European Parliament

WORKSHOP

DUAL USE
EXPORT CONTROLS

INTA, SEDE

EN

2015

European Parliament

WORKSHOP

Dual use export controls

ABSTRACT

Although EU Regulation 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items system is in line with the main export control regimes and is seen as a model for others to follow, there are a number of ways in which the regulation could be enhanced and refined. Part One outlines the current state of play, purpose and implementation of the current regulation. In Part Two, against the backdrop of the European Commission's reform proposal, the effectiveness of the EU's dual-use export controls regime is explored further with regard to its potential contribution to international, national and human security, as well as their impact on EU economic and trade interests. The study concludes that the system's effectiveness could be improved in a number of ways, but that this requires an effort to mobilise political will at different levels and across different institutions within the EU and its Member States, and to enhance human resources, cooperation and capacity-building. The European Parliament should also give consideration on a regular basis to issues relating to the scope and implementation of the regulation, in order to ensure that the objectives continue to be achieved.

WORKSHOP
POLICY DEPARTMENT, DG EXPO
FOR THE COMMITTEE ON INTERNATIONAL
TRADE (INTA) AND FOR THE SUB-COMMITTEE
ON SECURITY AND DEFENCE (SEDE)

WEDNESDAY 17.06.2015 – **10:30-12:30**
ALTIERO SPINELLI BUILDING – ROOM **A1E-2**

CONTACT AND REGISTRATION: **poldep-expo@europarl.europa.eu**

Parlement européen

DUAL-USE
EXPORT
CONTROLS

Co-Chairs: **Bernd LANGE & Anna FOTYGA**

Table of contents

PROGRAMME OF THE WORKSHOP

For the Committee on International Trade (INTA)
And for the Sub-Committee on Security and Defence (SEDE)

WORKSHOP
Dual use export controls

Wednesday, 17 June 2015
Brussels, Altiero Spinelli Building, **Room A3G-3**
10.30-12.30

PROGRAMME

10.30-10.40 Welcome and introductory remarks by

- **Bernd LANGE**, Chair of the Committee on International Trade (INTA)
- **Anna FOTYGA,** Chair of the Sub-Committee on Security and Defence (SEDE)

10.40-10.55 The cornerstones of the proposal for reforming the EU's dual-use control system

Speakers:

- **Paolo GARZOTTI,** Head of Unit for WTO coordination, OECD, Export Credits and Dual Use, European Commission, DG Trade

10.55-11.25 The need for reform of the EU's dual-use export control system and how to get it right?

Speakers:

- **Prof. Ian STEWART**, Head of Project Alpha, King's College, London
- **Dr Sibylle BAUER,** Director of Dual-use and Arms Trade Control Programme, Stockholm International Peace Research Institute (SIPRI)

11.25-12.20 Q&A

12.20-12.30 Concluding remarks by the co-chairs

BIOGRAPHICAL SUMMARIES OF THE SPEAKERS

For the Committee on International Trade (INTA)
And for the Sub-Committee on Security and Defence (SEDE)

WORKSHOP
Dual use export controls

Wednesday, 17 June 2015
Brussels, Altiero Spinelli Building, **Room A3G-3**
10.30-12.30

BIOGRAPHIES

Dr. Sibylle BAUER

Dr Sibylle Bauer is Director of the Dual-use and Arms Trade Control Programme at the Stockholm International Peace Research Institute. Before joining SIPRI in 2003, she was a Researcher with the Institute for European Studies of the Free University of Brussels (ULB). She holds a PhD in Political Science jointly from the Free University of Brussels (ULB) and the Free University of Berlin. Dr Bauer has published widely on dual-use and armaments-related issues, including contributions to the SIPRI Yearbook on developments in export controls since 2004. Since 2005 she has spent much of her time on capacity-building to enhance transit, transhipment, brokering and export controls for dual-use items, with a focus on Europe and South East Asia. This has included responsibility for national and regional activities on legal, industry outreach and enforcement issues. Publications include 'Nuclear export control', Routledge Handbook of Nuclear Non-proliferation and Policy (May 2015) and ,WMD-related dual-use trade control offences in the European Union: penalties and prosecutions' (EU Non-Proliferation Papers, no. 30), July 2013.

Mr. Ian STEWART

Ian J. Stewart is a Senior Research Fellow in the Department of War Studies and runs Project Alpha at King's College London, a collection of projects that work to improve the implementation of export controls. Research conducted by Project Alpha under Ian's leadership includes mapping the manufacturing base for key " chokepoint" technologies and mapping all known cases of illicit trade involving Iran's nuclear program. Project Alpha has also recently conducted a study into the production value of dual-use goods in the European Union.

Mr Stewart came to King's College London from the British Ministry of Defence, where he was an analyst working on issues related to non-proliferation and illicit trade. Before this, Ian held a variety of roles in the MOD including supporting the UK's nuclear deterrent and undertaking a placement in the British Embassy, Washington DC. Ian was formally also a Managing the Atom and International Security Program fellow at Harvard's Belfer Centre. He holds masters degrees in Nuclear Science and Technology and Electrical and Electronic Engineering and is studying toward a PhD on the subject of how supply-side controls have affected nuclear proliferators from the 1970s to present day.

PART I: EU EXPORT CONTROLS: THE STATE OF PLAY AND THE NEED FOR REFORM (by Ian J. Stewart)

1   Introduction

Through the adoption of regulation 428/2009, both the EU as an entity and its individual Member States committed to uphold international standards and obligations with regard to peace and security while also meeting the imperatives of trade facilitation.

In order for this to be achieved, the EU export control system is in constant need of re-evaluation so as to ensure that an ever-growing number of emerging technologies and a broader range of dual-use items are integrated in its approach to tackle worldwide WMD proliferation, while continuing to serve as a benchmark for non-EU member states. As such, a thorough review process has been underway since 2011. To date, several proposals for enhancing the EU's dual-use system have been made, including in relation to human rights and transparency issues. During the time of this review, several main issues in the export control policy of the EU have been identified. Some of these have already been addressed, such as the process by which the EU control list is updated. Other issues that have been identified include a need to recognise a shift in underlying control policy (e.g. human security dimension), technological relevance (e.g. list of goods), licensing architecture, brokering, transit and technology controls, intra-EU transfer controls, transparency and private sector implementation, EU implementation capacity and global convergence.

Part One of the report explores the state of play and the need for reform. It also provides an overview of the need for reform of regulation 428/2009, while also taking into consideration multilateral and major national control regimes that are comparable to that of the EU, including that of the United States. Current security challenges are also addressed, taking into account the main targets of the controls, including the transfer of goods, technology and knowledge via ecommerce, cloud cyber tools and surveillance technologies.

This examination of regulation 428/2009 concludes that while the regulation is fit for purpose, there are considerable improvements that can be made to the current approach. These are also discussed in the sections below.

2   Assessment of Regulation 428/2009

Regulation 428/2009 forms the basis of export control implementation in the European Union. In summary, the regulation sets a common policy for export controls but leaves each state to implement the regulation, including with regards to licence decision making – although coordination and administrative measures exist to promote common implementation. (European Council 2009) The approach of regulation 428/2009 is efficient but creates certain issues related to coordination and adminision that should be addressed in the review. It is thus helpful before examining specific areas in which the regulation could be improved to summarise the existing regulation itself and to identify the main limitations and issues that it produces. It is also important to note that export controls are compatable with free trade arrangements, including GATT (the General Agreement on Tariffs and Trade), through the various articles of exemption. [1]

---

[1] See https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm

2.1 Background to the Regulation

Council Regulation (EC) No 428/2009, adopted 5th May 2009, serves as the governing document for the EU's export control regime. It provides for common EU control rules, a common EU control list and harmonised policies for its implementation. 428/2009 represents a recast of the previous legislation: Regulation 1334/2000. The purpose of Regulation 428/2009 was to fold the significant number of amendments made to Regulation 1334/2000 into a new, clearer document, thus facilitating its implementation as well as subsequent amendments to the regulation.

The expansion in scope of 428/2009 compared to 1334/2000 (without its amendments) is clear from the documents' respective explanatory titles. The sub-title of 1334/2000 reads; 'Setting up a Community regime for the control of exports of dual-use items and technology.' (European Council 2000) This is less broad in scope than the title of regulation 428/2009 which includes the words; 'transfer, brokering and transit.' (Quentin Michel 2011) In real terms, this reflects the fact that amendments, including those adopted in response to UNSCR 1540, were fully integrated into the regulation as opposed to being bolted on to 1334/2000.

Regulation 428/2009 also requires the commission to conduct a periodic review, which drove the current review process. In the context of the Lisbon Treaty, it would be appropriate for the European Parliament to more regularly review the scope and implementation of the regulation. This could be achieved by holding periodic workshops and hearings on the fitness of purpose of the export control system created by the regulation.

2.2 Common Policy

It should be noted that many of the requirements of regulation 428/2009 originate outside of the EU in the various international treaties, conventions, and export control regimes in which most or all EU member states participate. In this context, it can be observed that regulation 428/2009 principally ensures a common EU approach to the implementation of such externally-originating requirements. However, the European Union can and does go beyond these external commitments.

The regulation thus creates a common policy and approach between member states on several issues including with regards to the legal basis of controls, control lists, definitions and interpretations. It also provides the legal basis for the implementation of export controls in member states where export controls cover the export, transit and transhipment of control goods and measures to control other goods based on end uses.

The regulation also creates a common list of technologies that are subject to control, although states have the right to control additional items in certain circumstances. In accordance with the treaty on the functioning of the European Union, the European Parliament became responsible for approving amendments to the control list contained in the regulation. An unfortunate real-world effect of this was to slow the adoption into EU law of changes to the lists made by the main export control regimes. This issue was addressed in regulation 599/2014, which gives the Commission delegated authority to address this point and other related matters.

Definitions and interpretations: A vital aspect of the regulation is in setting common definitions for certain export-control related issues across Europe. The control list contained in the resolution is used by many countries outside of the Union, making the EU export control regulation a de facto international standard. Despite this, there are places where the language of the regulation is not clear. In this context, the Dual Use Coordination Group has played an important role in interpreting the regulation – interpretations that have, so far, not been shared with external stakeholders.

It is important to note also that the scope of regulation 428/2009 provides for control not only of exports from the European Union, but also certain transfers through the Community, transfers within the Community and transfers from country to country outside of the Community.

- Transfers through the Community: the regulation includes controls on shipments passing through the Community that do not formally enter the Community for tax purposes (i.e. transit and transshipment). Such controls can play a vital role on intercepting shipments from other countries to programmes of concern, and their use is typically driven by intelligence or other information.

- Transfers from third country to country (brokering): the regulation includes provisions to cover brokering of dual-use items when the broker is aware or has been informed that the items are for a WMD end use. Such brokering controls play a conceptually important role in addressing the possibility that a European citizen could assist a country in the acquisition of WMD without exporting goods from the Union. In reality, such controls are only likely to be used as reactive rather than proactive measures: their primary purpose is to deter and, if necessary, punish individuals for involvement in this activity.

- Transfers within the Community: the regulation includes a requirement for the authorisation of transfers of certain sensitive items within Europe "pending a greater degree of harmonisation". The history of these measures partly relates to the reporting requirements under the IAEA's Additional Protocol and other international treaties. Specifically, EU member states are required to keep records of transfers of such goods – even to other EU member states – in order to report this information to international authorities. There is some possibility that this requirement could be replaced by a reporting requirement.

Beyond the question as to which destinations transfers may be controlled is the question of the scope of the regulation. Principally, the regulation controls a defined list of physical goods and the intangible 'technology' and software associated with these goods. However, the regulation also includes provisions to control goods not listed when destined for end uses of concern. (These are called 'catchall controls'). In keeping with Joint Action 2000/401/CFSP some member states enact controls on the the provision of technical assistance (i.e. in-person support to WMD programs).

The regulation also goes some way to defining how exports of the controlled items can take place: the regulation defines various types of licence, including community, national, single, individual and general. It is notable that the licence types available in each member state do vary, however; for example, many Member States do not offer national general licences, which could have the effect of distorting the market competition. The expansion in the number of community general licences in recent years is one part of a solution, but states should also be encouraged to offer more national licences.

While these aspects of the regulation can be thought of as common among EU member states, the regulation also leaves much to member states.

2.3　　　　National Implementation

While the regulation creates a common policy and approach on certain issues, implementation and enforcement of the regulation is primarily left to member states. Specifically, the regulation recognises that:

> *The responsibility for deciding on individual, global or national general export authorisations, on authorisations for brokering services, on transits for non-Community dual-use items or no authorisations for the transfer within the Community of the dual-use items listed on Annex IV lies with national authorities.* (European Council, 2009)

In order to implement the regulation, there are a variety of actions that member states must take. These include appointing competent authorities, operating a licensing process (with associated decision making) and carrying out measures to enforce the regulation.

Licensing process: The regulation outlines the items of information an authority must capture in order to consider the granting of an authorisation. Beyond this, however, it is largely up to member states' discretion to decide how to implement the licensing process (and indeed what types of licence to make available). There is considerable variation between states in terms of the licensing process: some states have fully-electronic systems whereas others use paper-based systems, or a mix of the two. Some member states have automated integration with customs systems, whereas others lack such applications. Some publish target turn-around times for applications whereas others do not. Some offer services to aid exporters in order to understand the control status of their goods, whereas others do not offer such amenities. To some extent, the variation in the licensing process among member states may reflect the amount and value of dual-use exports within each country. Nonetheless, the variation in the licensing process among states has the potential to distort the EU marketplace.

Decision making: the regulation lists the types of issues that states should take into account when reaching decisions on whether or not to grant specific authorisations. However, the regulation does not create an environment in which similar decisions would be reached in all states. There are perhaps two reasons for this: the regulation does not identify the assessment criteria that should be used, nor does it create the circumstances in which all states have access to the same information on which to make decisions. On this second point, while there is a common security and defence policy within the EU, it is perhaps unrealistic to expect that all states would reach the same decisions on particular exports when risk perceptions and decision making processes vary. Nonetheless, efforts should be made to minimise any such differences as they result directly in market distortion. Some of the recommendations provided at the end of this report were drafted with this in mind.

The regulation makes it illegal for individuals and entities to export controlled goods without authorisation. The enforcement of export controls in the EU's 28 member states is the responsibility of national authorities. This results in there being some variation in how export controls are implemented and enforced in practice. Conclusive data about implementation and enforcement remains elusive in most countries. This makes it challenging to analyse how the regulation is being enforced. More problematically, it also lessens the deterrent effect of past enforcement actions. As such, it is recommended that information on implementation and enforcement approaches be adopted at an EU-wide level so as to ensure that a clearer view is provided over enforcement practices.

Most EU member states have conducted few if any prosecutions for export control violations related to dual-use goods. While the powers of the respective authorities are outlined in legislation, individual cases of enforcement are difficult to track since they are not made public due to anonymity claims and thus offer a skewed view of Europe's compliance records. In some cases, it might appear that some member states have spotless prevention mechanisms in place when in fact their respective national authorities have failed to prevent, detect or prosecute illicit exports of dual-use goods.

While there are practical challenges to doing so, including some related to the split of competences between the EU and member states, consideration should be given to how to standardise penalties.

More generally, in order to improve national implementation, a high priority should be assigned to the task of creating a so-called 'inreach' program to build capacity among member states.

2.4   Coordination and Administration

Given that all 28 member states separately implement the regulation, there is evidently a need for common coordination and administration. The regulation provides for this, identifying several specific mechanisms tailored to specific coordination or administration requirements. Most notable among these are:

- The creation of a secure web-based communication platform through which to share information on denials of licences and other information, as defined;

- The creation of a coordination group.

The Dual-Use Coordination Group is a commission-chaired forum that meets to discuss implementation issues. There is also a Council Working Party which considers legal and policy issues, including with regards to legislative proposals from the commission. It should be noted that the coordination group works to address issues around implementation of the regulation, and it is not a forum in which issues relating to trends in illicit trade or enforcement cases are routinely raised: There is, as such, no equivalent within the EU of the licensing enforcement working group of the Wassenaar Arrangement or of the Licensing and Enforcement Experts Meeting of the Nuclear Suppliers Group. It is recommended that consideration be given to establishing such a forum, perhaps in partnership with TAXUD.

Another aspect of coordination relates to so-called denial notifications – notices that member states must, or in some cases should, provide to the Commission for onwards transmission to other states. Denial notifications provide a mechanism to prevent 'undercutting' – that is, the issuing of a licence from one jurisdiction when it had been refused by another. Proliferators are known to pursue 'licence shopping' tactics to circumvent controls, so such information sharing is key. There are several issues that limit the effectiveness of the current denial notification process, particularly in the context of catchall controls and the burden associated with checking all licence applications against denial notifications. These issues include the limited nature of the technical description of the goods that is typically included in denial notifications, which makes it difficult to determine whether there is match. Nonetheless, the system appears to be broadly fit for the purpose for which it is intended. More could be done to share information with international authorities, however, including the IAEA and UN Panels of Experts mandated to monitor the implementation of UN sanctions resolutions (such as those on North Korea and Iran). The sharing of information on denial notifications and details of authorisations granted concerning states that are subject to UN sanctions with the relevant panel of experts is typically allowed for under UN sanctions resolutions and would allow the panel to better monitor implementation of the sanctions resolutions, for example.

As was mentioned above, more could be done to build common understanding of proliferation risks and methods among member states. The licensing enforcement meeting that was suggested would be one forum for this. However, this should be supplemented by encouraging states to share information.

Two further aspects of information sharing should also be considered. The first relates to entity watchlists.[2] The second relates to country risk charts. In both cases, the option exists under this regulation to maintain either as a public or as a private document. There are merits and detriments to both approaches. In relation to both entity watchlists and country risk charts, the question arises of how this would differ from EU or UN sanctions, which are similar in nature. This highlights the importance of having a coherent approach between EU export control and sanctions policies.

Entity watchlists: Regulation 428/2009 allows for the possibility of maintaining common 'watchlists' of entities of concern. However, it is understood that this ability is not currently utilised even though individual member states do utilise watchlists.

Consideration should be given to expanding the use of watchlists. As with country risk charts, providing a mechanism for sharing a common understanding of risk among member states could prove highly beneficial.

