled information even classified. The foreign employee must act for and under the complete responsibility of the employing French legal entity.

50 Cf. Appendix D, Document MISWG no. 1 (http://avanco.com/_assets/pdfs/AppK_010106.pdf)

- Controlled unclassified information must not: be shown in public places, such as airports or train stations or even sent by non-secure email on public networks, unless it is encrypted. Computers, including laptops, that are used to process the information must prohibit unauthorised access, but need not be certified, unless they also process classified information.

2.7.5 "Information enabling the equipment to be produced or reproduced or its efficiency compromised" is controlled

Concerning information relative to technology, the rule it that it must be controlled: "when it enables the equipment to which it relates to be produced or reproduced or its efficiency to be compromised". For the most consistent and reasonable implementation possible, the spirit of this rule should be specified here. The important notion of this article does not lie in the terms "produced", "reproduced" or "efficiency compromised", but in the term "enables".

Controls are therefore required when the information sent, truly, directly and on its own, enables the weapon or component to be produced, reproduced or its efficiency to be endangered.

This means that an authorisation is required for the following information or documents, even in the case of negotiations or delivery of an offer for equipment, software or services. Documents[51] concerning key functions and containing technological information that can be directly used by the customer's departments or a manufacturer to produce or reproduce the Defence-related product.

2.7.6 Structured "Government-Industry" reflection would be useful

It has to be said that in terms of managing information and data, **operators are apparently still not very aware of certain basic principles and definitions** (mainly SMEs). These companies therefore encounter difficulties identifying, classifying and correctly managing their technical data. And this exposes them to substantial risks, since the penalties are laid down by the Penal Code[52]; any violations can indeed cause the entire country serious prejudice. **As an example, some practical measures taken by industry are indicated below.** They could no doubt serve as a basis for structured "Government-Industry" reflection coordinated by the HCOC.

At least one simple generic rule could be applied: **"*All classified information:***

1) is, by nature, subject to declaration in the export licence and

2) is controlled by regulations and procedures specific to classified information".

In this case, it is necessary to remember that classified information may only be transferred electronically

1) if it is handled by personnel that has:

a) clearance,

51 In particular, detailed industrial specifications, manufacturing packages, plans, user or maintenance manuals where they contain detailed functional descriptions of the equipment, functional models or models built with real materials.

52 In France, the export of Controlled Unclassified Information without a licence is liable to a fine of up to €75,000 and a 3-year prison sentence.

b) authorisation, and

c) a need to know,

2) and only if it is:

a) encrypted by means of government encryption measures, and

b) sent via dedicated networks having reinforced protection measures against any attack or intrusion that could affect the availability, integrity or the confidentiality of the data transferred[53].

3 PROSPECT FOR IMPROVING THE FIGHT AGAINST PROLIFERATION AND INTEGRATING NEW ENTRANTS

With a view to improving control of transfers by intangible channels, as a conclusion to this extensive review of the regulatory framework and practical proposals for securing satisfactory export control, **the challenge facing the most advanced countries in export control is no doubt today the successful integration of new countries entering the market**. China particularly comes to mind, as its technological and industrial development has enabled the country to grow its share of the weapons market at remarkable speed in recent years.

3.1 FOCUS ON CHINA

China, which only accounted for one percent of the market over the 2006-2011 period, became the third-largest global exporter of weapons over the 2012-2016 period, with almost 9% of the market, behind the USA (48%) and Russia (approximately 12%).

However, Beijing has announced that its military expenditure would increase 7% in 2017 which is the smallest rise seen for years. The Chinese arms industry will no doubt therefore need to turn to the international markets, with heightened aggressiveness, to find the outlets it will be lacking on a national level.

Already, the Chinese offering on the weapons market is very complete and includes all the most sophisticated systems and equipment expected for the development of modern armed forces (Army, Navy, Air Force): from traditional heavy tanks to tactical micro-satellites

53 If each of the following five points is guaranteed, then the system can be said to be secured.

1 - Confidentiality (ensure that only the recipient of the message will understand it).

2 - Integrity (ensure that the message sent has not been intentionally or accidentally altered).

3 - Availability (guarantee access to the information by the department or resources used).

4 - Non-repudiation (ensure that neither of the two parties can deny being the issuer or recipient of the message).

5 - Authentication (ensure that each party to the exchange is truly the person they claim to be).

via the J20 (5th generation fighter)[54], surveillance and fire control radars, infrared night vision and sighting devices, armed or surveillance drones and, of course, cruise missiles. For confirmation, one need look no further than the catalogue of the latest China Air Show that took place in Zhuhai in November 2016[55]. It shall further be noted that all the major weapons-exporting nations, including Russia, the USA, South Korea, France and the UK, travelled to the Zhuhai show in 2016.

54 According to the channel CCTV, the J-20 has come into operation in the People's Liberation Army (PLA). If this information is true, the Chinese armed forces would therefore be the second, after the US with the F-22 Raptor and the F-35 Lightning II, to use a fifth-generation stealth aircraft. Russia, whose aeronautical industry has developed some very high-performance aircraft, has not yet achieved this, even if the commissioning of the Sukhoi T-50 has been announced for this year. However, the stealth of the J-20 still remains to be shown, and US military heads do not appear very concerned. On the other hand, what may worry them is the J-20's capacity to strike from a distance with PL-15 air-to-air missiles, which could endanger refuellers and, as a result, compromise the missions of the F-22 and F-35. Cf.: http://www.opex360.com/2017/03/10/la-chine-affirme-avoir-mis-en-service-le-chasseur-bombardier-furtif-j-20/.

55 https://www.google.fr/search?q=china+airshow+2016&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwi9-76e34_UAhXG5xoKHbCZBmkQsAQITw&biw=1304&bih=658#tbm=isch&q=china+air+show+2016&spf=1495876802471

In particular:

Cloud Shadow Chinese HALE reconnaissance or attack UAV proposed for export (Chengdu Aircraft Corporation; member of the *Aviation Industry Corporation of China* (AVIC)). This UAV is developed for high-altitude, long-endurance (HALE) missions. With a wingspan of 17.8 m and measuring 9.05 m in length and 3.66 m high, it has a take-off weight of 3,000 kg including 1,000 kg of fuel for 6 hours of flight. Its flight altitude is 14,000 m. It can carry up to 400 kg (*editor's note:* ***for memory, the limit of the MTCR category I = 500 kg!***) of equipment in reconnaissance version. The attack model has four hard points, including two double nacelles to integrate air-to-ground weaponry such as missiles or guided bombs. In this configuration, the payload is 200 kg. The control station is arranged in a removable container presented at the show on a *Dong Feng* truck. The transmission between the ground segment and the drone, of LOS type *(Line Of Sight*), has a range of 290 km (*editor's note:* ***for memory, the limit of the MTCR category I = 300 km!***). According to CAC, the export market is the main target. (cf. http://www.defense.gouv.fr/ema/sitta/les-salons-precedents/china-airshow-2016/article-china-airshow-2016.).

Divine Eagle HALE UAV (the Shenyang 601 Design Institute has been working on this anti-stealth aircraft drone project for more than ten years). This drone measures approximately 6 metres in height and 15 metres in length (since most high-altitude large UAVs have a wingspan to body length ratio of 2.5:1 to 3:1, the wingspan of the Divine Eagle is likely its be 35 to 45 meters across). With a maximum take-off weight of at least 15 tons, the Divine Eagle is the world's largest UAV, ahead of the US RQ-4 Global Hawk. With its giant double bodied design, carrying high performance anti-stealth radars, the drones are a potential key part of China's offensive and defensive military strategy in the coming years, emphasizes the magazine *Popular Science*. Formations of Divine Eagle UAVs are expected to provide an early warning line to detect threats to China's airspace, like cruise missiles and stealth bombers, as well as be able to take on such missions as hunting for aircraft carriers in the open waters of the Pacific. The drone can also vector enemy aircraft and ships into combat zones. Some experts also believe that the Divine Eagle could be able to find targets for the "sadly" infamous DF-21D anti-ship ballistic missile, nicknamed by some as the "carrier killer". It would therefore be a new threat for the deployment of US forces in the West Pacific whereas the United States have made this region the "pivot" of their strategy.