Country risk charts: certain countries – notably, the United States – formally publish country charts, consisting of lists of countries and the categories of goods that can be exported to them without a licence. For the United States, this provides a relatively straight forward method of pursuing a risk-based approach to licensing: if a potential recipient state is viewed as an end use or diversion risk, exporters will require a licence to exports good to that country, In the Community General Export Authorisations are available which may be considered compatible, but the scope of these CGEAs is less. Additionally, CGEAs only change, rather than remove, the administrative burden on companies, as authorisations are still required.[3]

There are evidently positive and negatives about making both or either watchlists and country risk charts public. Benefits include making it easier to communicate with potential exporters, the public and with third states. Difficulties relate to the diplomatic relations with the target country and the ability of proliferators to make more use of deceptive practices when under scrutiny. Additionally, listed entities can challenge their position on such lists meaning that there must be a solid legal foundation and systematic approach taken when creating such lists.

It should be borne in mind also that while EU member states are the main implementers of the regulation, it is also used as the main model for many other states. At present, there is no standing forum through which states that use the EU regulation or control list can discuss policy issues surrounding the regulation.[4]

---

[2] Specifically, article 19 (2) of 428/2009 requires states to take all appropriate measures establish direct cooperation and exchange of information between competent authorities with a view to enhance the efficiency of the Community control regime." where "such information may include…data on sensitive end users, actors involved in suspicious procurement activities, and, where available, routes taken."

[3] Authorisation for CGEAs typically requires "registration" and compliance with the stated conditions of a standard, published authorisation.

[4] There is no definitive list of countries that use the EU list, but countries that use the dual-use list are understood to include: Albenia, Bosnia & Herzegovina, FYROM, Montenegro, Serbia, Georgia, Moldova, Ukraine, Kazakhstan, Jordan, UAE, Malaysia, Phillipines, and Thailand.

2.5 Transparency

Beyond the question of whether information should be shared with countries outside the EU is the question of which information should be shared with the public and civil society. Presently, transparency is an issue for each member state, which results in considerable variance in the level of transparency across Europe. Some member countries, such as the UK, publish licensing statistics and related information, including information on the control status, value, and destination country. Most do not, however. This should be standardised.

The regulation also allows the Commission to issue non-binding guidance for exporters and brokers, including with regards to the interpretation of the regulation. Little of such guidance has been made public. In the absence of Commission guidance, other bodies have issued such guidelines, including the UN Security Council, the export control regimes and the Security Council's Resolution 1540 Committee. Academic and civil society organisations have also issued similar guidelines. The commission could benefit from issuing such guidelines in the future, including but not limited to:

• Compliance guidelines (i.e. what internal compliance measures should a company put in place to ensure compliance with export control requirements?)

• Competence frameworks (i.e. what types and level of training should staff involved with export controls have undertaken?).

As will be explored below, such guidance is necessary not only for brokers and exporters (those sectors traditionally affected by export controls) but also for shippers, financiers and insurers, all of whom share responsibility in export control.

Acting on behalf of Member States, the Commission should also centrally publish information on national implementation of the regulation to include the licensing agency and process, licence types and processing times, number and value of licences and enforcement actions. In addition to helping companies and informing civil society, this would also encourage standardised implementation across the EU.

3 Major National and Multilateral Control Regimes

The European Union is not the only implementer of export controls. Indeed, since 2004, all states have been required by UN Security Council Resolution 1540 to maintain a system of export controls to prevent the proliferation of WMD and 'related materials', which can be understood as 'dual-use' goods in the context of the regulation. (United Nations 2004) Resolution 1540 does not itself go into much detail about what this means in practice. Instead, this is the role of the four main export control regimes.

3.1 Export Control Regimes

Beyond the EU regulation, the primary rule-making mechanisms for export controls are the four main export control regimes: the Nuclear Suppliers Group, Wassenaar Arrangement, Missile Technology Control Regime, and the Australia Group. These regimes are voluntary mechanisms through which non-binding 'guidelines' are maintained. They operate by consensus.

Table 1. Purpose of Each Export Control Regime

Regime	Purpose	Relevant Treaty[5]
Nuclear Suppliers Group[6]	The Nuclear Suppliers Group (NSG) is a group of nuclear supplier countries that seeks to contribute to the non-proliferation of nuclear weapons through the implementation of two sets of guidelines for nuclear exports and nuclear-related exports. The NSG has 48 members.	Nuclear Non-proliferation Treaty
Missile Technology Control Regime[7]	The Missile Technology Control Regime (MTCR) is an informal and voluntary association of countries which share the goals of non-proliferation of unmanned delivery systems capable of delivering weapons of mass destruction, and which seek to coordinate national export licensing efforts aimed at preventing their proliferation. The MTCR has 34 members (known as 'partners').	N/A
Wassenaar Arrangement[8]	The Wassenaar Arrangement was established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. The arrangement was formed soon after the disbanding of the COCOM arrangement which controlled Western exports to the Soviet Bloc during the Cold War. The items included in the Wassenaar Arrangement's List of Dual Use Goods and Technologies, containing nine Categories and two Annexes ('sensitive' and 'very sensitive' items, respectively) and the Munitions List (WAML), containing 22 main entries on items designed for military use. It has 41 members.	Potentially the Arms Trade Treaty
Australia Group[9]	The Australia Group (AG) is an informal forum of countries which, through the harmonisation of export controls, seeks to ensure that exports do not contribute to the development of chemical or biological weapons. The Australia Group has 38 members, with the EU participating as an observer.	Chemical Weapons Convention. Biological and Toxic weapons Convention

The lists of the four export control regimes are integrated into the EU control list based on the structure shown in Figure 1 below, which itself is based on the control list structure of the Wassenaar Arrangement dual-use list. It is important that the EU fully reflect the lists of the export control regimes. Failing to reflect the regime lists can have two effects. First, if items are missing from the EU's list, there is a danger that the EU could become a weak link in the non-proliferation chain. Second, by controlling items not on

---

[5] Note: the export control regimes are separate from the international treaties, but can be relevant.
[6] See http://www.nuclearsuppliersgroup.org/en/
[7] See http://www.mtcr.info/english/
[8] http://www.wassenaar.org/
[9] See http://www.australiagroup.net/en/

the lists of the regimes, EU business could be disadvanted. There are real-world examples of both scenarios. The current regulation requires that the list be "in comformity" with the regime lists, although it should be noted that delays caused by the process related to the amendment of the list resulted in the EU list falling behind the regime lists.

Figure 1. Structure of EU Control List As Included in Regulation 428/2009
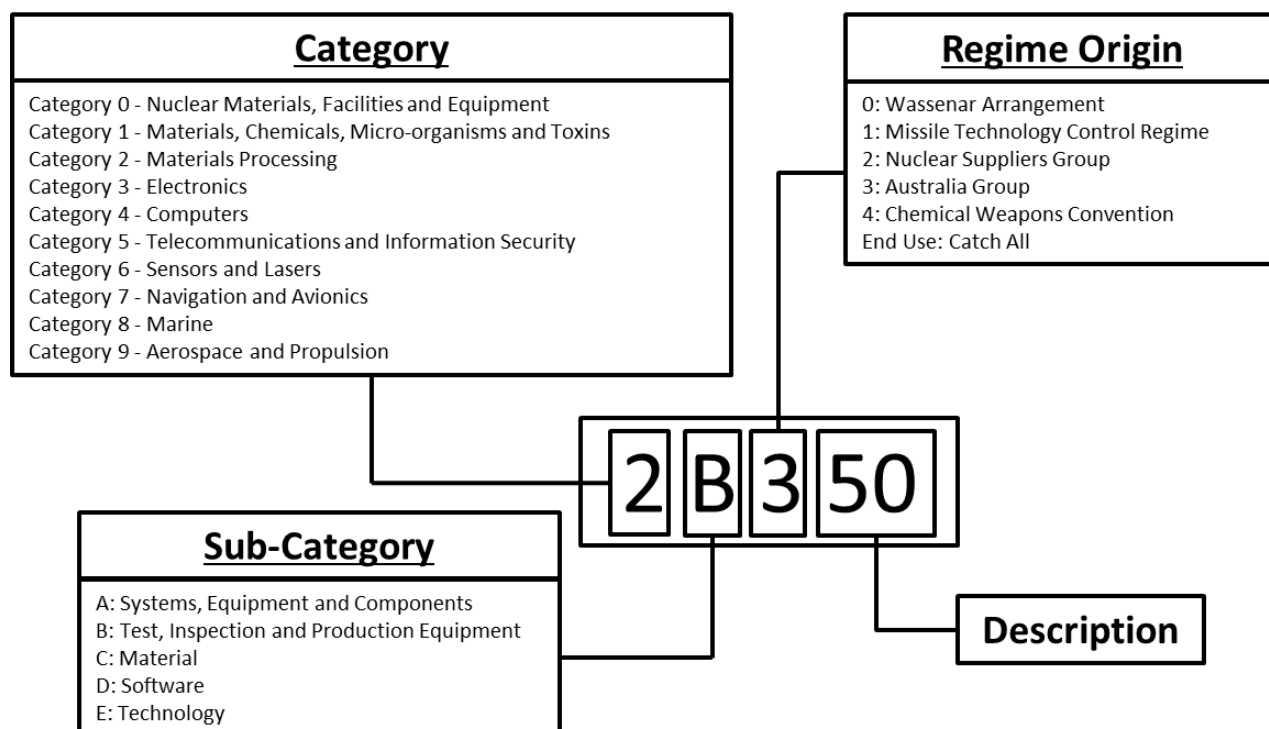
In some cases these regimes are directly complementary to the main international non-proliferation treaties, such as the Nuclear Non-Proliferation Treaty, Chemical Weapons Convention and Biological and Toxin Weapons Convention. These regimes produce two main outputs with relevance to the EU: the first is their control lists; the second is their criteria or guidance – the factors that determine when a licence will be exported. The lists are directly incorporated into the control list of the EU (which itself uses the structure of the Wassenaar Arrangement list and is in turn used by many non-EU states). In the absence of a single agreed EU licensing assessment criteria, the criteria and guidelines from these regimes is implemented directly by member states.

The export control regimes also play other functions. They are the forum at which possible additions to the control lists are discussed. They, together with forums such as the Proliferation Security Initiative are also the forums through which practitioners from each member country meet to share experience and information. (Presently, the Commission does not convene such forums for EU member states. The EU also does not formally participate in two of the four main export control regimes).

3.2   US Export Controls

When evaluating the EU export control system, the US provides perhaps a natural comparison. The commission noted in its communication to parliament on the review of the regulation that the US is currently undertaking a reform of its export control system. (European Commission 2014a) It was highlighted also that in some instances the US may be able to grant licences in a process that is better suited to the needs of industry than those used by most EU states.

The reality is more nuanced, however. The US is undertaking a system of export control reform, with an aim to result in a single control list, single IT system, single enforcement coordination capability and single licensing agency. In practice, it seems likely that while many goods will be transferred from the US munitions to the dual-use list (and hence become the responsibility of the Department of Commerce rather than the Department of State with its International Traffic in Arms Regulation 'ITAR' controls), little progress will be made on the other singularities. Even if the US was to achieve all such goals, it is not clear that the US system would be 'better' than that of the EU. Some EU member states already have a single agency and single list, for example. More generally, it is important to note that many of these issues are beyond the scope of the export control regulation: presently, it is for each member state to decide how to administer the export licencing process to best suit their government structure and industrial needs.

Another frequently expressed concern relates to the discretion the US government takes over the licensing process. In recent years, the US has adopted an expedited system for exporting items containing certain types of encryption and, as discussed further below, has lessened controls on semiconductor manufacturing equipment, largely as a result of a determination that the goods were being produced outside of the Wassenaar Arrangement.[10] The US Department of Energy can also grant certain types of licences for longer periods (such as the widely-discussed nuclear project licences). These are certainly areas where EU member states should be responsive, although it is worth noting that it is not necessarily clear that this must be through the regulation. Member states can, for example, grant licences for longer terms if they wish.

US Licensing Process for Dual-use Goods

In the U.S., the export of dual-use commodities, software or technology is regulated by the Bureau of Industry and Security (BIS) of the U.S. Department of Commerce. Such licenses are required in certain situations where national security, foreign policy, short-supply, nuclear non-proliferation, missile technology, chemical and biological weapons, regional stability, crime control, or terrorism are of concern.[11] An item's technical characteristics, as well as its destination, end-use, and the end-user, are all used to determine whether a dual-use export license is required. The product's Export Control Classification Number (ECCN) on the Commerce Control List (CCL) identifies reasons for control which indicate licensing requirements to certain destinations. However, an item may fall under U.S. Department of Commerce jurisdiction and not be listed on the CCL – in this case, it will be designated as EAR99. EAR99 items generally consist of low-technology or consumer goods and do not require a license unless the proposed export is to an embargoed country, to an end-user of concern or in support of a prohibited end-use. Exporters are generally prohibited from doing business with persons or entities if they are listed on any of the following: Denied Persons List, Unverified List, Entity List, Specially Designated Nationals List and/or Debarred List. License applications in the U.S. are processed under an online electronic licensing system called the Simplified Network Application Process - Redesign (SNAPR).[12]

Certain encryption technology is eligible for export under License Exception ENC, which authorises export and re-export of certain systems, equipment, commodities and components as well as related software and technology. (It does not authorise the export or re-export to, or provision of any service to Cuba, Iran, North Korea, Sudan, and Syria.)

A manufacturer/exporter must complete an encryption registration process, which takes the form of a prescribed set of information about the manufacturer/exporter and the items with which it deals, after which it is submitted to the Bureau of Industry and Security. Once this has been completed the firm is

---

[10] See https://www.bis.doc.gov/index.php/policy-guidance/encryption
[11] http://www.export.gov/regulation/eg_main_018219.asp
[12] See https://www.bis.doc.gov/index.php/licensing/simplified-network-application-process-redesign-snap-r

authorised to export the eligible goods (those classified under ECCNs 5A002 a.1,2,5,6, and 9 or b. ECCN 5B002, and equivalent software and technology classified under 5D002 and 5E002) to eligible "private-sector" end-users (an individual or firm not acting on behalf of or owned or controlled by a foreign government). The manufacturer/exporter must also either submit a self-classification report on the products it is to export or allow BIS classify them. (United States Government Publishing Office)

US Export Control Reform

In the U.S., Export Control Reform (ECR) denotes an initiative launched by President Obama in 2009 with the intention to modernise the country's export control system. By that time, the U.S. Munitions List (USML) administered by the Department of State's Directorate of Defense Trade Control (DDTC) and the Commerce Control List administered by the Department of Commerce's Bureau of Industry and Security (BIS) had not been updated since the early 1990s. The purpose of this comprehensive review was to protect America's most sensitive defence technologies and to address threats inherent to the rapidly changing technological and economic landscape of the 21st century. The initiative overhauls the Cold War-era system of regulations on exports of controlled technologies.

The ECR aims to transfer tens of thousands of less sensitive military items from the State Department's jurisdiction to the more flexible Commerce Department regulations and establishes new criteria for determining which items need to be controlled based on a three-tier construct. This will include a "catch all" control for sanctioned end-users and destinations, proscribed entities, proliferation and counterterrorism end-uses. Furthermore, the ECR requires that a coordinated set of policies for determining when an export license is required be implemented. The ECR process has been structured for implementation in three phases:

> Phase I. Develop methodology for rebuilding control lists. STATUS: Phase I completed in 2010;

> Phase II. Apply methodology, reconcile various definitions, regulations, and policies restructuring the USML and CCL into identical tiered and positive lists. STATUS: PENDING;

> Phase III. Create a single control list, single licensing agency, unified information technology system, and enforcement coordination centre. STATUS: PENDING (contingent on completion of Phase II as well as Congressional legislation).

While these changes will go some way to making the US more competitive in terms of export control implementation, in reality these changes will bring the US in line with how most EU states implement controls. The overall EU implementation of export controls is of course more complex because of the split in competence between the European Union and Member States.

A particular aspect of the US review could be relevant to the EU review. The US is transferring some military-list items to its dual-use list, with a corresponding switch in administrative oversight and process. Consideration should be given to whether it would be advantageous to mirror this in the EU. This would be complex because presently controls on military goods are a matter for member states.

3.3   Export Controls in Other Countries

The remainder of the world can roughly be subdivided into two categories when it comes to export controls: countries that are members of the main export control regimes and countries that are not. Countries in the first category include the majority of the manufacturers of high-tech goods. These countries are bound by the same international commitments as the EU, though implementation does vary.

The second group of countries primarily includes states that are not members of the export control regimes. By and large, these countries are not manufacturers of dual-use goods. Some of these states can

still become involved in proliferation, although the risk is primarily from transit and transhipment of goods made elsewhere rather than from the export of domestically manufactured goods. These states are bound to implement export controls, including transit, transhipment and reexport controls, by resolution 1540, and some states are making substantial progress towards improving implementation, such as Malaysia and the UAE.

There are three main exceptions to the above generalities. These concern China, India, and the Eastern and South East European States.

China, which is rapidly becoming a substantial producer of dual-use goods is only a member of one of the four export control regimes (the NSG) to date. Export control implementation in China is often said to be lacking, although the reality is somewhat more nuanced. China has in recent years taken some important steps toward strengthening its implementation of export controls, including creating a new licensing agency. A new law may also be adopted in the coming years.(Stewart, I, 2015b) From a European perspective, it is important that Chinese implementation of non-proliferation controls does improve given the country's market significance to the European Union. However, at the same time, it should also be recognised that there are proliferation risks and challenges with the country, as discussed below.

India is another example substantial producer of dual-use goods that is not yet a member of the four export control regimes. After the NSG passed an exemption to supply goods to India, the country has become increasingly sympathetic to the international export control regimes, and India recently applied to join the MTCR as its first step in joining all four of the regimes. Its system of control appears to be in keeping with international standards, although it has not yet harmonised its control lists with that of the export control regimes. (Nayan, R., Stewart, I.)

Eastern and South-East European States, many of which are either members of the European Union or are candidates for membership, are generally only modest producers and shipment points for EU-manufactured products. The level of export control implementation is considered variable. The membership of the export control regimes also varies between these countries. In part, this is a result of the politics of the export control regimes, which are beyond the control of the European Union. Nonetheless, an effort should be undertaken to ensure that EU member states are members of the export control regimes and, importantly, that a plan is in place for any countries that join the European Union in the future.