Wing Loong II (Chengdu Aircraft Design & Research Institute (CADI)). This multi-role *Medium Altitude Long Endurance* (MALE) UAV is equipped with an electro-optical surveillance and fire-control system, an SAR (*Synthetic Aperture Radar*) and laser and GPS weapons guidance systems. Other equipment can be integrated including ELINT (*electronic intelligence*), COMINT (*communication intelligence*), radar jammers or communication relays. Measuring 11 m in length, and 4.10 m in height, with a wingspan of 20.50 m, the maximum takeoff weight is 4,200 kg. It has six hardpoints for a total payload of 480 kg (*editor's note:* ***for memory, the limit of the MTCR category I = 500 kg!***). Its maximum flying speed is 370 km/hr for a maximum altitude of 9,000 m. It has a range of 20 hours. It features a control station

3.2 A SERIOUS COMPETITOR IN THE MEDIUM TO LONG TERM

This attendance should no doubt be seen as recognition that China is a competitor to be taken seriously and treated carefully in the medium to long term, failing the possibility of building real Defence partnerships in the near future, while the 1989 arms embargo imposed for violation of human rights has not been lifted[56].

---

and a logistics container. The LOS transmission has a range of 200 km (*editor's note:* ***for memory, the limit of the MTCR category I = 300 km!***). This drone offers both military and civil applications. It would appear to directly compete with the new CH-5 UAV from the *China Aerospace Science and Technology Corporation* (CASC). (cf. http://www.defense.gouv.fr/ema/sitta/les-salons-precedents/china-airshow-2016/article-china-airshow-2016.).

Broad-spectrum target missiles (Beijing Symbol of Power Technology Development Co. Ltd (BEIWEI)). Third generation complex from the *TY Gen. III* family, still partly under development. Consisting of 1) the command and control vehicle (*Beiben Truck 1928* 4x4) which carries the fire control and telemetry equipment; 2) two launchers (on *Beiben Truck 3232* 6x6 carriers), equipped with four target-missile containers. Three types of targets proposed: a) The *TYK-1* simulates an air-to-ground missile (flies at 330 m/s up to an altitude of 6,000 m and a distance of 50 km); b) the *TYD-1* characteristic of a tactical ballistic missile (average speed of 1,500 m/s, altitude of 50 km, range of 280 km); c) the *TYX-1* simulates a cruise missile (speed 280 m/s, flying at altitude of between 50 m and 2,500 m over a distance of 35 km). **These three missiles are equipped with inertial guidance and GPS receiver**. The growing export of Chinese ground-to-air production should favour its ambitions internationally. (cf. http://www.defense.gouv.fr/ema/sitta/les-salons-precedents/china-airshow-2016/article-china-airshow-2016.).

SLC-7 **long-range aerial detection 3D RADAR for the export market** from **Nanjing Research Institute of Electronic Technology** (NRIET), the CETC group's radar manufacturer. This radar operates in L band; it is equipped with a **radiator**. Its primary vocation is medium-altitude/medium-distance air search for targets such as aircraft, cruise missiles and guided munitions. Its maximum detection range is announced at 400 km. It may be associated with medium-range search radar operating in S band, usable for long-range ground-to-air weapons systems or aerial defence control stations. (cf. http://www.defense.gouv.fr/ema/sitta/les-salons-precedents/china-airshow-2016/article-china-airshow-2016.).

JY-50, the Chinese multistatic radar (CETC-China). Discretion remains the best solution to conceal one's position and guarantee one's security. Faced with the problem of radar emissions, the use of passive systems based on detection of adverse electromagnetic signals is a good alternative. However, it requires a so-called "cooperative" target. Institute no. 38 of the CETC offers a piece of equipment based on the multistatic radar concept which **uses, by way of emitters, FM-band radio broadcasting stations**. The principle has already been prepared by the main players in radar. It consists in using radar reception equipment, the *JY-50*, to establish a fixed map of the FM radiation received. **Any aerial target penetrating** this bubble reflects energy and **modifies the radar's electromagnetic environment**. The *JY-50* can process two FM emitters simultaneously and cover a sector of 60°. Signal analysis and processing define the course, distance and speed of the target. Maximum detection distance is 300 km. The frequency band used is particularly suited to detecting stealth aircraft. The *JY-50* is the equipment of the future that will work in support of more conventional search radar. (cf. http://www.defense.gouv.fr/ema/sitta/les-salons-precedents/china-airshow-2016/article-china-airshow-2016.).

The VT 5 main battle tank (Norinco) is destined for export in the 30-ton class; it is equipped with a laser detection system and can feature combined composite and reactive amour ballistic protection.