4 Current Security Needs and Challenges

The purpose of export controls is loosely to prevent proliferation and to protect national security. More specific definitions of the purpose of export controls could be taken from each of the export control regimes and are shown in Table 1 above. The EU could also set its own definition for the purpose of export control, although any such definitions should be linked through to broader EU strategies, such as the WMD strategy. Perhaps the two key security needs and challenges of the dual-use regulation relate to the proliferation of WMD and human security.

4.1 Non-proliferation

The current regulation provides a solid foundation through which EU states can meet their non-proliferation commitments.

There are aspects of the regulation that could be improved or clarified in order for the regulation to best contribute to non-proliferation. This could relate to reviewing how NSG trigger list items are incorporated into the EU control list and clarifying the definition of WMD. On the question of the definition of WMD,

consideration should be given to the question of whether exports to unsafeguarded nuclear facilities would constitute proliferation.

In theory, at least, an updated relation could allow the EU to go further and be a leader in terms of non-proliferation. This could manifest itself, for example, in a council decision not to export enrichment and reprocessing capabilities to countries that have not implemented the IAEA's Additional Protocol (or indeed, to any country that does not already have the capability). This would be in keeping with the EU's sponsorship of the IAEA's Fuel Bank. However, in reality, such decisions would have substantial political and diplomatic consequences and could infringe on national sovereignty. This thus highlights the importance of linking export control with broader strategies, such as the EU's WMD strategy.

4.2 Human Security

It is notable that certain important issues such as human security considerations do not fit within the purpose of the existing regimes, with the possible exception of the Wassenaar Arrangement, which can be considered somewhat as a 'multi-purpose' regime. Therefore, when factoring in such issues, a decision must be taken about whether to broaden the purpose of one of the existing regimes or create a new regime. If the latter option is pursued, the question arises of whether this should be an EU-only mechanism or whether it should include likeminded states, which would in effect make it the fifth main export control regime. Such an EU-only approach, if pursued, should be linked to appropriate EU strategies instead of being adhoc in nature (i.e. an EU strategy on promoting human rights).

It should also be borne in mind that it is for national governments (Member States, in cases of the EU) to decide on specific bases to issue or refuse an export licence. The current regulation advises states on what factors to take into account when considering licences, but there is no common assessment criteria and no common risk assessment.[13]

Another issue that should be considered relates to end use controls. The current regulation includes two end use controls – a WMD end use control and a military end use control. However, the WMD end use control is much broader in scope than the military end use control. Consideration should be given to broadening the military end use control to control exports when the exporter knows or has been informed that the goods will be used for human rights violations, paramilitary activites or terrorism.

5 Technological and Scientific Evolution

There is an ever-present risk that some new technology will emerge that could cause mass destruction, aid proliferation, or otherwise undermine the existing controls. It is thus necessary to monitor the evolution of technology and to consider potential application to proliferation. Presently, it is the export control regimes that are chiefly responsible for this activity, although there are no reasons that the EU could not supplement the regime lists with a list of its own as the US does.

While most EU member states are represented at these consensus-driven regimes, the European Unionas an entity is under-represented. The European Commission participates as an observer in two of the four export control regimes.[14]

---

[13] Art 12 of 428/2009 requires that Member States take into account "all relevant considerations including Council Common Position2008/944/CFSP". However this is not the same as having a single defined assessment criteria.
[14] Note: The communication proposes that the European Union should push for inclusion in the other export control regimes. While logical, it should be noted that this would require support of all participants in each export control regime.

The Commission proposed in its Communication to Parliament that a technical reaction capacity be created that explores the implications of emerging technologies even beyond the work undertaken by the export control regimes. (European Commission 2014a) Given that not all EU member states can be expected to have access to technical experts for each technology that could be discussed at the export control regime, this seems sensible. Additionally, the European Union could take actions outside the export control regime where it deemed that risks warrant doing so, but it should be recognised that this would impose additional burdens on EU industry compared to competitors in non-EU regime participating states. In this context, the types of issue that this capacity could be asked to explore include the following:

- Additive manufacturing (3D printing) capabilities, which have the potential to fundamentally change the nature of existing supply chains. The technology could thus have implications for the effectiveness of controls which should be understood.

- Nano-technology, for which the proliferation implications are not yet understood.

- Intangible technology and cloud computing, through which vast amounts of data can be rapidly transferred.

Another set of risks relates to the nature of proliferation. Given the relatively limited manufacturing base for proliferation-sensitive goods (see image three below), proliferation tends to involve dynamic efforts to acquire goods from a relatively small number of manufacturers. It is worth noting that the technology sought by proliferators as well as the methods and techniques used by proliferators to evade controls have largely remained consistent for many decades, although the specific entities and countries involved in proliferation have varied.[15]

One implication of this relates to the need to integrate non-proliferation and export control principles into the supply chain. There have been examples of overseas subsidiaries of multinational firms becoming complicit in proliferation by falsifying end-use paperwork that was sent back to the parent company. (Stewart, I., 2014) The development of robust supply chains is complicated by the nature of export controls and the structure of the international system: bureaucracies exist in states to implement export controls, but invariably these organisations focus on licensing. It is thus appropriate in the context of the review to consider what measures could be taken to systematise supply-chain non-proliferation principles, including through the provision of guidance on supply-chain security such as that adopted by the Nuclear Suppliers Group, and the integration of export compliance with supply-chain compliance measures perhaps as a condition of use of general licences and supply-chain mechanisms, such as the Authorised Economic Operator framework as explored in part two of this report.

6   Main Targets of the Controls

Export controls affect goods, technology and software. It is helpful in the context of the review to consider how export controls affects exports in each of these categories.

6.1   Goods

EU export controls directly regulate the goods specified in the four main export control regimes and the non-proliferation treaties. This results in a substantial list of goods being subject to control. A review of

---

[15] One exception relates to cyber intrusion, through which sensitive technology transfer is believed to have taken place.

the control list shows that there are as many as 3000 specific entries on the control list, which is 2.5 cm thick when printed out in full.

The catchall principle[16] extends the coverage of control to a theoretically unlimited number of additional technologies, although in practice the authors' experience suggests that the use of catchall controls typically relates to goods of conceivable utility in nuclear or missile programmes.[17]

While specific figures are not available, a study undertaken by the author placed the value of dual-use production between €26.43bn and €37.23bn. (Stewart, I,. 2015a) Other studies have placed the value higher. The value for exports of EU-produced goods will be significantly below the value of production. However, it should be borne in mind that EU exports of dual-use goods include items that were produced elsewhere (i.e re-export). Figures from the Commission's annual report on export control are shown in Figure 2 below. (European Commission 2015)

Figure 2. Controlled Trade Value. (European Commission, 2015)
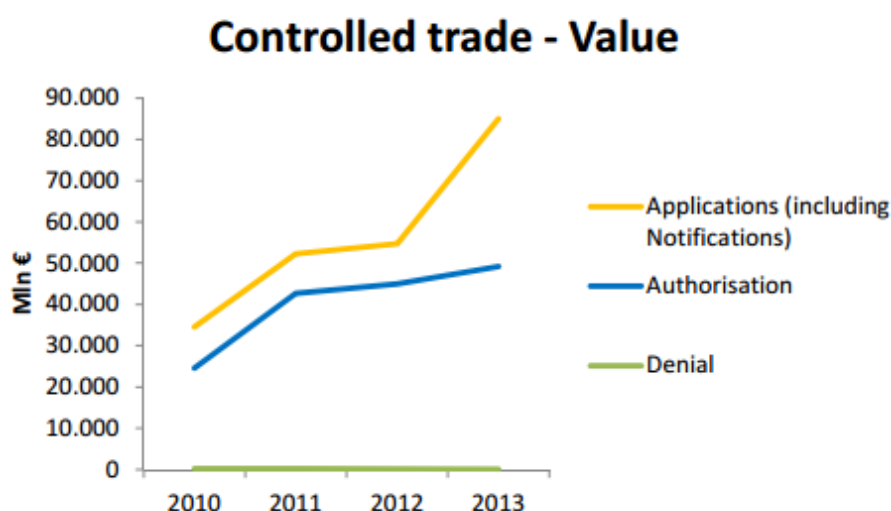
Beyond the specific figures, which will be returned to below, it is clear that the European Union is a substantial producer of dual-use goods. This can be seen graphically in Figure 3 below, which is a snapshot of the locations of the headquarters of 25 of the most sensitive dual-use goods.

---

[16] "catch-all… permits the control of items not listed on the EU Control List… and is a valuable tool providing the authorities with ability to respond swiftly to the evolution of proliferation risks by applying greater scrutiny and, where necessary, preventing transactions of concern." http://trade.ec.europa.eu/doclib/docs/2013/february/tradoc_150459.pdf

[17] The author was responsible for assessing the proliferation risks associated with dual-use applications in the UK in the time period 2009-2011.

Figure 3. Headquarters of firms manufacturing around thiry especially proliferation-sensitive technologies.

The sheer size of the control list creates challenges for EU member states, as states are responsible for ensuring that their industry knows and is compliant with the regulations. The number of sectors affected makes this a challenging endeavour, one further complicated by the existence of open or general licences, as producers must know the status of their goods if they are to comply.

In terms of the numbers and types of control, it is the Wassennaar Arrangement that is responsible for many of the specific control entries (65% of the total), as Figure 4 demonstrates.

Figure 4. Breakdown of EU Control List by Regime
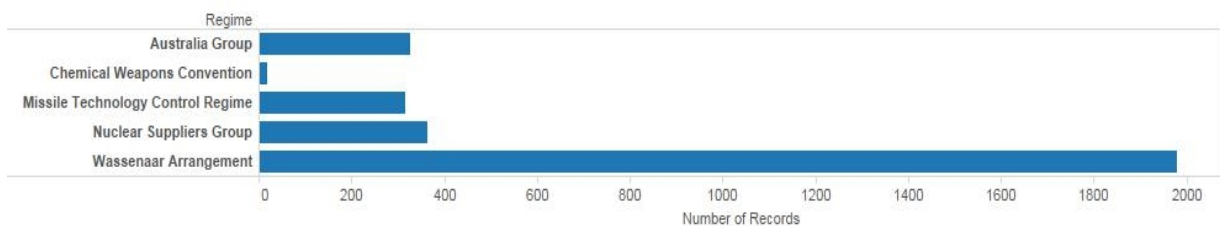
An unpublished review of UK single individual export licence value over six years conducted by the author also suggests that Wassenaar Arrangement is responsible for the majority of controlled exports by value, although it is not necessarily the case that the results of this UK-centric study can be assumed in other EU states. The UK study specifically suggests that, as shown in Figure 5, Category 5 goods account for the majority of the value of production, with Category 5 accounting for more than 66% of SIEL applications over the period 2008-2014.

Figure 5. Breakdown of UK Individual Export Licence Applications (2008-2014) By Category, and Year
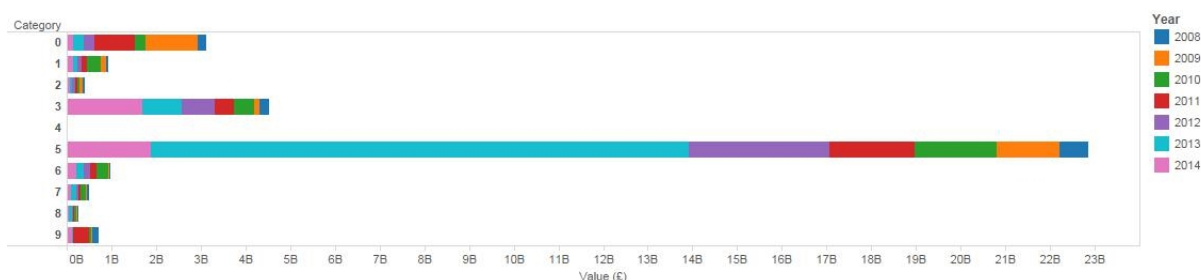
A separate study (summarised in Figure 6 below), sought to use data that is available for all EU member states (PRODCOM data which is collected under Council Regulation 3924/91) found that the space (which dominates the category "manufacture of other transport equipment"), nuclear and machine tool sectors were collectively the largest producers of dual-use goods in Europe, although again there are numerous caveats with this study. (Project Alpha, 2015)

Figure 6. Estimated Production of Dual-use Goods by NACE Code
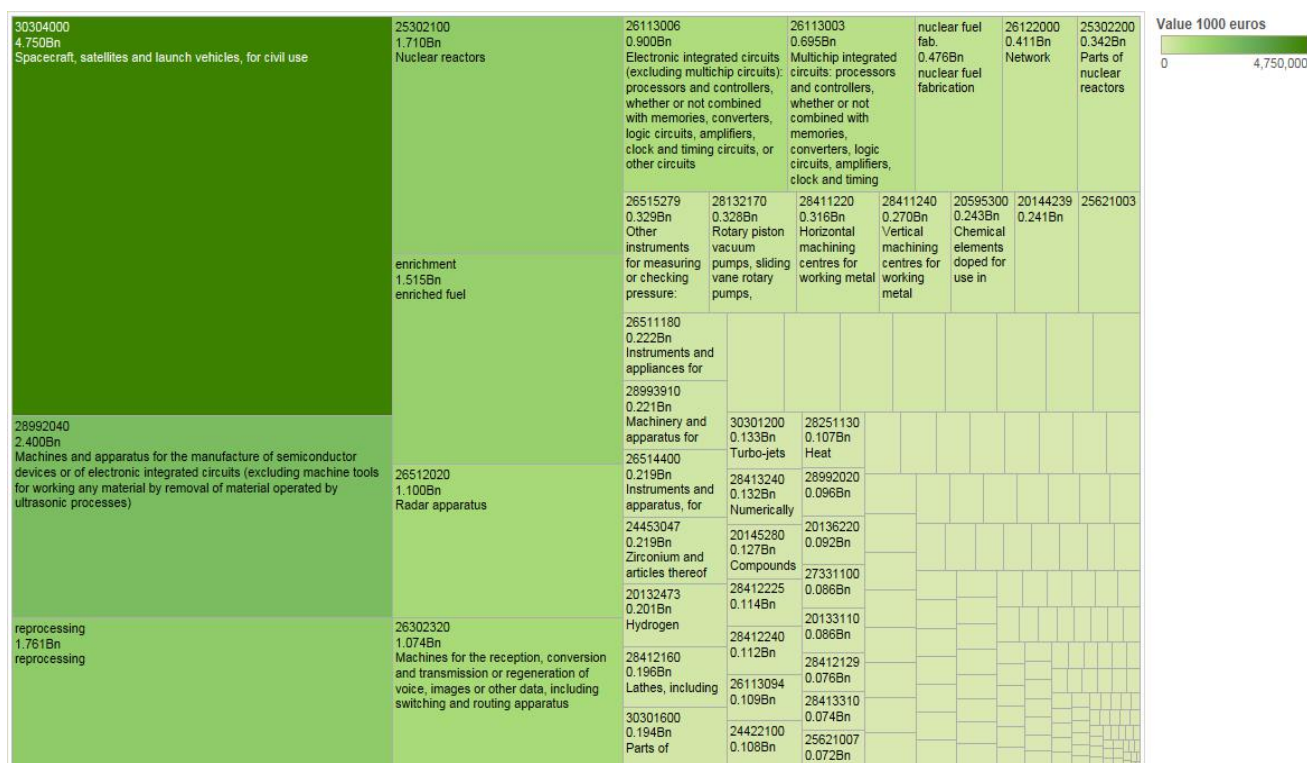
It should be noted that there are important caveats with the method employed in this study which means that it likely undervalues some sectors and overvalues others. Indeed, no methodology has so far been identified that can provide an accurate picture of the production of dual-use goods within the European Union.

6.2 Software and Technology

The controls cover not only physical goods, but also software and technology. The definition of 'export' provided in Regulation 428/2009 includes technology and software:

> *Export shall mean… transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and partnerships outside the Community. Export also applies to oral transmission of technology when the technology is described over the telephone;*

> *where*

> *"technology" means specific 'information' necessary for the "development", "production" or "use" of goods or "software"; Technical Note: 'Information' may take forms including, not limited to: blueprints, plans, diagrams, models, formulae, tables, 'source code', engineering designs and specifications, manuals and instructions written or recorded on other media or devices (e.g., disk, tape, read-only memories); 'source code' (or source language) is a convenient expression of one or more processes which may be turned by a programming system into equipment executable.*

Technology is not controlled when it is in the public domain or the information comprises basic scientific research, defined as:

> *"In the public domain" (GTN NTN GSN), as it applies herein, means "technology" or "software" which has been made available without restrictions upon its further dissemination (copyright restrictions do not remove "technology" or "software" from being "in the public domain").*

> *"Basic scientific research" means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.*

In practice this definition would mean that a blueprint associated with a controlled missile would itself be controlled unless it was in the public domain.

One challenge with these definitions is in determining what falls within and what is outside the scope of controls. It is perhaps unlikely that research on missile design could be described as "basic scientific research". However, it is foreseeable that research into structural materials for use in high-stress environments could be defined either as basic or applied research depending on intended end use.

It is difficult to quantify the importance of software and technology. When viewed graphically as in Figure 7 below, the number of control entries related to software and technology appears relatively low. However, a single technology control entry will often apply to a number of control entries for physical goods, which may result in an under-representation of their significance.

Figure 7: Breakdown of EU Control List by Sub-Category
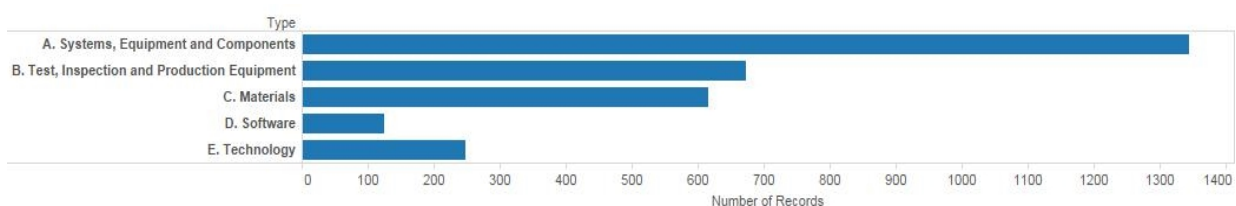
It is difficult to precisely identify the value of software and technology from controlled goods. Using data from the UK study mentioned above, software and technology could form up to around 5% of the value, as shown in Figure 8 below, although there is some possibility of double counting in this number due to the way the information is compiled. Regardless, the value of software and technology is significant.

Figure 8: Breakdown of UK SIEL data (2008-2014) by Sub-control Entry
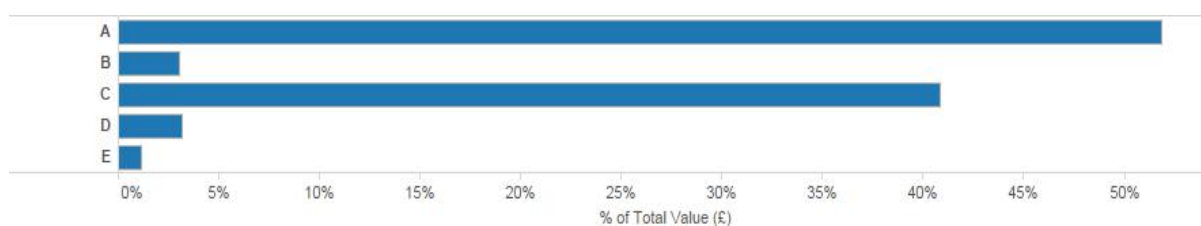
There is also clearly an intangible value to technology that cannot be quantified: the exchange of information and ideas is central to the innovation process. It is in this context that concern is often expressed about how intangible technology controls affect universities in particular.

6.3   Proliferation Risks

The control of goods through Regulation 428/2009 is a means, not an end. The ultimate purpose of export controls is to prevent the use of EU-origin items in ways that would be contrary to EU national security, foreign policy, or international commitments. It is notable that no single list of the risks that EU controls are intended to counter can easily be referred to: presently, Regulation 428/2009 allows for states to decide which criteria to utilise when assessing individual export licences, although the regulation does refer to 2008/944/CFSP of 8 December 2008 as one of the relevant considerations that should be taken into account.

Again, there is a lack of EU-wide data available in the public domain related to how states use export controls, with the UK being one of the only countries that systematically publishes statistics on licence refusals. Examination of the UK data can provide some insights into the use of export controls within Europe, although the UK's use of the controls likely differs substantially from other states. Nonetheless, it is notable that UK licence refusals are, as shown in figure 8, highly concentrated on a small number of countries where sanctions and restrictive measures are often also (or were) in place.

Three countries that stand out as particularly problematic for the UK licensing authorities are Iran, China and India. In order to understand why that is, it is important to consider the historical and legislative factors that have shaped trade relations between these countries in the past decades. (India also features prominently as a destination of repeated export licence denials, although less so in recent years.)

UK licence refusals in the period 2006-2014

Figure 9 below shows UK export licence refusals over the period 2006-2014. The data are derived from the Export Control Organisation's Licence Statistics website, which perhaps provides the most concrete data on export licence data available in any country in the world. The chart also shows countries against which the EU and/or UK has sanctions and restrictive measures.

It is notable that licence refusals appear to be concentrated in those countries that are also targets of sanctions or restrictive measures. While a correlation between the two datasets may seem intrinsically correct, it is notable that export controls and sanctions are viewed at the EU level as being distinct instruments with a separate legal basis.

It is notable that most refusals related to the use of the catchall control or to goods controlled under the Wassenaar Arrangement, whereas refusals of goods controlled by the other export control regimes (Nuclear Suppliers Group, Missile Technology Control Regime, Australia Group, and Chemical Weapons Convention, etc) are comparatively few.

Figure. 9: Visualisation of UK Export Licence Refusals By Country (2006-2014)[18]
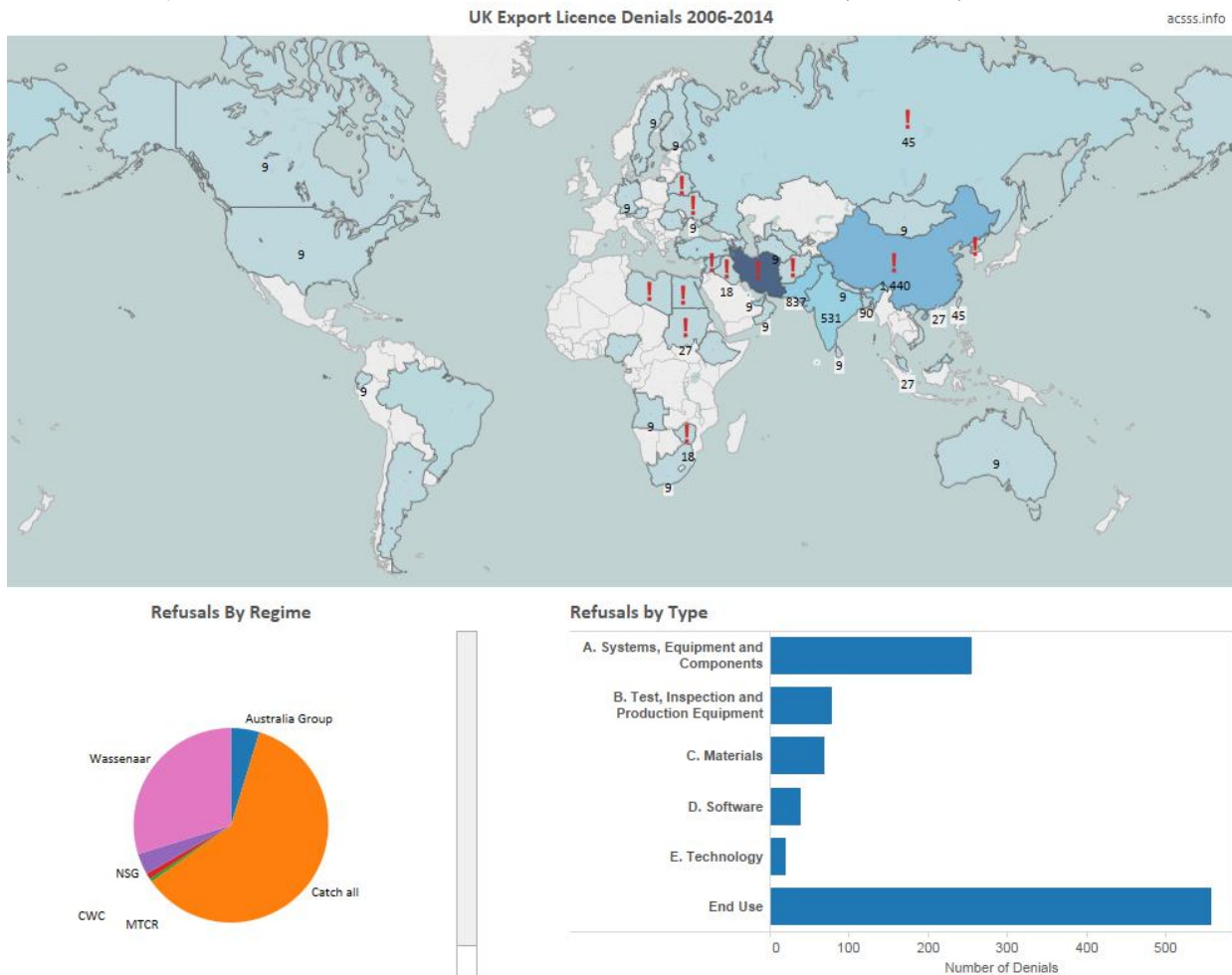
Given the concentration of refusals to a small number of countries, it is worth considering why this might be the case:

Iran: Iran has faced international isolation since the overthrow of the Shah in 1979, but it has only been since the mid-2000s that Iran has been subject to a wide range of international sanctions. EU sanctions expanded in 2010 to encompass the oil, gas, petrochemical, insurance, reinsurance, banking and shipping sectors. In 2006, the UN Security Council passed Resolution 1696, imposing additional sanctions on Iran after it refused to curb its uranium enrichment programme, which Western countries feared would lead to Tehran developing the capability to produce nuclear weapons. These so-called targeted UN sanctions were augmented by a multitude of other non-UN-mandated sanctions against Iran, including a total EU embargo on Iran's oil sector and a freeze of assets of Iran's Central Bank since 2012.

Iran has been notoriously apt at circumventing these sanctions, leaving licensing countries such as the UK concerned about its intentions regarding exports of sensitive and dual-use products and technologies. As a direct result of this, it follows that Iran should be the country with the most export license denials between 2006 and 2011.

China: China is one of the countries counting the most export license denials, as it is currently still subject to a partial EU arms embargo. As such, it should come as no surprise that a total of 124 export licenses destined for end-use in China were denied by the UK government between 2006 and 2011.

---

[18] Note: this graphic is available in interactive form at http://www.acsss.info/visualisations.

India: Examination of the map reveals a substantial number of refusals to India. However, reviewing India by year reveals also that the numbers of refused licences has declined steadily over the period of study. India was subject to broad sanctions after its nuclear test in the 1990s. The high number and changing pattern is likely a result of the US nuclear deal with India and gradual reengagement with the country by the West following its nuclear test-based estrangement.

Proliferation Trends and Europe

It could be expected because of the size of production of dual-use goods within Europe that European companies would be targeted by proliferators. In fact, there is a long history for this dating back at least until the 1970s. Figure 10 is a dataset assembled by Project Alpha at King's College London in relation to attempted and actual procurement for Iran's nuclear programme. The first image shows the origin of the goods. The second shows countries involved in transit, transhipment or reexport.[19] It is notable that, if grouped together, EU member states would account for among the largest number in both cases.

Figure 10 – Points of origin and diversion for Iranian nuclear procurements
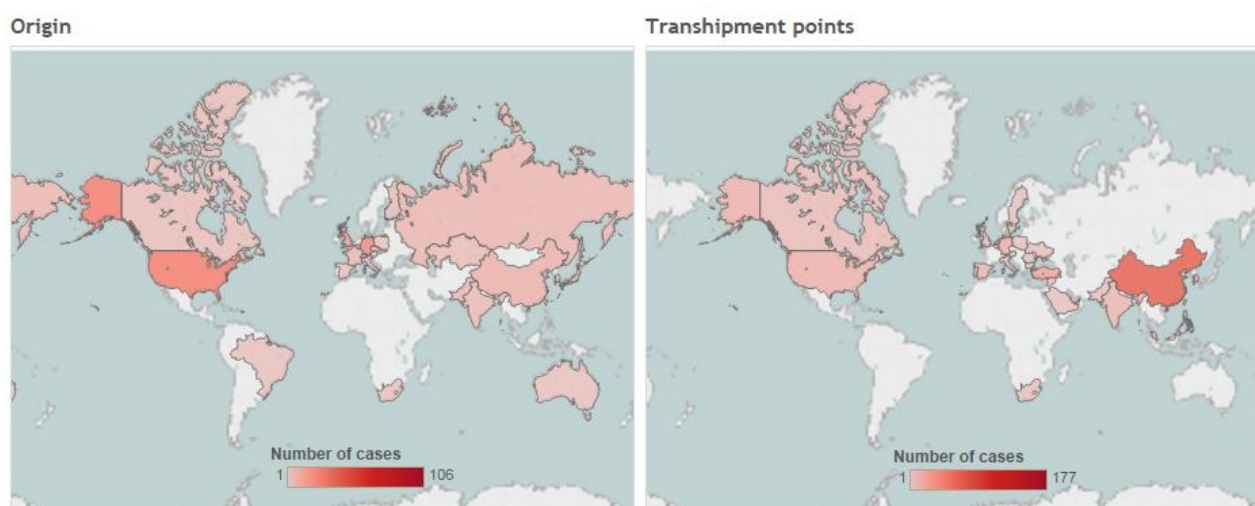
It can be expected that all states will have some cases of non-compliance and that it is inevitable that some goods will reach programmes of concern. There are also some methodological limitations of any study into illicit trade precisely because the trade is clandestine by nature. One important limitation is that it could be those states that are most proactive in stopping and prosecuting cases that come to the fore in such studies, notably given that they are largely assembled from publicly available information which include court cases.

Nonetheless, when combined with data on the states that have conducted a prosecution or related enforcement action, the inferences of the data in these graphics are cause for concern.[20] EU states are being targeted and there are signs that implementation and enforcement action varies depending on the state.

---

[19] There is little sign of European-origin goods being exported directly to end uses of concern. Instead, the proliferation risk tends to relate to transhipment of goods through at least one country.

[20] Note: there is no single dataset that records all prosecutions. Project Alpha at KCL has sought to develop such a dataset from open source information, although there are challenges in doing so as legal settlements can be reached in some states on the condition of anonymity. This issue should be considered as part of the review. See www.acsss.info/visualisations for a visualisation of KCL findings. For a discussion prosecutions related to dual-use goods in Europe, see: See Bauer, S,. "WMD-related Dual-use Trade Control Offences in the European Union: Penalties and Prosecutions", EU Non-proliferation Consortium, Non-proliferation Papers, No. 30, July 2013

6.4　　Cyber Tools and Surveillance Technologies

In recent years, there has been a rise in the availability of off-the-shelf surveillance technology that could provide governments with the capabilities to intercept substantial amounts of private information even if encrypted.

Exports of such cyber-technologies have remained relatively free from regulation or scrutiny to date. However, in 2013, changes to the Wassenaar Arrangement adopted controls on specialist software that can communicate and control intrusion software. This initiative has found some international support, particularly among policymakers and privacy advocates concerned with keeping network surveillance tools out of the hands of repressive or totalitarian regimes. However, the measures have also caused considerable alarm among security researchers, some of whom charge that the controls could make the internet less safe. (Google)

The European Union adopted these changes in October 2014. In May 2015, the U.S. Bureau of Industry and Security (BIS) proposed to implement the same provision of the Wassenaar Arrangement with regard to cyber intrusion and surveillance. BIS also proposes to add the definition of "intrusion software" to the definition section of the EAR pursuant to the WA 2013 agreements.

Some believe that the Wassenaar Arrangement has not yet gone far enough and that other technologies should be subject to control. There is also a view that the EU should create its own list of such technologies in pursuit of human security interests, even though this would mean that other producers did not enact the same degree of control. It seems sensible to first put proposals to the Wassenaar Arrangement in the first instance and consider EU-only controls if these proposals are not accepted. In the context of the review, consideration should be given to providing the Commission with the means to enact such additional controls if it proves necessary.

7　　Effects of Globalisation

There is a general assumption that the forces of globalisation lessen the effectiveness of national (or community) export controls. In the context of the review, the question arises of whether this is the case and what the implications may entail, if so. Aspects of these questions can be addressed drawing upon existing research. However, there is a need for the Commission to continue to study each of these factors in order to inform the implementation of the resolution. The technical reaction capability proposed by the Commission would be a suitable mechanism through which to fulfil this requirement provided that it was suitably resourced.

7.1　　Changing Manufacturing Base

Overall, the manufacturing base for the items examined in this study is expected to remain relatively stable. All items are well-developed technologies and all are produced in mature industries, meaning that from an economic perspective, rapid growth is unlikely. Still, evidence of business activity seen in the course of a study conducted by King's College London and summarised in Table 2 below suggests that the market is expanding slightly in a number of areas.

Table 2. Growth or contraction in the manufacturing base of 'chokepoint' technologies (Project Alpha 2014)

	All Primary Manufacturers	EU Primary Manufactures	All Secondary Manufacturers	EU Secondary
Bellows-sealed valves	59	18	87 (32 EU)	32
Beryllium	22	1	-	
Carbon fibre	14	1	-	
Calcium	25	1		
Controlled-atmosphere furnaces	48	8	-	
Flash x-rays	6	2		
Flow-formers	11	3		
Frequency inverters	38	20	75	53
High-strength aluminium	13	3	~2,400	Unknown
High-speed cameras	13	4	-	
Heavy water	6	1	-	
Maraging steel	21	10	8	0
Mass spectrometers	8	3	42	17
Pressure transducers	12 (5 EU)		-	
Radiation-shielded windows	38 (5 EU)		-	
Reactor pressure vessels	33 (8 EU)		64 (9 EU)	
Remote manipulators	17 (7 EU)		-	
Triggered spark gaps	11 (3 EU)		-	
Vacuum pumps	18 (9 EU)		-	
Zirconium	14 (1 EU)		40 (8 EU)	

Where expansion is occurring, it is spiking most noticeably in China. Already, Chinese manufacturers produce many of the items reviewed by King's College London; by the end of the decade, they will probably produce most of them. (Project Alpha 2014) For some proliferation-sensitive goods that Chinese companies have yet to produce, these firms already make lesser-quality versions and are actively working towards producing nuclear-suitable types. Carbon fibre provides a good example: no Chinese firm yet produces high-strength carbon fibre suitable for use in making gas centrifuge rotors, but several existing Chinese carbon fibre makers have announced their intention to produce the higher-quality material. (Project Alpha 2014) The technological leap required to make this material is substantial, but by no means insurmountable. In fact, the key barrier to indigenous production of controlled goods is often tacit knowedge, which is not subject to control. Similar advancements by Chinese companies into technologies like corrosion-resistant vacuum pumps should also be expected.

For some items, contractions in the size of the manufacturing base can already be seen, with further shrinkage likely. For example, the number of aluminium producers worldwide has dropped in the last decade due to multinational takeovers and a reduction in Chinese smelting capability, and there is evidence to show it may fall further. Heavy water, too, has a shrinking number of suppliers due to a decline in the popularity of heavy water-moderated reactor designs.

Unanticipated technological leaps in uranium enrichment or other processes involved in producing fissile material or nuclear weapons may change this picture, as might the disclosure of currently classified information relating to proliferation-sensitive technologies. For example, key technological aspects of the commercially-successful SILEX laser isotopic separation process remain classified by the US government, and their leakage (or recreation by other scientists) could drive a proliferation surge in niche laser-related items, perhaps including items not currently controlled by multilateral regimes. National and international authorities will need to monitor these developments closely.

Foreign availability

The Wassenaar Arrangement includes a foreign availability clause in the criteria that is used to determine what technologies should be subject to control. This indicates that technologies could be decontrolled should the manufacturing base spread.

In recent months, the US Department of Commerce has ruled that foreign availability exists for certain semiconductor manufacturing equipment (specifically, anisotropic plasma dry etching equipment and related software and technology) that has been controlled by the Wassenaar Arrangement. The practical effect of this ruling was that the US licensing agency moved to introduce more relaxed licensing requirements for the technology and to press the Wassenaar Arrangement to decontrol the item. (Department of Commerce)

It should be noted that the foreign availability criteria is unique to the Wassenaar Arrangement. Conceptually, such a criteria would seem to be incompatible with the goals of the Nuclear Suppliers Group, for example. Instead, the goal of the other regimes should be to ensure that other producing states adhere to the guidelines of the regime even if they do not actually join the regime itself. The EU should thus promote adherence through its outreach program and through policy instruments.