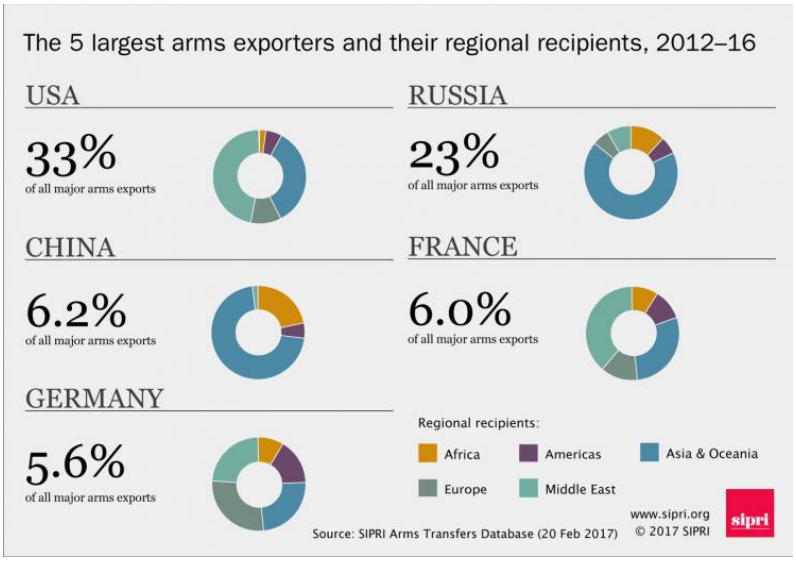
WR 901 **land combat drone (Beijing Hua Xin Fagn Zhouke Ji Co Ltd)**. This drone can use rubber tracks or wheels. Used mainly for observation and intelligence missions, it can be armed with a machine-gun or a rifle (e.g. *QBZ 95)* to deal with targets up to a distance of 400 m. The on-board equipment (digital radar, scanning radar and sonar) means it automatically avoids obstacles, whether stationary or mobile.

SeaFly **sea surveillance USV** (Beijing Sifang Automation Co Ltd); intended for the navy, coastguards, oceanographic research or environmental protection services. The *SeaFly* can be armed or carry a small UAV.

56 The EU's sanctions against China were taken on 26 June 1989 in a Council declaration in Madrid. Again in Madrid, on 16 December 2015, the Council clarified and limited the framework of the embargo to "lethal weapons and

To expand its military-industrial capacities, **China may well seek to initially develop its exports in the conventional sector** (the one controlled by the Wassenaar Arrangement) **rather than in the extremely sensitive sector of WMD targeted in particular by the NSG, the Australia Group and the MTCR.**

From this viewpoint, in its latest report (20 February 2017), the SIPRI indicates that China is the world's third-ranking arms exporter, selling abroad more and more, with the most spectacular increase being in Africa: +122% over the 2012-2016 period[57].



The SIPRI underlines the growth of the African market as follows: "While the continent is the world's smallest arms importer, some African countries stand out for their frenetic purchases of frigates, submarines, and fighter helicopters". **Which African countries import the most arms?**

Not surprisingly, Algeria and Morocco rank top amongst the biggest arms importers. Together, they account for 56% of arms imports to the continent. While Algeria is the largest importer of arms in Africa, its purchases abroad have dropped 18% compared to the 2006-2010 period. These figures should be put into perspective: in the next five years, Algeria plans to heavily equip its powerful military institution. Expected deliveries include the purchase of four frigates, 190 tanks, 42 helicopters, 14 fighter aircraft and 2 Russian submarines. As for Morocco, the

---

ammunition", but in compliance with the 8 criteria of the 1998 "Code of Conduct" (which became the **Council Common Position 2008/944/CFSP** of 8 December 2008), defining common rules governing control of exports of military technology and equipment. NB: it would seen that only France applies this position very clearly; the other major arms-producing Member States such as Germany or the UK officially retain an extensive interpretation of the sanctions and state that they apply them to all the Defence-related items covered by Directive 43/2009 on transfers of military products within the Community.

57 According to the latest SIPRI publications (http://books.sipri.org/files/FS/SIPRIFS1602.pdf), China currently exports its arms to neighbouring countries that it can protect from the India/Pakistan conflict. Pakistan is the largest importer of Chinese weapons (with 35%, the latter protects the country against the United States). China's other major customers are currently Bangladesh (20%) and Myanmar (16%).

increase in arms imports is impressive, growing 528% between 2011 and 2015 compared to the previous five years. Despite this stunning increase, volumes remain below the purchases of neighbouring Algeria. Far behind, Uganda is the continent's third arms importer, with 6.2% of African imports between 2011 and 2015. In total, Sub-Saharan Africa represents 41% of arms purchased outside the continent. And while Uganda ranks first in the sub-region, Nigeria and Sudan are close behind Kampala.