7.2   Service Providers

Finance, (re)-insurance, transportation and shipping

Regulation 428/2009 focuses on exporters and brokers. In recent years, the role of other service sectors in export compliance has been increasingly recognised. This has primarily been a result of actions to implement UN, EU and unilateral sanctions measures. However, the changing expectations on service providers in terms of sanctions means that they should also be viewed as important actors in relation to the review of the export control regulation.

In a globalising world, this is particularly important. It is increasingly these service providers – rather than manufacturers – that have visibility of the movement of goods and end users of products. Service sector firms typically collect information that can be used for trade compliance purposes, but this is presently not systematically utilised for non-proliferation purposes. In this context, the regulation should focus on setting expectations around the role of service providers in export compliance. This could include:

- Systematically checking transactions in which entities known to be involved in proliferation are not involved;

- Screen transaction information against a list of keywords associated with the EU control list to prompt the exporter to demonstrate that any required licence has been granted. (A weaker version of this could be to ask the client to confirm that all required export licences have been granted.)

Separate work should be undertaken by the Commission around the expectation of export control implementation among the service sectors. This should include consideration of whether EU member states should appoint competent authorities for each service sector.

Consideration should also be given to issuing as guidance the document "Sanctions compliance for the maritime transportation sector", which was published as an official document of the UN Security Council in early 2015. (United Nations 2015)

7.2.1 Supply-chain issues and E-commerce

Trading via the internet – or e-commerce – has expanded substantially in recent years, leading to questions about the implication of this expansion for traditional export controls. Distinct from other service sectors, e-commerce refers to the use of internet platforms to connect customers and suppliers (i.e. Alibaba and Ebay) and the sale of goods to consumers from stock (i.e. Amazon). Firms operating in this second category could be based entirely online or could have an online aspect of their sales business.

Presently, export controls would treat this second category as any other exporter. If the firm sells to an overseas customer, it would be expected to seek an export licence to do so. This would require the firm to know whether the goods were subject to control or not.

Firms in the first category are different, however. Such firms are typically not exporters: they do not ship goods to the customer. Instead, these firms act to link potential buyers and sellers. Such firms, while usually not physically handling the goods, have the potential to transform supply chains. Traditionally, customers would connect with potential suppliers through recognised distribution chains and agents. Since the advent of this form of ecommerce, however, potential suppliers can link with potential consumers as never before. This has allowed for an unprecedentedly direct connection between supplier and customer, one offering a level of discretion and anonymity to both.

The role of e-commerce platforms in export compliance thus varies depending on the nature of the business model. In the context of the export control review, consideration should be given to the export control obligations for both categories. It would seem that the second category can simply be treated as an exporter. However, in the first category, a decision is required about what maybe the role of such firms in export compliance.

7.3 Intangible Technology Controls

As explored above, the current regulation results in intangible technologies being controlled alongside physical goods.

Export controls and academia: Academia finds itself in an unusual position in relation to export controls. The primary purpose of academia is to generate and distil knowledge – a mission that could be in conflict with the principles of export controls. Academia also regularly deals with 'technology' without necessarily also handing controlled goods, meaning that the assumption that technology will usually be associated with controlled goods may not be valid.

Universities are engaged in some activities that are of higher concern, however, particularly with regards to applied research (often conducted for foreign commercial entities) and technical consulting.

Much attention has also been given to the publication of genome data that could potentially be used to recreate viruses and bacteria. The use of export controls to prevent such transfers is certainly a crude tool.

On a case by case basis, the formation of closed, pre-approved communities and codes of conduct should be considered.

In terms of export compliance in academia, a distinction should be made between universities and academics. In a business environment, the company is responsible for export violations unless individual employees act without authorisation. In the academic environment, academics often operate 'semi-autonomously' within the university. The implication of this is that the role of universities should be to adopt a systematic approach to compliance and training of students and staff, but that it is academics who should be liable for export control violations related to their research activities.

The Commission should consider adopting issuing informal guidance to universities on export compliance, such as that prepared by KCL and AULP. (King's College London and Association of University Legal Practitioners) The Commission should also explore promoting the adoption of codes of conduct in pursuit of non-proliferation controls.

Tacit knowledge transfer: The history of proliferation has seen European citizens directly assist programmes of concern through technical assistance. This involves 'tacit' knowledge transfer which typically must be done in person rather than via electronic or other impersonal means. Some European member states implement either or both types of control In line with Joint Action 2000/401/CFSP. Considerations should be given to incorporate these measures into an updated EU export control regulation for the purpose of deterring, and if necessary, punishing, such activity. The regulation should control technical assistance in support of WMD programmes.

Manufacturers and experts: Intangible technology controls on technology associated with physical goods are challenging for national authorities to enforce. For this reason, it is suggested that the commission move towards an internal compliance programme model rather than a specific export model. This would involve requiring firms that manufacture controlled goods to show how they manage the intangible controls. This should include demonstrating how they incorporate export control considerations into any contracts with universities and with regards to the emerging challenge of cloud computing.

Cloud computing and export controls: Cloud computing is the practice of using a shared reservoir of computers, hardware, software, servers, storage facilities and other similar functionalities "virtually," hosted though the Internet. This practice holds significant advantages as it provides businesses, universities, government agencies, and other entities with access to more flexible, more cost-effective and often physically dispersed computing resources. Though not generally considered as a risk area for breach of traditional export controls and sanctions, the use of cloud computing services has raised some interesting questions about compliance with national and international regulations. The increasing prevalence of the cloud is centred on the premise that there is no need to track the details of data movement among various destinations – a premise standing in direct opposition to the very essence of export control regulations.

The United States has gone some way to provide guidance on the issue of cloud computing. The EU should do so aswel.

7.4 Synergies with Outreach

By virtue of its political and economic influence, the European Union is well placed to promote implementation of non-proliferation controls in countries outside the Union. This is known as 'outreach'. There are many mechanisms through which the EU can promote the improved implementation of non-proliferation controls. This includes the EU's outreach program on dual-use goods, trade agreements and individual authorisations. The Commission should develop an outreach strategy that explores how to bring together these various policy levers to best encourage improved implementation of non-proliferation controls in third countries.

Consideration should also be given to whether trading partners could be notified of authorisations granted by EU member states. The purpose of such notifications would be to encourage the partner country to conduct targeted industry outreach and, if appropriate, end user and end use verification. Consideration should also be given to how third countries can be kept abreast of guidance and decisions taken by the dual-use coordination group.

The EU could also use the 1540 mechanism to better effect for outreach purposes by, for example, submitting the EU control list as an example of an "effective practice".[21]

8 Conclusion: The State of Play and Need for Reform

This report has explored the state of play and the need for reform concerning the current EU export control system for dual-use goods, as embodied in Regulation 428/2009. The examination has found that the regulation is generally fit for purpose, although there are areas in which the dual-use export control system can be improved. Some of these improvements would require a change to the regulation. Nonetheless, Regulation 428/2009 should be seen as an effective regulation which serves as a sound foundation upon which to build. It is notable that many of the recommendations could be dealt with by the issuing of non-binding guidance.

This examination has also not found that other export control systems are substantially more competitive when compared to that of the EU. Indeed, the EU is in line with the main export control regimes and is seen as a model for others. This issue of adherence should be borne in mind during the course of the review and after – countries outside of the European Union that adhere to the EU control list do not benefit from the EU's collective resources, including the 'corporate knowledge' that has been built on how to interpret and implement the EU control list.

While this examination has found that the regulation is generally fit for purpose, several challenges remain. Having 28 Member States decide on how to implement one regulation naturally results in variable implementation. When viewed together with the EU's substantial production of dual-use goods, the EU is looked upon as a target by proliferators.

The regulation should thus be updated with the recommendations below in mind in accordance with option 4 of the Commission's Roadmap. (European Commission, 2014) The European Parliament should also periodically consider whether the scope and implementation of the regulation is in keeping with the regulation's objectives, perhaps through workshops and hearings on an annual basis.

9 Recommendations

In reviewing the implementation of regulation 428/2009, numerous specific areas where the regulation or its implementation could be improved were identified.[22]

Scope and Definitions
3.2   That consideration be given to the question of whether the US action in moving goods from the military to dual-use list should and/or could be replicated in the European Union.

4.1   That the definition of weapons of mass destruction be clarified. For example, the definition of nuclear proliferation could be clarified to mean: for use in unsafeguarded nuclear activities or nuclear programmes that are not in good standing with the International Atomic Energy Agency.

---

[21] The 1540 Committee maintains a list of effective practices as submitted by states. See
http://www.un.org/en/sc/1540/experiences.shtml
[22] The number below refers to the proceeding section in which the recommendation was discussed.

4.2   That consideration be given to broadening the military end use control to control exports when the exporter knows or has been informed that the goods will be used for human rights violations, paramilitary activites or terrorism.

6.3/7.3 That the definitions associated with technology be reviewed and guidance be provided on their scope.

Coordination and administration

2.3   That an 'in-reach' programme be created through which experience can be shared among EU member states in pursuit of common implementation.

2.3   That consideration be given to the question of how penelties could be standardised across the union and how enforcement actions can best be promulgated to maximum effect.

2.4   That a licensing enforcement working group be created through which information and experience can be shared among EU member state experts, perhaps in partnership with TAXUD.

2.4   That consideration be given to mechanisms to take advantage of synergies between export control and sanctions mechanisms within the EU.

2.4   That the regulation require states to share relevant information with international authorities including the IAEA and UN Panels of Experts

3.1   That a common assessment criteria be adopted to ensure that states assess licences in a similar way. This should include a clarified definition of WMD as described above. It should also include a presumption of denial for licences to entities designated by the UN or EU for involvement in proliferation.

4.2   That consideration be given to requiring an evaluation of the human security implications of an export.

7.4   That guidelines be adopted on how academia should implement export controls.

Synergies with outreach

7.5   That the Commission develop a strategy for promoting strong implementation of non-proliferation controls in third countries which would bring together the EU's various policy leavers and capacity building programs.

7.5   That the Dual-Use Coordination Group consider holding meetings with accession states, key trading partners, and states that use the EU control list.

7.5   That consideration be given to publishing the guidelines agreed by the Dual-Use Coordination Group to inform stakeholders, including industry and the groups of countries mentioned above.

7.5   That consideration be given to submitting the regulation (including its extant control list) to the 1540 committee as an example of an effective practice.

7.5   That consideration be given to notifying the authorities in recipient countres when an export authorisation is granted.

Supply chain issues

5.   That guidelines be issued on internal compliance programs and consideration be given to requiring internal compliance programs (ICP) as a prerequisite to the use of General and Global licences.

5.   That the EU endorse and publish the document "Good Practices for Corporate Standards to Support the Efforts of the International Community in the Non-Proliferation of Weapons of Mass Destruction". (Nuclear Supplier Group)

7.2   That the EU recognise the document "Sanctions compliance for the maritime transport sector" as being good practice for export compliance in those sectors.

<u>Role of Parliament</u>

That the European Parliament monitor implementation of the regulation by holding workshops and hearings on a regular (at least annual) basis, and that Parliament makes recommendations to the Commission as needed.

That the European Parliament request tht the commission respond to the recommendations contained herein.

10   Bibliography

Department of Commerce, 'Wassenaar Arrangement 2014 Plenary Agreements Implementation and Country Policy Amendments', Federal Register, Vol 80 No. 98, 21 May 2015. Available online at: https://www.federalregister.gov/articles/2015/05/21/2015-10579/wassenaar-arrangement-2014-plenary-agreements-implementation-and-country-policy-amendments. Accessed 17 July 2015.

European Commission, Com(2015)331, 'Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items', July 10, 2015, Available online at: http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153612.pdf.

European Commission, 'Communication from the Commission to the Council and the European Parliament, The Review of export control policy: ensuring security and competitiveness in a changing world', COM(2014) 244 final, Brussels, 24 April 2014. Available online at: http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf. Accessed 2 September, 2015.

European Commission, 'Roadmap. Review of the EU dual-use export control regime – Regulation 428/2009', DG Trade F1, 15 July 2014, Available online at: http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2014_trade_014_dual_use_en.pdf.

European Commission, 'Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items', Brussels, 10 July 2015 COM(2015) 331 final. Available online at: http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153612.pdf. Accessed 29 August 2015.

European Council, 'EC 1334/2000', 2000, Available online at: http://www.sussex.ac.uk/Units/spru/hsp/documents/2000-0622%201334-2000.pdf. Accessed 13 July 2015.

European Council, 'Council Regulation (EC) 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items [2009] L 134', 5 May 2009, Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF. Accessed 17th July 2015.

Google, "Google, the Wassenaar Arrangement, and vulnerability research", Google Public Policy Blog, 2015, 20 July 2015. Available online at: http://googlepublicpolicy.blogspot.co.uk/2015/07/google-wassenaar-arrangement-and.html. Accessed 27 August 2015.

King's College London and Association of University Legal Practitioners, *Higher Education Guide and Toolkit on Export Controls and the ATAS Student Vetting Scheme*, 2015. Available online at: https://www.acsss.info/academia.

Michel, Dr. Quentin, 'The European Union Export Control Regime: Comment of the Legislation: Article by Article', 2011, Available online at: http://csis.org/files/attachments/130828_3EUExportControlRegimeCommentary.pdf. Accessed 13 July 2015.

Nuclear Supplier Group, 'Good Practices for the Corporate Standards to Support the Efforts of the International Community in the Non-Proliferation of Weapons of Mass Destruction,' Available online at: http://www.nuclearsuppliersgroup.org/en/national-practices/132-good-practices-for-corporate-

standards-to-support-the-efforts-of-the-international-community-in-the-non-proliferation-of-weapons-of-mass-destruction.

Project Alpha, 'Global Nuclear Manufacturing Base Study', Project Alpha, King's College London, 1 July 2014.

Nayan R., and Stewart, Ian J., 'Export Controls and India', CSSS Occasional Paper Series, January 2013, Available online at: https://www.kcl.ac.uk/sspp/departments/warstudies/research/groups/csss/pubs/India-export-control.pdf. Accessed 2 September 2015. hrsi

Stewart, I,. 2015a, 'EU Production of Dual-use Goods', Project Alpha, 3 June 2015 Available online at: http://www.kcl.ac.uk/sspp/departments/warstudies/research/groups/csss/pubs/India-export-control.pdf. Accessed 29 August 2015.

Stewart, I,. 2015b, 'China and Non-Proliferation: Progress at Last?', 25 March 2015, Available online at: http://thediplomat.com/2015/03/china-and-non-proliferation-progress-at-last/. Accessed 29 August 2015.

Stewart, Ian J, Stricker, Andrea, and Albright, David, 'Chinese Citizen's Involvement in the Supply of MKS Pressure Transducers to Iran: Preventing a Reoccurrence', ISIS Reports, 30 April 2014, Available online at: http://isis-online.org/uploads/isis-reports/documents/MKS_China_30Apr2014-final.pdf. Accessed 27 August 2015.

United Nations Security Council, 'Resolution 1540', UN Doc S/RES/1540 (2004), 28 April 2004. Available online at: http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540%20(2004). Accessed 17 July 2015.

United Nations Security Council, 'Letter dated 15 January 2015 from the Permanent Representatives of Australia and Singapore to the United Nations addressed to the President of the Security Council: Sanctions Compliance for the maritime transport sector', UN Doc S/2015/28, UN Security Council, New York, 16 January 2015, Available online at: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2015_131.pdf . Accessed 17 July 2015.

United States Government Publishing Office, 'Licence Exceptions: Encryption commodities, software and technology (ENC)', 2015, Available online at: http://www.ecfr.gov/cgi-bin/text-idx?SID=86d59a5fcda4eb9ca286e85d7e818517&mc=true&node=se15.2.740_117&rgn=div8. . Accessed 17 July 2015.

POWERPOINT PRESENTATION

Regulation 428/2009

Created a single approach to licensing that is implemented at the national level

- Defines what (dual-use) goods are subject to control
- Sets out what types of considerations should be taken into account
- Includes mechanisms for information sharing and preventing undercutting

Comparison with others:

- US controls more goods (unilateral controls) and is moving toward a single licensing agency
- No clear signs that the US is or is becoming more competitive than EU other than in relation to certain specific sectors

EU Exports of Dual-use Goods

- Total value of dual-use goods produced is unknown. One estimate - **€26.5bn and €36.2bn** (must improve data capture).
- Substantial producer of dual-use goods
- Signs that implementation varies considerably among states

Production of chokepoint goods

Transshipment of goods

Priority 1

Human Security

- How can export controls contribute – criteria, additional controls?
- Likely that it would be necessary to redefine export controls to incorporate human security. Role of Regimes?

Smart Security

- Smaller states may lack the technical expertise to identify and evaluate proposals etc.
- Some M/S not represented in export control regimes.

Priority 1

Immaterial control

- Area of substantial weakness in current regulation
- Definitions often open to ambiguity
- Guidance for industry and academia weak or absent
- Little collective knowledge or case law
- Unclear whether controls as designed actually contribute to non-proliferation (explicit knowledge rather than tacit knowledge)
- Unclear whether / how to link export controls and visa / student vetting schemes.

Priority 2 — Licensing In EU M/S

Considerable variation among states:
- Some states offer open licences, others do not
- Targets for processing licences varies between states

Use of EU General licences does act to level playing field but limited scope to date.

Priority 2 — Optimising controls (Method)

There is scope for relaxing some controls without increasing risk:
- Sectoral
- Value
- Destination Country

UK SIEL Licence Value per Year
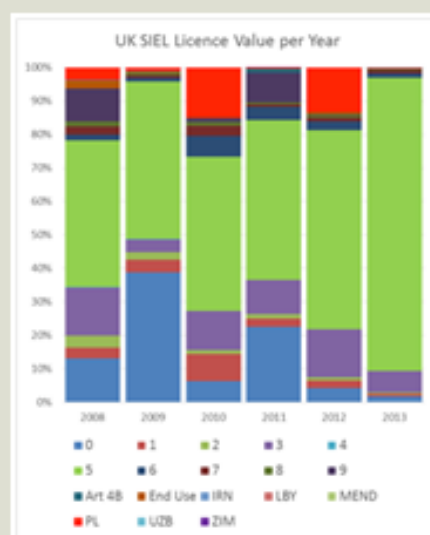
Priority 3 — Risk-based Approach

- No common risk approach among M/S. Even assessment criteria are not standardised.
- No formal "watch lists" of entities or recipient states (other than those covered by sanctions).
- Licensing decisions do differ between M/S.
- Little common understanding of technological risk: not all control entries are equal.