What about the countries at war against Boko Haram? The SIPRI also focuses on countries fighting Boko Haram, whose arms imports paradoxically remain small. In total, arms deliveries to Cameroon, Chad, Niger and Nigeria accounted for 0.6% of total global imports between 2011 and 2015, asserts the Institute. Their acquisitions include numerous military aircraft, including some combat UAVs. Between 2011 and 2015, China sold five aircraft of this type to Nigeria. However: "We only count heavy weapons, not light weapons. But countries facing terrorist groups buy more light weapons for their armed forces", explains Aude Fleurant, head of the SIPRI Arms and Military Expenditure programme.

So, where do the arms purchased by Africans come from? Most of the weapons imported onto the continent come from Russia, followed by France that now ranks equal with China on the market: in the arms sectors, China is indeed recording consistent growth as a result of the increase in its production capacities over the past twenty years. "China has also invested heavily to improve the quality of its production", says the head of the SIPRI Arms and Military Expenditure programme. But China's production capacity does not explain everything. These contracts are also closely linked to Beijing's economic influence on the continent, explains Aude Fleurant: "In some African countries where China has developed strong relations in trade, mining or energy, it is easier to secure arms contracts." [58]

Consequently, although a certain slowdown is being seen in Africa's military expenditure overall, China probably has the biggest chance of maintaining its market share on this continent, owing to its massive capacity to produce items offering good performances at extremely competitive costs, and its foreign policy that aims to expand its footprint in all the emerging countries. Tanzania is one of the many African countries that receive weapons from China to improve its defence against the crisis in Sudan, with six Chinese ships, three squadrons of fighter planes and military transport aircraft.

3.3 ASSESSMENT OF CHINA'S STRATEGY FOR ARMS EXPORTS

To attempt to assess China's strategy based on some concrete signs, it is interesting to examine the country's membership to the various international circles of sensitive product control. The table below lists the main multilateral agreements in the most sensitive areas[59].

Nuclear Weapons Treaties

58 http://www.jeuneafrique.com/305138/politique/marche-de-larmement-afrique-achete-quoi-a/

59 cf. Philippe Achilleas, (p.91 to 116) and Marion Feurtey (p. 201 to p.204) in "*Export Control Law And Regulations Handbook*, *third edition* (– published by Yann Aubin and Arnaud Idiart on 06/28/2016 at Kluwer Law International). https://lrus.wolterskluwer.com/store/products/export-control-law-regulations-handbook-third-prod-9041154434/hardcover-item-1-9041154434.

Treaty Name	Overall Status	Specific Status	Enforceable in China
Test Ban			
Limited Test Ban Treaty[60]	OS: 5 August 1963 EF: 10 October 1963	–	No
Comprehensive Nuclear Test Ban Treaty[61]	OS: 24 September 1996 EF: not in force	S: 24 September 1996	No
Non-proliferation			
Nuclear Non-Proliferation Treaty[62]	OS: 1 July 1968 EF: 5 March 1970	A: 9 March 1992	Yes
IAEA Comprehensive Safeguards Agreement(s)[63]	EF: 18 September 1989	N/A[64]	Yes
IAEA Model Additional Protocol[65]	S: 31 December 1998 EF: 28 March 2002	N/A[66]	Yes

Abbreviations: OS: Opened for signature; EF: Entry into force; S/R: Signature/Ratification; A: Accession.

Biological and Chemical Weapons Treaties			
Treaty Name	Overall Status	Specific Status	Enforceable in China
Geneva Protocol[67]	OS: 17 June 1925 EF: 8 February 1928	A: 24 August 1929	Yes

60 Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, *UNTS,* vol. 480, 43.

61 UNGA, resolution 50\245.

62 Treaty on the Non-Proliferation of Nuclear Weapons, *UNTS*, vol. 729, 161.

63 Agreement Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), INFCIRC/153 (Corrected).

64 This treaty is a bilateral one and, accordingly, the differences that apply to multilateral treaties (between the overall status and the specific status) do not apply.

65 Model Protocol Additional to the Agreement(s) Between State(s) and the Agency for the Application of Safeguards, INFCIRC/540(Corrected).

66 This treaty is a bilateral one and, accordingly, the differences that apply to multilateral treaties (between the overall status and the specific status) do not apply.

67 Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, 94, *League of Nations Treaty Series*, No. 2138 (1929).

Biological Convention[68]	OS: 10 April 1972 EF: 26 March 1975	A: 15 November 1984	Yes
Chemical Convention[69]	OS: 13 January 1993 EF: 29 April 1997	S: 13 January 1993 R: 25 April 1997	Yes

Abbreviations: OS: Opened for signature; EF: Entry into force; S/R: Signature/Ratification; A: Accession.

Multilateral Export Control Regimes		
Regime Name	Formation	Participation
Zangger Committee[70]	1971	Yes
Nuclear Suppliers Group	1974	Yes
Australia Group	1985	No
Missile Technology Control Regime	**1987**	**No**
Wassenaar Arrangement[71]	1994	No

Others		
Name	Adoption	Participation
UN Register on Conventional Arms[72]	9 December 1991	Yes[73]
Programme of Action on Small Arms and Light Weapons[74]	20 July 2001	Yes
International Code of Conduct - HCoC[75]	**25 November 2002**	**No**

68 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and On Their Destruction, *UNTS*, vol. 1015, 163.

69 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Doc.CD/CW/WP.400/Rev.1.

70 Non Proliferation Treaty Exporters Committee (also called the Zangger Committee).

71 Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies.

72 A/RES/46/36/L.

73 Information provided for the calendar years 1992 to 1996.

74 Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Aspects, A/CONF.1992/15.

75 The Hague Code of Conduct against Ballistic Missile Proliferation, not yet published.

3.4 CHINA'S POSITION IS ACTUALLY QUITE "REASONABLE"

For all that, China is a member of the UN Security Council and, as such, enjoys undeniable influence and special relations with the main Western powers. It is therefore probably not prepared to run the risk of losing this privileged status, by clashing too violently with its peers. Even though the negotiations are sometimes very "strained", **on the most serious matters, its position is ultimately quite "reasonable"**; this was again the case recently, in the P5+1 negotiations during nuclear work for the partial lifting of sanctions against Iran and the development of the JCPOA[76].

In this case, the very firm attitude taken to North Korea is not therefore surprising, even though the threat and the direct stakes for the Chinese territory or government do not seem decisive; **another explanation (not exclusive of the first) could be that the priorities of Chinese foreign policy lie elsewhere**[77]**.**

It would therefore seem that, for many years still, the "great powers" will continue to jealously keep a watchful eye, like China, to guarantee their own security, on all developments in the international arms market and particularly on risks of proliferation of WMD.

4 CONCLUSION AND PRACTICAL RECOMMENDATIONS

In the spirit and within the framework of resolution 1540 on the non-proliferation of weapons of mass destruction, **three major problems of export control must be considered.**

Ballistic missiles are very high-tech products that use a great many products covered by the European **Dual Use** Regulation no. 428/2009. They are also **Defence-related products** coming under Directive no. 43/2009 for the purpose of regulations on exports of military goods and technologies. Finally, concerning **nuclear, chemical or bacteriological items**, specific

76 https://en.wikipedia.org/wiki/Joint_Comprehensive_Plan_of_Action.

77 On 25 January 2017, within the framework of Resolution 1718 (2016), China published a new list (reference "2017 no. 9") of dual-use goods and technologies prohibited for export to North Korea, adding new articles that can be used for weapons of mass destruction (WMD). The section on sensitive materials includes, for example, chemicals such as TDI (toluene diisocyanate), HMDI (hexamethylene diisocyanate) and IPDI (Isophorone diisocyanate), for the synthesis of HTPB solid propellant used in certain ballistic missiles and space launch vehicles. Materials absorbing electromagnetic waves, ranging from VHF to the J band, and ceramic composites and other metal alloys that would enable North Korea to manufacture coatings and the light and solid missile airframe, while reducing the anti-missile detection distance also feature on the list. 6×6 chassis trucks or more are now part of the Chinese products that may no longer be exported to North Korea, although the TEL (Transporter-erector-launcher) of the North Korean intercontinental ballistic missile **KN-08** (화성-13) is derived directly from the **WS-51200** chassis from the Chinese group CASIC for example. The latter was imported into North Korea under the name "roundwood transport vehicle". Devoid of mobile launch platforms and incapable of manufacturing them itself in the short or medium term, North Korea will be compelled to fire its missiles, the range of which can reach the US base in Guam for example, from fixed missile pads that are easily detectable and destroyable by aerial and naval strikes. But it is also interesting to note that this embargo by China is not "total", and does not cover items capable of contributing to the articles capable of contributing to the threat on South Korea and Japan, two vassals of the United States, no doubt indicating an umpteenth compromise between the US, Russia and China… cf.: http://www.eastpendulum.com/chine-interdit-exportation-biens-double-usage-vers-coree-du-nord.

regulations reinforce the general obligations of sensitive product control and thus the ensuing administrative burden.