Priority 3 — Intra-EU Transfers

- Certain goods require licences for transfer even within the EU
- Historically, these are items for which the M/S has a reporting obligation to an international body.
- Generally, transfers pose low proliferation risk but it is vital that reporting is accurate. Could a notification-based system provide similar results?
- Balance of investment: should avoid making substantial changes that benefit few firms.

Priority 4   **Enhanced Structural Exchange**

- Presently, the export control regimes may do a better job at information exchange than the EU.
- No forums for information exchange between technical or assessment staff. Limited sharing of electronic information (mainly denials, customs information).
- Should this be left to the export control regimes?

Priority 4   **Outreach and In-reach**

- Other States do use the EU approach and list. Is it presented in the best format for this? (why not a filterable table?)
- Participation in outreach missions upskills EU staff: must be encouraged.
- Lack of "in-reach" program an oddity: can the EU expect other states to engage in training, capacity building when there is no such program in the EU?

Priority 4 — **Supply-chain Engagement**

Most EU M/S have industry engagement programs.
However, little standardisation:
- Many states do not encourage firms to have an 'internal compliance program'.
- No common training or competence framework.
- Little Europe-wide guidance on what firms should do to combat supply-chain proliferation risks.
- European Union has not recognised NSG good practice guidelines documents etc.

Conclusions and key judgments

EU regulation for controlling dual-use goods among the best in the world. The opportunity is to improve and leverage it to help others
- Implementation across the EU is variable. A so-called 'in-reach' program is essential.
- Common risk assessment required. This can be used to facilitate trade (open licensing etc).
- New controls should link to strategy: export controls are the means, not the ends.

THANK YOU

**IAN STEWART
HEAD, PROJECT ALPHA
KING'S COLLEGE LONDON
WWW.ACSSS.INFO
+442078481342
IAN.STEWART@KCL.AC.UK**

PART II: IMPROVEMENT OF EU DUAL-USE EXPORT CONTROLS IN THE CONTEXT OF THE EUROPEAN COMMISSION'S REFORM PROPOSAL
(by Dr Sibylle Bauer)

1 Introduction

The second part of this study explores how to improve the effectiveness of EU dual-use export controls against the backdrop of the review options presented by the European Commission in the April 2014 Communication, which aims to set out 'concrete policy options for the modernisation of EU export controls and their adaptation to rapidly changing technological, economic and political circumstances' (European Commission 2014a).

The title of the Communication, 'Ensuring security and competitiveness in a changing world', reflects the overall rationale for export controls, which requires balancing their contribution to security, with their impact on EU economic and trade interests. At the same time one can argue that a well designed and effectively implemented export control system can enhance both security and economic and trade interests: in other words, there is no reason to present this as a trade-off between security and economic interests. Moreover, one could add a third dimension to this balancing act: academic freedom, the limits of which are currently under discussion in the context of the further clarification of controls of intangible transfers of technology (ITT), for example through publications.

The April 2014 Joint Statement by the three institutions (European Parliament, Council and Commission) included in Council Regulation 599/2014 also highlights the importance of 'enhancing the effectiveness and coherence of the EU's strategic export controls regime, ensuring a high level of security and adequate transparency without impeding competitiveness and legitimate trade in dual-use items' (OJ L173, 12.6. 2014). This illustrates the same drivers and resulting balancing act while additionally underlining the role of coherence, which is also an important feature of the Commission Communication and will be considered further in this study. Indeed, a lack of coherence between different EU instruments and between Member State implementation and enforcement may already be partially undermining the effectiveness of the regime. At the same time, it is important to keep in mind that different implementation approaches do not necessarily constitute a lack of coherence, but may rather be a way to tailor controls to a country's institutional set-up, geographical location, industrial structure and trading patterns, and its foreign and security policies.

The Joint Statement furthermore points to one of the main goals of the EU's current dual-use export control regime: ensuring security through preventing or disrupting illegal dual-use exports and related activities, in particular those contributing to Weapons of Mass Destruction (WMD) programmes and to military capabilities in embargoed destinations, without impeding legitimate trade. While estimates differ and no precise figures are available (European Commission, 2013a), there is wide agreement that only a few per cent of the overall EU export volume are dual-use. Moreover, dual-use items that are destined for a military end-use in an embargoed destination, or are intended or diverted for a WMD end-use constitute a very small percentage of the total trade. For example, Triethanolamine will normally be destined for shower gel and tooth paste production rather than a chemical weapons programme. Filament winding machines will mostly be intended for the manufacture of tennis rackets and other civilian products rather than missile parts. And aluminium has multiple uses that are not related to nuclear weapons. Many dual-use items such as lasers, sensors or sophisticated IT equipment, are controlled because of their conventional military applications, and associated risk assessments are therefore closely linked to those for military equipment. The broader underlying idea has thus been to monitor security-relevant trade and make risk assessments to determine which transfers should be authorised.

The joint document also calls for the modernisation of the EU dual-use system to take account of new technological, economic and political developments, and emphasises that while doing so the EU should continue to serve 'as a benchmark for third countries'. This is important in the context of arguments that EU-based companies may have a competitive disadvantage due to certain export provisions, compared to some of their competitors. The counter-argument is that the EU should set standards that other countries may choose to adopt. This has been the case, for example, for the EU control list and some other provisions of the EU Dual-use Regulation 428/2009, which is the centrepiece of the EU dual-use export control system. 'Modern' has been defined as 'characterized by or using the most up-to-date techniques, ideas, or equipment'.[23] Modernisation therefore requires rethinking and reviewing all aspects and dimensions, consulting a wide range of stakeholders, and also looking at other possible approaches in other countries and regions.

To understand the political, legal, technological and economic backdrop against which the review is taking place, the rationale and purpose of EU dual-use exports need to be kept in mind. The primary purpose of dual-use export controls is rooted in security concerns, based on the definition of dual-use items as those that have both military and civilian applications. These items are also sometimes referred to as strategic items (a term which also includes goods and technology that are specially designed for military use). There is an on-going discussion about making items subject to dual-use export controls on the basis of a broader set of considerations and applying a broader set of concerns when assessing export licences. These include human rights violations and a broader range of security risks. One way to facilitate this expansion would be to apply a 'human security' approach to export controls for dual-use goods. This process has been closely tied to the application of export controls to a range of cyber-surveillance technologies.

The dual-use **items** governments seek to control include software and technology (in both tangible and intangible form). As has been explained in Part One of this study authored by Ian Stewart, items subject to control may be explicitly included on a control list, or only subject to control based on a specific end-use or end-user (also referred to as catch-all or end-use controls). Related **activities** subject to control in addition to export can include transit, transhipment and brokering. Nevertheless export control remains the key principle around which associated controlled activities and actors revolve.

This expanded range of items and activities subject to control has resulted in an increased number of supply chain actors that are affected, or potentially involved in 'exporting' through export-relevant activity: in addition to exporters, there are traders, shippers, transport agents, freight forwarders and brokers, as well as the research community (e.g. academics and laboratory staff). In addition, the range of company staff involved in 'exporting' has also expanded: in addition to those directly involved in the export, there are also those staff transferring controlled technology through email, software uploads or travel to meetings with a laptop containing controlled technology. Moreover, the exporter is not necessarily the producer of the items.

The April 2014 Communication covers a broad range of issues, including the practical implementation of the new transit and brokering controls introduced in 2009; the uniform implementation of catch-all controls across the EU; and the appropriateness of activities and items subject to control in the current trade, political and technological environment. Before proposing amendments to the legislation, the European Commission will further engage and consult stakeholders (European Commission, 2014b, 2015).

---

[23] <http://www.oxforddictionaries.com>

The process began in 2011 with the publication of a Green Paper reviewing the EU's trade controls on dual-use products (European Commission, 2011). EU Member States, the European Parliament, industry associations, economic operators, civil society organizations and academia, as well as consultants and other stakeholders, provided views in response to this paper. Although the views are made public only if put into the public domain by the author(s), they were summarized and published in a staff working document in 2013 (European Commission, 2013a). A public consultation on the Commission Communication and its review options was initiated on 15 July 2015.[24]

This study analyses the individual review actions presented from the perspective of their potential contribution to the effectiveness of the export control system, and also discusses their impact on key stakeholders, notably government, industry and academia. Importantly, for many of the review options the question determining the economic and security impact is not **whether** they will be adopted and implemented, but **how**, as there are a number of ways to approach them**.** For example, the extent to which companies in the ICT sector are affected by an expansion of controls on cyber-surveillance technologies, will depend on whether their products are covered by an expansion to the dual-use control list or the adoption of catch-all controls in this area, what criteria are adopted in relation to the assessment of licences for the export of those items, and whether their national licensing authorities implement these controls via individual, global or general licences.

The Roadmap (European Commission, 2014b) categorises the different review actions discussed in the 2014 Commission Communication into five broad review options: (1) No policy change; (2) Implementation and Enforcement Support; (3) EU System Update; (4) EU System Modernisation; and (5) an EU System Overhaul.

Option 2 includes strengthened information exchange between Member State authorities and enhanced cooperation between enforcement authorities, as well as a range of actions summarised under the heading 'partnership with the private sector'. The latter include guidelines, consultations, e-licensing etc. Option 3 could entail changes to the existing legal-regulatory framework, such as export facilitation measures for certain items; convergence of the implementation of catch-all, brokering and transit controls across the EU; a review of transfer controls for Annex IV items; a review of key definitions such as the notions of dual use and exporter; internal compliance requirements for companies and other concerned stakeholders; and a review of ITT controls. The Roadmap explicitly specifies that elements of Option 2 could also be included in Option 3. They are therefore not mutually exclusive. Similarly, Option 4 may also contain elements of options 2 and 3, but would add controls on exports of cyber-surveillance technologies from the EU. Option 5 (the 'full harmonisation and centralisation of controls'), is not further detailed given the lack of interest in pursuing this option among a number of EU Member States. Options 2 through 4 include a substantial number of review actions, which are grouped under review issues. These review actions are discussed in detail below.

The discussion below on how to enhance the effectiveness of controls is structured according to the four 'priorities' of the Commission Communication: (1) 'adjust to the evolving security environment and enhance the EU contribution to international security'; (2) 'promoting export control convergence and a global level-playing field'; (3) 'develop an effective and competitive EU export control regime'; and (4) 'support effective and consistent export control implementation & enforcement'.

The study takes up individual review actions, considers the different ways they could be shaped, and describes the respective benefits, potential downsides, as well as challenges to be addressed and overcome in their realisation. Finally, it explores additional options for enhancing the effectiveness of

---

[24] <http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190>.

controls against the background of level playing field objectives within the EU and internationally, and the demands of international security. The study thus illustrates the role of global value chains, and the challenges created by different control requirements and systems, transit regimes, foreign availability and risk of circumventions. In doing so, it builds on the sections on these issues in the first part of this study.

Finally, two points should be highlighted. First, different actors may disagree in their assessment of the export control system's effectiveness, based on their respective interests and perceptions, in particular regarding trade, security interests and human rights. While some mechanisms or actions may contribute to all three, others will present a trade-off or balancing act. Second, harmonisation should not be a goal in itself, but serve a purpose. Where differences in dual-use export control policy within the EU are rooted in different foreign policy priorities, security perceptions or commercial interests, this will not be resolved through harmonised procedures but will require broader political solutions.

2 Adjust to an evolving security environment and enhance the EU contribution to international security'

Dual-use export controls are a major component of the EU's 2003 Strategy on the Non-proliferation of Weapons of Mass Destruction (EU WMD Strategy) and the complementary New Lines for Action by the European Union in Combating the Proliferation of Weapons of Mass Destruction and their Delivery Systems (New Lines for Action, NLA) of 2008. Increasingly complex procurement patterns for illicit WMD programmes and technological developments make proliferation-sensitive flows more difficult to control through the application of traditional legal concepts and enforcement methods (Bauer, 2013a, p. 4). The use of intermediaries, front companies and transhipment — and thus potential diversion — points has multiplied (Bauer and Micic 2010, p. 447). In addition, the increased complexity of regular production and trading patterns and supply chains has made it easier for illegal procurement efforts to disguise the actual end-use and end-user of transactions. These developments require constant adjusting and fine-tuning of regulatory systems, including outreach to stakeholders as well as revisions to legal provisions, control lists, licensing types and procedures, and enforcement tools and mechanisms.

Additionally, the often referred to fast pace of technological developments may require adaptation of the legal-regulatory mechanisms governing the use or spread of certain goods and technologies through de-controlling or adding controls. However, the term 'rapid' in connection with responses may be not realistic. Rather, appropriate mechanisms have to be put in place that: (a) anticipate certain developments to the extent possible while avoiding over-controlling (which is one function of the catch-all provision in Article 4 of the EU Dual-use Regulation); and (b) monitor technological changes and find appropriate responses from security, human rights, humanitarian law and other relevant perspectives. However, security and economic interests and perceptions regarding the controls of certain good and technologies may differ between countries and regions, and dual-use export controls will always have a strong, or even dominating political dimension.

2.1 Human security dimension[25]

The Commission Communication[26] considers: the application of human security criteria to exports of cyber-surveillance technologies; obligatory self-regulation on the part of industry producing cyber-surveillance technologies; introduction of an EU autonomous list for cyber-surveillance technologies (via a technical or descriptive list); and introduction of an EU cyber-surveillance catch-all mechanism), either through a dedicated catch-all for cyber-surveillance technologies or application of general catch-all.

During 2011, companies based in the EU (as well companies based in other parts of Europe and North America) were identified as having been involved in the supply of security, surveillance and censorship goods, services and technologies to states in the Middle East and North Africa. In a number of cases, national security forces used these in violation of international human rights law. In certain cases, exports of the items concerned were covered by dual-use export controls on the grounds that they contained certain levels of encryption. However, in many instances, existing EU and Wassenaar Arrangement control lists did not cover the goods, services and technologies involved (Bauer and Bromley 2013, pp. 463-465).

During 2011 to 2013 steps were taken at both the EU and Wassenaar Arrangement level to expand controls on the export of certain cyber-surveillance technologies. However, a number of NGOs have argued that gaps still exist and that there is a range of cyber-surveillance technologies being supplied by EU-based companies that are not subject to export controls (CAUSE, 2015).

These developments have fed into a broader discussion about the potential need to expand both the items covered by the EU's dual-use export controls and the considerations that Member States take into account when assessing export licences. This would involve making more items subject to control on the basis of a broader range of human rights and security risks and taking a broader range of human rights and security considerations into account when making licensing assessments. One way to facilitate this expansion would be to apply a 'human security' approach to export controls for dual-use goods. According to the European Commission, this would potentially involve 'a clarification of control criteria to take into consideration broader security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations' (European Commission, 2014a).

Currently, at least three definitions of '**dual-use' items** exist in parallel.

1. Civilian or military applications (WMD-related and conventional), which is the concept that is currently the basis of the EU Dual-use Regulation.

2. In the nuclear community dual-use means also non-nuclear uses as opposed to single (exclusively nuclear) use, including civilian nuclear power.

3. A third definition, currently under discussion, would expand the first concept to include items used by law enforcement authorities and intelligence agencies that can potentially be linked to human rights violations, such as cyber-surveillance technologies.

Additionally, there is a wider debate about 'security' rather than just military as a key concept, which has impacts on measuring spending, procurement and exports.

In late 2011 and early 2012, the EU arms embargoes on Iran and Syria were both updated to include prohibitions on the sale of surveillance technologies (OJ L319, 2.12.2012, p. 56; and OJ L87, 24.3.2012, p.

---

[25] Thanks to Mark Bromley for providing input into this section.
[26] All further references to the Commission Communication refer to European Commission (2014a) in the list of references.

85). In December 2011, the EU embargo on Syria was updated to include a ban on the sale of 'equipment which might be used for internal repression' including 'equipment or software intended primarily for use in the monitoring or interception by the Syrian regime, or on its behalf, of the Internet and of telephone communications on mobile or fixed networks', as well as the provision of associated services (Council Decision 2011/782/CFSP of 1 December 2011, OJ 2.12.2012). In March 2012, equivalent language was inserted into the EU embargo on Iran (Council Decision 2012/168/CFSP of 23 March 2012, L87, 24.3.2012).

In 2012 and 2013 certain categories of surveillance technologies — specifically, 'mobile telecommunications interception or jamming equipment', 'IP network surveillance systems' and 'intrusion software' — were added to the Wassenaar Arrangement's dual-use control list. In December 2014, these items were added to the EU's dual-use list (Annex I of the EU Dual-use Regulation). In 2014 the EU's Dual-Use Coordination Group established a Surveillance Technology Expert Group to examine issues relating to controls on the export of cyber-surveillance technologies.

While the expansions to the EU's Syria and Iran embargoes were tied to human rights considerations, the additions to the Wassenaar Arrangement's control list were based — at least in part — on traditional considerations of national and regional security. For example, the language on intrusion software was proposed at the Wassenaar Arrangement by the UK Government and was aimed at addressing both the human rights and national security concerns associated with their use (UK Department for Business Innovation & Skills, 2015). Any attempt to add items to the Wassenaar Arrangement dual-use control list on purely human rights grounds would likely meet resistance from some Participating States. Agreeing additions to the dual-use control list on purely human rights grounds would likely only be possible at the EU level.

Such an expansion of controls at the EU level could be implemented via a list-based approach or a catch-all control, or a combination of both. Article 8 of the EU Dual-use Regulation gives Member States the option to introduce additional national controls based on public security or human rights considerations. EU Member States have used this provision to require authorisation for the export of certain types of cyber-surveillance systems. For example, in 2012, Italy imposed controls on the export of 'public LAN database centralised monitoring systems' to Syria.[27] However, EU Member States have been unwilling to agree EU-wide additions to the dual-use control list that have not already agreed via one of the existing multilateral export control regimes. Generally, list changes that are made in the multilateral control regimes rather than solely at the EU level have less effect on the competitiveness of EU companies.

A proposal for a dedicated catch-all mechanism for exports of cyber-surveillance technologies was made by the European Parliament in October 2012 in its list of proposed amendments to the European Commission proposal for changes to the 2009 Dual-use Regulation.[28] However, the amendment was not adopted. Cyber-surveillance technologies are evolving at a rapid pace and a catch-all clause would potentially be better able to keep pace with these developments than a list-based control system. The precise economic impact naturally would depend on the wording, precision and scope of such a

---

[27] 'Information note — Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items: Information on measures adopted by Member States in conformity with Articles 5, 6, 8, 9, 10, 17 and 22', OJ C283, 19.9.2012,
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.283.01.0004.01.ENG>.
[28] Specifically, the European Parliament proposed the inclusion of a requirement for authorization of exports of unlisted dual-use items if the exporter has been informed by either its national authorities or the Commission that the items may be used in connection with violations of human rights, democratic principles or freedom of speech through the use of 'interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use' European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) no. 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (COM(2011)0704 – C7-0395/2011 – 2011/0310(COD)), 23 Oct. 2012.

provision. However, there are concerns that it could introduce a substantial degree of uncertainty, and a wide range of companies might need to acquire new competence and expertise. Any uncertainty could generate a large number of speculative licence applications and lead to increased costs for industry and governments.

The **application of human rights considerations to exports of dual-use goods** is already required under the EU Dual-use Regulation. In particular, Article 12 requires Member States to take into account 'all relevant considerations' when assessing dual-use authorisations. The article specifies that these include:

> '(a) the obligations and commitments they have each accepted as members of the relevant international non-proliferation regimes and export control arrangements, or by ratification of relevant international treaties;
>
> (b) their obligations under sanctions imposed by a common position or a joint action adopted by the Council or by a decision of the OSCE or by a binding resolution of the Security Council of the United Nations;
>
> (c) considerations of national foreign and security policy, including those covered by Council Common Position2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment[29]
>
> (d) considerations about intended end use and the risk of diversion.'

Hence, Member States can apply foreign and security policy criteria in their risk assessments, which can (and should) include human rights considerations. Second, their international commitments include international human rights law. And third, the eight criteria of the 2008 Common Position on the export of military technology and equipment (OJ L335, 8.12.2008) and its associated User's Guide include certain human rights and security concerns associated with the export and use of cyber-surveillance technologies. In particular, criterion 2 of Council Common Position 2008/944/CFSP requires Member States to deny an export licence if 'there is a clear risk that the military technology or equipment to be exported might be used for internal repression.' Meanwhile, criterion 5 requires Member States to take into account 'the potential effect of the military technology or equipment to be exported on their defence and security interests as well as those of Member State and those of friendly and allied countries.'

However, not all of the human rights and security concerns associated with the export and use of cyber-surveillance technologies are covered by the EU Common Position and it's associated User's Guide. In many cases, the end-users for exports of cyber-surveillance systems are private companies while many of the human rights violations associated with their use concern violations of the right to privacy, freedom of expression, or freedom of association. However, in the User's Guide that accompanies the EU Common Position, the sections on criteria 2 and 5 make no direct mention of deliveries to private companies and focus on transfers to police or security forces while the section on criterion 2 does not explicitly mention the recipient state's standards on the right to privacy, freedom of expression, or freedom of association. Finally, when discussing criterion 5, the User's Guide does not consider many of the security risks associated with the export and use of cyber-surveillance technologies, such as the theft of government and commercial secrets.

In addition, the link between the EU Dual-use Regulation and the EU Common Position is not entirely clear. As noted, the Dual-use Regulation states that all exports of dual-use items should be assessed against the 8 criteria of the EU Common Position. However, Article 6 of the EU Common Position states that exports of dual-use goods should be subject to assessment under the EU Common Position criteria

[29] OJ L 335, 13.12.2008, p. 99.

'where there are serious grounds for believing that the end-user of such goods and technology will be the armed forces or internal security forces or similar entities in the recipient country.'

Expanding the scope of human rights and security considerations that states take into account when assessing dual-use exports would help to address the different concerns raised by the export and use of cyber-surveillance technologies. However, it may also generate calls for further expansions to the range of items that are subject to control. For example, a number of goods and technologies raise concerns related to the right to privacy, freedom of expression, or freedom of association. These include Internet content filtering and blocking systems.

Applying 'human security' considerations to export licensing assessments would expand the range of human rights and security concerns that are taken into account, but may also generate confusion and differences in national practices. The United Nations Development Programme (UNDP) coined the term 'human security' in 1994 (UNDP, 1994). It was an attempt to broaden the notion of security, which was seen to be excessively focused on state security, to include other components, including 'economic security, food security, health security, environmental security, personal security, community security and political security' (UNDP, 1994). Human security is thus a broad concept that informs and shapes the broader policy debate and context. However, the concept is not legally binding and does not have a universally agreed definition.[30] Both industry associations and NGOs have voiced concerns about its application to export control decisions. The AeroSpace and Defence Industries Association of Europe (ASD) has argued that it might lead to the addition of items to the EU control list 'that are not accepted internationally' (ASD, 2014). Meanwhile, the Coalition Against Unlawful Surveillance Exports (CAUSE) have stated it may have 'unintended consequences, such as narrowing rather than broadening human rights protection' (CAUSE, 2015). Human rights criteria are more suitable for specific decisions since there are clear legal documents which decisions can be based upon.

While there is a clear need to address the issue of misuse of cyber-technology for human rights violations or against the EU's own security, the challenge is to find the most appropriate instrument. Effectively regulating exports of cyber-surveillance technologies represents significant challenges. In particular, defining the technology to be controlled, designing and implementing feasible enforcement measures, determining appropriate risk assessment criteria, and ensuring that the European ICT and security industries remain internationally competitive are just some of the significant hurdles that will need to be addressed. Moreover, human rights criteria for controlling items adds a layer of complexity since this combines an assessment of technical capabilities with an assessment of their use, while listing dual-use items with military application is based on a technical assessment.

Any attempt to seriously tackle the human rights and security implications associated with the export and use of cyber-surveillance technologies will require policy instruments beyond export controls, including enhanced self-regulation on the part of companies. In particular, various technologies in this area — such as Deep Packet Inspection (DPI) — can be used for both quality of service and surveillance purposes. These will be difficult to regulate via export controls. There are good practice guidelines drafted by international organisations, governments and NGOs that could be utilised when developing standards for industry self-regulation (e.g. Cohn and York 2011; European Commission 2013b). However, significant gaps exist. For example, while there are a range of guidelines for lawful interception (LI) and

---

[30] A recent report noted that '(h)uman security is a flexible approach and can be tailored to different contexts and topics, according to the specific context.' Oscar A. Gomez and Des Gasper, 'Human Security: A Thematic Guidance Note for Regional and National Human Development Report Teams', (UNDP, without date), <http://hdr.undp.org/sites/default/files/human_security_guidance_note_r-nhdrs.pdf>.

telecommunications companies, there is little in the way of agreed standards for the manufacture and use of targeted surveillance systems, such as intrusion software.

2.2 Response to technological changes

The Commission Communication considers an 'EU technological reaction capacity', to make an active contribution to control list discussions in regimes, also involving 'structured engagement with industry' and guidance on emerging technologies.

The Commission Communication places the proposals for an appropriate response to technological developments under the heading 'smart security'. As discussed in the first part of this study, the fast pace of technological change requires a multi-pronged approach.

A technological response capacity requires technological expertise across a very wide spectrum, combined with knowledge of potential military application. The full range of such expertise is neither available to the European Commission nor to smaller or even most medium-sized Member States. To be effective, it also requires input from industry and academia, who are at the forefront of many new developments, and are usually very aware of technical advances in other countries that undermine export controls through wide foreign availability.

A technical advisory group on proposals for list changes could gather input from industry and would be one way to develop a '**structured engagement with industry'**. This is an approach taken by the United States, for example. Were such a group to be set up, it would need to include all key dual-use sectors and not only large companies, and be drawn from different parts of the EU. And beyond the question of participation, the procedures of such a group would need to mitigate any perceptions of lobbying or undue influence on decisions. Moreover, the advice from industry would necessarily focus on technical dimensions not security issues, which is the role of government.

A dimension that is sometimes overlooked is the security impact of research, which should also be considered against the criteria of international security and human rights. Certain EU-funded projects may even be subject to dual-use export control provisions without those involved being aware. While some guidelines have been drawn up to make applicants and evaluators more aware of obligations under dual-use export controls, such awareness raising measures could be conducted more broadly and systematically.[31] This issue also closely relates to ITT controls and the possible impact on academic research as discussed further below.

ICT is not only rapidly developing but also becoming more interwoven with other technological developments within a multitude of fields. Examples of this are how additive or 3D printing technologies present disruptive technologies that could completely change future manufacturing processes. This evolutionary pattern also expands into areas of biology through synthetic reconstruction and molecular chemistry, and where the primary innovation of these ICT dependent technologies currently is spearheaded by SMEs and academia. Additive printing is also expected to transform parts of the transport sector, since many goods will no longer be transported, but produced in-country, with the required technology transferred by electronic means rather than container ships.

---

[31] 'Explanatory note on the control of "export" for "dual-use items", including technology transfers, under Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items', <https://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-drs-2015/1645163-explanatory_note_on_the_control_of_export_for_dual-use_items_en.pdf>.

As regards the EU's **active contribution to control list discussion in the export control regimes,** this faces several challenges: the fact that not all EU members are represented in all the regimes; the lack of comprehensive expertise for all parts of the control list in many Member States; and concerns about institutional competence and the representation of EU governments through EU institutions in those groups. Regardless of the complex decision-making process in the regimes (Evans, 2014), once those agreed changes are to be integrated into the Annex I of the EU Dual-use Regulation, it is crucial to keep the international implications of EU legislative changes in mind. While updating the EU control list is an internal process, an increasing number of countries use EU legal provisions (in particular the control list) as a model or reference point. Those countries are therefore directly impacted by the efficiency and speed of the list updates, including technical checks and translation. After all, the EU as a model function has been highlighted in the Joint Statement of 2014.

Finally, in the light of the need for an effective export control system in the EU, it is important to keep in mind that not only is technical expertise required for different parts of the control list, but it also has to be tailored to the function it supports. Each element of the dual-use export control system requires and draws upon technical expertise: the legal-regulatory framework, the licensing process, industry outreach and enforcement. Enforcement in turn can be divided up into different aspects and phases: prevention, detection, interdiction/interception, investigation and prosecution. For example, product classification is required in the licensing process, and to some extent for industry outreach. In-depth knowledge of the potential uses of an item and the plausibility of a declared end-use are crucial to the licensing process. Technical expertise, which can be drawn from a range of different government entities such as the licensing authority or nuclear regulatory authority, in turn is required to support enforcement officers in their work, be it through correct identification of a suspect shipment stopped in transit or at export, or giving evidence in court should a case proceed this way. This has to be seen against the background of the increased complexity of export controls, which requires more, different and sometimes quicker access to technical expertise. This could mean that an unlisted machine that is upgraded through software, for example, becomes subject to control due to enhanced capacity above a certain threshold defined in the control list.

Consequently, the technical expertise required varies with regard to: (a) the type and depth of technical background and detail; (b) the speed of access to expertise (24 hours /7 days and as soon as possible, or with several days or even weeks to decide); and closely related, (c) the precision of the advice (a quick approximate advice for an enforcement officer who just stopped a shipment or has questions about the paperwork, or a definitive answer that has to hold up in court, or in fact be evidence in court); (d) the depth of knowledge about proliferation/WMD issues; and (e) the extent of knowledge about industry, pricing and trading patterns (to be able to determine what is unusual one needs to be familiar with what is usual). Countries' difficulties in sufficient or timely access to technical expertise may be of different types: practical/procedural, legal or financial – or the fact that certain expertise is simply not available in a certain region or language. Each of those challenges requires specific responses.

However, the speed of technological change should also not be exaggerated in relation to export control. Key technologies and items for the production of nuclear and chemical weapons that pose current security concerns are not cutting edge but have been available for many decades.

2.3   Intangible transfers of technology (ITT)

The Commission Communication considers providing guidance; outreach to the academic research community; codes of conduct for scientists; and Community General Export Authorisations (CGEAs) for intra-company ITT.

Technological developments have led to substantial changes in export controls as they have expanded beyond the export of goods to include the transmission of technology through intangible means (thus referring to the means of transport, export or transmission) and transfers of intangible technology (where the technology itself is not and has not previously been tangible, such as oral transmission/technical assistance). ITT includes electronic transfers through email attachments, but also server up/downloads or making technology available for a end-user in another country via cloud computing or other internet-based sharing platforms. These developments pose challenges not only for licensing but also for enforcement, since customs officers traditionally deal with goods, not with intangibles including technical assistance. Only those customs or other services (e.g. the licensing authority) that dedicate resources to company audits on dual-use export controls may have a clear role to play in enforcing ITT controls, since their audits will include computers and email transactions. The traditional control function of physical borders is not applicable in this case.

The intangible transfer of technology is however central to normal business interactions, which routinely involve intra-company electronic transfers and shared server access as well as participation in international meetings where information is communicated. Traveling to meetings often involves cross-border travel outside the EU and may involve importing, exporting and transiting controlled technology stored on portable computers. The latter would qualify as a transferring technology in tangible form—like other electronic media such as data storage devices. Should technical information be downloaded in that non-EU country from a server in the EU, this constitutes an export.

More complications arise through the use of cloud computing. Here, the question of access, not of a classical cross-border activity, is key, and may require different solutions such as encryption.

Industry has on a number of occasions, including stakeholder meetings in the context of the dual-use export control policy review, highlighted the need for legal clarification and practical guidance/tools in the area of ITT. The Commission Communication mentions the possible introduction of ITT facilitation tools such as EU General Export Authorisations (GEAs) for intra-company research and development, combined with a focus on pre-transfer control, such as registration and self-auditing, as well as post-transfer monitoring through compliance audits. While companies will in principle welcome EU-wide GEAs, record-keeping measures will add administrative burdens for them, while compliance audits will add administrative burdens and cost for authorities. The area of ITT will require constructive engagement with industry—in particular international companies with research centres and other operations in EU and non-EU countries and thus a need to share and exchange knowledge—to find legal and practical/operational solutions that meet both security policy requirements and are suited to current business operations. While competitiveness and innovation require international cooperation in R&D, a general licence that authorises all technology transfers to foreign subsidiaries could enable technology export without the possibility to apply controls, for example over whether the technology is used not only for R&D but also production, and over the final end-use. A company would only need to establish an entity abroad to transfer dual-use technology without licensing requirements. A global licence may thus be a suitable compromise between security and economic considerations. From the enforcement perspective, there may be little difference between the different types of licences. From the policy perspective, the underlying question is whether it is a) desirable and b) possible to control these transactions. The focus may need to shift to creating a context that facilitates and encourages

compliance, and such policy reflections may even result in the lifting of control requirements rather than a general licence.

This is a key example of the need to modernise controls in order to keep up with evolving technological advances and approaches to research and development, especially as there appears to be a considerable amount of uncertainty, both regarding the correct way to act within safe legal boundaries and regarding suitable options that can be pursued by government and industry. This constructive engagement could be done in the context of an expert forum gathering academic, industry and governmental experts, for example.

ITT are also essential to academic research, exchange and publications. They are part of academic life through the transmission of know-how at lectures, in joint research programmes and in academic publications. In the biological area this may also involve the exchange of samples, although the awareness of any applicable dual-use controls for those goods is likely to be low. Other academic fields such as chemistry and engineering also routinely include transfers of physical items, which may be subject to export control. Constraints on foreign researchers through visa vetting programmes, as practiced in different ways across the EU and a prominent feature of the 2008 New Lines for Action, are controversial and run counter to normal procedures in academia. While a number of Member States have undertaken specific initiatives to reach out to academia and other research institutions (including for example Croatia, Germany, Hungary, the Netherlands and the UK), this aspect of stakeholder outreach is still in its initial stages compared to outreach to companies that export dual-use products. It will require a dedicated outreach strategy and approach. Currently, control authorities and academics in natural sciences, which are or may be relevant for military use, tend to speak different languages, so to say. 'Models for awareness raising for undertakings, scientific and academic circles' was included among the main deliverables in the 2008 'New Lines for Action in Combating the Proliferation of WMD and their Delivery Systems', but follow-up to this aspect of the document has been limited. In seeking to address this issue, a key question to be raised and assessed is the perceived security risk associated with academic research. In this context, one of the terms requiring clarification is basic or fundamental research which, unlike applied research, is exempt from the licensing requirements of the EU Dual-use Regulation.

A limited number of universities and research institutes in Europe have internal compliance programmes or guidelines/codes of conduct. These include entities in the UK (for example Cambridge University) and Germany (for example the Leibnitz institute DSMZ). King's College London and the Association of University Legal Practitioners have drawn up guidance for academia (2015). In addition, codes of conduct have been developed in a number of research communities. However, it appears that awareness across the EU is still low, and the number of dual-use export license applications from academic and research bodies is likely very small across the EU. The precise number would be an interesting question for licensing authorities to explore and compare.

ITT present special enforcement challenges, because, like brokering, they are unlikely to be detected through border customs procedures and are not subject to the normal border controls that apply to tangible exports. Detecting this type of unlicensed transfer will require information (for example, a voluntary disclosure by the company), intelligence about the offence or audit methods. The latter involve specialized electronic data processing auditors, which in turn requires training and resources. Good compliance procedures within the companies who produce or have access to controlled dual-use technology are essential to prevention.

2.4 Legal clarifications and amendments

According to the Commission Communication, legal concepts and definitions that may be revised include: the notion of export and exporter; determination of the competent authority (especially for non-EU companies); the control of technical assistance; ITT controls; transit and brokering provisions; and extraterritorial provisions for EU persons (to prevent circumvention).

Currently the core concepts of the Dual-use Regulation are those of **export** and **exporter**. While brokering and **transit** controls have been made possible through the 2009 amendments to the Regulation, the precise nature and responsibility of the 'transiter' is not defined in the EU Dual-use Regulation. This is relevant given the complexity of the supply chain and of both legal and illegal dual-use transactions. The transport sector, which one of its representatives has called the 'forgotten piece of export control regulations'[32], deserves a stronger focus, which may involve both the clarification of legal responsibility and the design of appropriate compliance guidelines and tools. However, clarification does not necessarily involve an increased legal responsibility. Rather, this issue could also be addressed through a combination of increased awareness-raising measures and of provisions in national penal law. For example, where any actor in the supply chain supports, facilitates or contributes to an illegal export with intent, this could be made subject to criminal penalties. Appropriate wording across the EU Member States could thus capture the full range of the supply chain. At the same time, exporters may be concerned they could be held accountable for freight forwarders falsely declaring dual-use items due to a lack of awareness (they don't know about dual-use issues), competence (they are aware but make mistakes or have insufficient knowledge of the right customs codes or procedures) or due diligence (they don't care).