In return, this accumulation of regulations automatically multiplies the verifications of documents and products. Controls are therefore carried out every stage in the chain: negotiations, procurements, production, commercial channels, transports, etc., multiplying the opportunities to detect any inaccurate declaration, manipulation, or attempted unauthorised re-export **to ultimately reduce the risk of diversion considerably.**

All industrial operators in the major exporting nations concerned by the risk of proliferation are today very aware of export control and they are practically all organised to guarantee the quality of their internal export control.

The problem is well identified and the constraints and limits of solving it are well known or anticipated. **The difficulty for export control, introduced particularly to control the spread of weapons of mass destruction, can still today be summed up in three words 1) identification, 2) marking and 3) traceability of data.**

Technical solutions to these three problems are developing at the speed of the exponential growth[78] in digital production, which constantly requires new processing and storage methods to be found.

This explosion in volumes leads, despite progress in "Big Data" analysis, to abandoning the dream of government agencies (which had been assessed in 2004 by the European Commission[79]) of controlling all export transactions thanks to a big database and a computer system entrusted to the European Commission. This material impossibility will no doubt accelerate the **basic shift, initiated at the end of the 1990s, from "ex-ante" control[80] of sensitive military and dual-use equipment exports to an "ex-post" control of transactions, with an almost total transfer of responsibility to companies.**

In companies, just like "Quality Control" in its time, "Export Control" is now evolving towards audit and qualification of procedures.

In parallel, regulatory requirements are adapting. A significant development has just been launched by the USA concerning controlled data exchanges covered by the EAR[81]. The regulations have been adapted according to the pragmatic Anglo-Saxon "best efforts" logic. The aim was to address both the impossibility for industry to guarantee full compliance of all intangible exchanges, and the

78 According to an IDC study for EMC (Infographic, PDF) published in April 2014, the volume of data produced in what they call the Digital Universe should increase ten-fold between 2013 (4.4 Zettabytes) and 2020 (44 Zettabytes). *44 Zettabytes = 44 trillion gigabytes.* If the Digital Universe were represented by a stack of tablets (Apple iPad Air 0,29" and 128 GB of storage), in **2013** it would have stretched 2/3 the way to the Moon and in 2020, there would be 6.6 stacks of tablets from the Earth to the Moon.

79 Cf. UNISYS report, Intra-Community Transfers of Defence Products, Brussels, February 2005, 191 pages.

80 Almost systematically governmental, via customs

81 The Export Administration Regulations – EAR – apply to all purely civil, dual-use and even military goods not considered very sensitive (sensitive military products are covered by the International Traffic in Arms Regulations – ITAR).

Government's inability to continue performing satisfactory control of operators within the existing framework. **Henceforth, if the technical data they exchange is encrypted[82], an export licence is not required for companies** whose organisation, procedures and information system security tools are **certified**.

IN A NUTSHELL

• **The efforts made** in export control by all the most industrialised countries over the past 30 years **are truly beginning to deliver results** and particularly as regards transfers of WMD-related technologies by intangible channels.

• For **"well-known" companies recognised as "responsible exporters",** it is therefore time to **stop** cumulating the two administrative systems of **"ex-ante"** and **"ex-post"** control that seriously penalise their competitiveness.

• **Improvements will particularly be achieved by capillary dissemination of export control "best practices"**. This role should be encouraged and recognised by the authorities. It is already largely and naturally fulfilled by "responsible exporters", on a daily basis, within the framework of "supply chain" quality assurance via the requirements of subcontracting and partnerships.

• **At the same time,** with the main aim of introducing harmonised governmental procedures recognised as being equally valid, **outreach actions must be reinforced**. Led by government agencies, extensive involvement of operators is key to achieving this improvement, as they can provide invaluable experience and input for the success of operational organisational measures.

82 "Neither Transfer or Export Licence should be required for encrypted technical data between certified companies (as far as their IT security organisation, processes and tools are certified)".