Today's complex trading environment encompasses a wide range of supply chain actors, including integrators, shipping lines (from ocean liners to smaller shipping companies that may be subcontracted by larger carriers), shipping agents, freight forwarders and customs agents, as well as air carriers, road transport, fast parcel operators and postal services, brokers, and even insurance companies and financial institutions. Some of these terms and associated activities overlap, and are understood differently in different countries and communities, but tend to relate to different functions and degrees of responsibility. These actors are usually neither commodity owners nor the exporter, and therefore tend to have very little or no information about the products they transport or trade. While the enforcement of export control is the main focus of most EU Member States, transit may be the main risk in some EU countries.

In this context, there is also a need to resolve the differences of terminology between the Dual-use Regulation and the EU Customs Code regarding transit, as this has led to confusion.[33] Even internationally, there is no agreed definition of the terms transit and transhipment.

Technical assistance is generally defined as manual services and the oral transfer of know-how, but also a term without an internationally agreed definition. Such technical assistance falls within the scope of ITT, but is legally distinct in the EU due to a decision that it constitutes services involving the cross-border movement of persons and thus considered outside the scope of the EU Dual-use Regulation. Instead, it

---

[32] Email communication of June 2015.
[33] The Union Customs Code entered into force in 2013 (Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, OJ L69, 10.10.2013, p.1), replacing the 2008 Community Customs Code (OJ L 145, 4.6.2008, p.1). Its substantive provisions are applicable only from 1 May 2016, once the corresponding Commission acts are in force. See URL
<http://ec.europa.eu/taxation_customs/customs/customs_code/union_customs_code/index_en.htm>.

was covered by a Joint Action of 2000 (2000/401/CFSP), which provides for controls of technical assistance through a prohibition or an authorisation requirement. This applies where such assistance is provided by a legal or natural EU person outside the EU and 'is intended, or the provider is aware that it is intended, for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons' (OJ L159, 30.6.2000, pp. 216-217). Most but not all Member States have implemented corresponding provisions in national law. Technical assistance is therefore another element that requires consideration as to how to enhance convergence between the different elements of the EU export control regime (see section 5.1.3 below). Moreover, in the context of EU restrictive measures (regarding Iran, North Korea and Syria), technical assistance measures have been included in a number of Council decisions and Council regulations, together with controls on a range of activities involving dual-use items as well as financial sanctions. This therefore raises two questions: is technical assistance within Community competence, which the European Court of Justice would need to clarify and second, what legal possibilities exist to encourage or oblige all Member States to implement a Joint Action that dates from 15 years ago.

While enforcing **extraterritorial provisions** for EU persons naturally poses challenges in terms of both detection and investigation/prosecution, such controls are considered important as a preventive and deterrent measure, and to enable legal action should evidence emerge that an EU person is involved in a WMD programme abroad or brokering dual-use items for WMD end-use abroad. Extraterritorial provisions are already included in the Joint Action on technical assistance, but if and how they are implemented and subject to penalties differs substantially across the EU.

Regarding dual-use **brokering**, the current regulation covers transactions between two or more non-EU countries facilitated by a person established within the EU if the items concerned are or may be intended for a WMD end-use, and the brokering activities takes place from EU territory. If the items are located in the EU and exported from there, export control provisions apply rather than brokering controls, in order to avoid double regulation. In the dual-use area, arranging transactions is normal business practice for companies that operate internationally. Some Member States have additional extraterritorial provisions in specified cases if the brokering activities take place outside of EU territory, which may be considered as an EU-wide provision.

3 Promoting export control convergence and a global level-playing field

3.1 Licensing architecture

The Commission Communication considers: guidelines for consistent licensing practices (e.g. best practices for processing times); reviewing parameters for existing EUGEAs; introducing additional EUGEAs, e.g. for low-value shipments; encryption; intra-company technology transfers for R&D (see also section 2.3 on ITT); intra-EU transfers of Annex IV items in large projects; regular review of National General Export Authorisations (NGEAs) and discussing possible transformation into EUGAEs; standardised IT support tools and electronic licensing systems across the EU; and emphasis on end-use monitoring.

While it may not be possible for licensing authorities to commit to a pre-determined timeline for all licensing decisions, **processing times** rather than denials appear to be the main concern of dual-use exporting companies. There is scope to optimise routine licensing processes in some EU countries through more staff resources, more frequent decision-making opportunities where inter-agency

committees take decisions and/or electronic or otherwise swifter procedures. Agreed targets or guidelines for routine cases and a formal obligation to have sufficient staff to meet those could assist licensing authorities in mobilising sufficient resource from their national or institutional budget. There also seem to be substantial differences in the situations in which national authorities use individual, global or national general licences. This has considerable impact on compliance costs and processing times.

To enable a focus on the most sensitive transactions, routine and non-sensitive transactions should be dealt with in a way that involves as little administrative capacity and delays as possible. The European Commission is therefore considering additional EUGEAs and modifying the conditions of existing ones. While those reforms would generally be favourable for companies, the benefits of a given type of general licence for a company depend on the type of dual-use items exported, the specifics of the sector and trading patterns (e.g. high value or low value shipments, products with a short shelf life, frequent exports to the same customer or occasional one-off shipments, regular supplies of spare parts), as the use of such licences nevertheless requires keeping track of shipments and following notification procedures. Generally it can be said that measures that facilitate non-sensitive export enable companies and authorities to focus on potentially sensitive transactions. However, authorities will almost certainly voice concerns about certain facilitation measures. For example, the commercial value of an item may be disproportionate to its utility for a WMD programme. In fact, whether a shipment has high or low value is irrelevant from a non-proliferation perspective. Facilitation measures could also be used for fraudulent shipments. One way forward would be to explore less sensitive destinations and products that could benefit from facilitated export procedures, combined with (more onerous) record-keeping requirements and company audits (see section 6.2 below).

End-user monitoring or verification could also be a way to increase certainty over the final end-use. This however, will have resource implications for authorities, as existing embassy staff will usually have no dual-use expertise. Moreover, the legal status of such 'verifiers' would need to be clarified, and related international legal questions be addressed. Unless contracts between companies foresee such checks and bilateral or international agreements are in place that create a legal basis for government representatives from foreign countries to conduct end-use checks, this will be very difficult to put into practice. Lessons could be drawn from the US 'blue lantern' programme for end-use monitoring.

Electronic licensing systems for submission and processing of license applications are in place in many European countries, and while the necessity to establish such a system may be dependent on a country's size and dual-use export volume, it is imperative that any given system be compatible with the customs risk management system. It should also enable dual communication and thus automatic checking whether the licence number provided is valid, and if authorised volumes have been reached or exceeded. Moreover, as all electronic systems, IT security is a key issue, not only for governments but also for industry that provides a wealth of commercially sensitive data in licence applications. Finally, substantial investments in IT maintenance are required.

3.2   Outreach, cooperation and assistance to partner countries and dialogue with key trading partners

International capacity-building (in the EU context often referred to as outreach) not only contributes to international security but also to international convergence and thus to levelling the playing field. It has also contributed to international and EU-internal exchange of information, experience and practices. EU-internal capacity-building (in-reach) and outreach are thus mutually reinforcing, and both are essential for effective and credible EU dual-use export controls. The EU explicitly acknowledged the need for international cooperation to prevent and combat WMD proliferation in 2003, when it introduced a range of measures to strengthen its approach to security in general and WMD proliferation in particular. The EU

WMD Strategy states the EU's commitment to 'strengthen export control policies and practices within its borders and beyond, in co-ordination with partners' (Council of the EU, 2003). The establishment of export control systems can also open up new markets to foreign investment and technology transfers.

The expansion of items, activities and actors subject to some form of control also means that not only producer countries are required to put control systems in place, but also importers, transit and transhipment countries, which are potential diversion points. Therefore, international cooperation and capacity-building can also enhance the effectiveness of controls, especially since the supply-side control approach is increasingly undermined by wider foreign availability of technology, which puts certain controls into question and regularly leads to deregulation of controls.

Since 2005 the EU has developed the world's second biggest dual-use trade control capacity-building programme, after that of the USA, now involving countries not only in Europe but also in Africa, Asia and the Middle East. To date, the EU programme, Cooperation in Dual-use Export Control, has been implemented by the German export licensing authority, the Federal Office of Economic Affairs and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle, BAFA), with a pool of legal, licensing, industry outreach and enforcement practitioners drawn from Member States across the EU. The successor programme will be managed by a French-led consortium. The EU programme started with a pilot project initiated by the European Parliament in 2004. Since this first pilot project, implemented by SIPRI in 2005–2006, cooperation has expanded from 4 to nearly 30 countries. In 2006 the EU created the Instrument for Stability (IFS), which allocated at least €14 million specifically to dual-use export control capacity building for the period 2007–13.

The EU has thus played a leading role in international dual-use export control capacity-building. However, resource constraints among EU Member States' licensing and enforcement officers and specialised legal and technical experts also limited the resources available to participate in international activities, be it through receiving delegations in-country or traveling abroad. Effective capacity-building requires including international cooperation and capacity building as part of the core tasks of enforcement officers and other export control practitioners. Such exchanges moreover contribute to internal capacity-building as mutual learning is invariably an element of all international cooperation (Bauer, 2013a).

The declared purpose of the review action to develop **export control dialogues with key trading partners** is to avoid 'conflicting regulatory requirements' and to reduce the 'administrative burden on export-oriented industries'. This in fact overlaps with outreach and assistance, since some trading partners may also be partner countries in EU-funded capacity-building programmes. Moreover, whether joint activities are called outreach, cooperation, assistance or dialogue often only reflects the nature of the funding source but not the substance of the meeting. Ideally, each assistance activity should be conducted in a cooperative manner, and involve dialogue and mutual learning among participants and peers (Bauer, 2013a).

Such EU dialogues could also address differences in terminology that continue to create confusion and therefore variations in interpretation and implementation, for example regarding definitions of terms such as brokering, transit, trans-shipment and items vs. goods. At the same time, as export controls continue to be implemented by Member States, EU dialogues will be in addition to bilateral export control dialogues, which have a complementary function.

3.3   Promoting global convergence

While difficult to achieve, global convergence remains a key objective, motivated both by security and economic interests. The definition of items, activities and actors subject to controls differs across the globe. The area in which convergence among suppliers has probably come the farthest is the list of items subject to control, through inclusion of common lists in some dual-use related UN sanctions, and through the adoption of lists negotiated in the international export control regimes and consolidated into the EU list structure which has – in turn – been adopted by an increasing number of countries, including in Asia. Moreover, UN Security Council resolutions 1718 and 1737 incorporate the then-control list of the Missile Technology Control Regime (MTCR) and the Nuclear Suppliers Group (NSG) and thus made them binding on all UN Member States with regard to transfers to Iran and North Korea.

The Commission Communication proposes the promotion of coherent, comprehensive, unified **EU representation in the regimes**. Not all EU Member States are represented in all export control regimes, in particular the MTCR. However, since accession to these regimes requires consensus, which has not been achieved to date, this is a political decision outside of the scope of the EU dual-use export control policy review. The review action also relates to a second aspect which is partly internal to the EU (and highly political) and partly dependent on the views of other regime participants: the representation of the EU as a distinct body in addition to Member States, or statements on behalf of the Member States by the EU.

The issue of global convergence cannot be discussed without reference to UN Security Council resolutions, especially in the light of global supply chains. UN Security Council resolution 1540 (2004) includes a requirement for export, brokering, transit and transhipment controls for WMD relevant items, although it contains no definition of these terms. States are obliged to:

> *'Establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export and controls on providing funds and services related to such export and trans-shipment such as financing, and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations'.*

For the purposes of the resolution, related materials are defined as 'materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery'. Additionally, a number of resolutions imposing trade control obligations on UN Member States have been adopted since then, targeting specific countries. Resolutions 1695 and 1718 adopted by the UN Security Council in July and October 2006, respectively, inter alia impose restrictions on missile and nuclear weapon-relevant transfers to, or involving, North Korea. UNSCR 1718 calls upon all Member States 'to take, in accordance with their national authorities and legislation, and consistent with international law, cooperative action including through inspection of cargo to and from the DPRK, as necessary'. Resolutions 1874 (2009) and 2094 (2013) expand on these obligations and give UN Member States broader powers to inspect suspicious cargo in transit to and from North Korea.

Resolutions 1737 (2006), 1747 (2007) and 1803 (2008) include embargoes on missile and nuclear weapon-relevant activities involving Iran. In enforcing these UN Security Council resolutions, the EU has adopted additional sanctions against Iran, in particular through Council Decision of 26 July 2010 (OJ L195, 27.7.2010); and the following Council Regulations: No. 961/2010 of 25 October 2010 (OJ L281, 27.10 2010); No. 359/2011 of 12 April 2011 (OJ L100, 14.4.2011); and No. 267/2012 of 23 March 2012 (OJ L88, 24.3.2010). (Sanctions against Iran are being modified or lifted as this study is drafted.)

UNSCR 1737 requires states to 'take the necessary measures to prevent the supply, sale or transfer directly or indirectly from their territories', which can be interpreted to include transit and transhipment. UNSCR 1929 expands upon these obligations and 'calls upon' states to 'inspect, in accordance with their national authorities and legislation and consistent with international law (…), all cargo to and from Iran, in their territory, including seaports and airports, if the state concerned has information that provides reasonable grounds to believe the cargo contains items the supply, sale, transfer, or export of which is prohibited' under the provision of the resolution.

4 'Develop an effective and competitive EU export control regime'

While there is one common legal basis for export controls on dual-use items in the EU, there are 28 different implementation and enforcement systems and approaches. This poses particular challenges through different application and interpretation, but also creates opportunities through the possibility to adjust systems to particular national factors such as the industrial structure, geographical location and volume of exports. The goal of a level playing field for business in the EU and internationally is often referred to. While impossible to fully achieve, the impact on fair competition is still an important element when assessing reform proposals. EU-wide legal requirements for international compliance programmes (ICPs), further discussed below, are also relevant from the aspect of fair competition and the ideal of creating a level playing field in the EU.

Already in 2004 the EU conducted a peer review of the dual-use export control systems of EU Member States and acceding countries. Discussions were structured around 20 issues relevant to licensing, enforcement, industry awareness and the control of technical assistance. The peer review revealed a number of discrepancies in interpretation, implementation and enforcement between national systems. Based on national and cluster reports, the peer review task force produced a report and recommendations for future action. The General Affairs and External Relations Council (GAERC) of December 2004 decided that these recommendations should be acted on without delay (Council of the EU, 2004). In order to 'further improve EU export controls and thereby enhance Member States' capabilities to prevent access by undesirable end-users, including terrorists in third countries, to dual-use items relevant for WMD purposes', it was decided that actions should be taken inter alia to:

- minimise any significant divergence in practices amongst Member States;
- investigate the possibilities for adding controls on transit and transhipment;
- provide assistance in recognition of dual-use items subject to control;
- improve exchanges of information on denials, and consider the creation of a data base to exchange sensitive information;
- agree best practices for the enforcement of controls;
- improve transparency to facilitate harmonisation of implementation of controls on nonlisted items (catch-all);
- enhance interaction with exporters; and
- agree best practices for controlling intangible transfers of technology.

While some of these recommendations were followed up, a number or recommendations were not acted on sufficiently, in particular those related to enforcement. This is also evident from the fact that they were taken up again in the current review process. A follow-up peer review process incorporating the then-27 Member States was initiated in 2010. No peer review process dedicated to enforcement issues has been

initiated to date, but would certainly be useful in light of the need to create a forum for enforcement practitioners and to enhance information exchange, cooperation and coordination (see section 5.1).

4.1　Common risk management framework

A common risk management framework, which in the Commission Communication is discussed under the heading of effectiveness and competitiveness, is also directly relevant for the EU contribution to international security (Priority 1). Risk management for dual-use items is conducted both by licensing authorities (in the licensing process) and by customs (in the transit and export process).

The proposed development of common risk management tools and framework is in progress in the relevant **customs** working groups, but to become a reality requires a further increase in trust and information sharing. Joint operations and enhanced information sharing are also proposed in the Commission Communication. One complication is that these areas fall under DG TAXUD not DG Trade. This in turns reflects the situation in EU Member States, where customs (and not the licensing authority) is responsible for customs risk management, since it relates to enforcement.

The risk is that any of the provisions set out in the Dual-use Regulation is evaded or breached. Given the complex nature of dual-use export controls, it is not uncommon for exporters to be unaware that their goods need an export licence. Potential breaches of the controls can be separated into two broad categories: those that occur due to ignorance, lack of knowledge, understanding or awareness of dual-use trade controls; and those that occur as a result of deliberate evasion of trade controls. Although the potential harm caused by either category could be the same, the way to address them will differ. For example, outreach to industry and other stakeholders and other transparency measures (further discussed in section 5.2 below) is an effective way to reduce the risk of inadvertent breaches, whereas effective enforcement, including penalties may be necessary for deliberate breaches.

In April 2005 the EU introduced the 'safety and security' amendments to the Community Customs Code. These have three main elements. First, the status of Authorized Economic Operator (AEO) was created, which is available to those economic operators who meet strict compliance requirements in securing their supply chains (see also section 5.2). In return, these operators should benefit from the EU-wide recognition of their AEO status, including fewer customs checks and faster freight clearance at the border. Second, a common risk management framework was established intended to ensure greater consistency in the identification of illegal trade across the EU, as well as harmonised treatment of AEOs. Third, a requirement for advance electronic notification of the arrival and departure of goods at the EU frontier was introduced to support automated security and safety risk analysis prior to arrival and departure of goods and implementation of the EU risk management framework. While the initial driver behind these amendments was internal security/terrorism concerns, they also include other international security related risks (Anthony and Bauer, pp. 789-790).

Following the amendments to the Code, DG TAXUD and the Member States launched various legal measures and IT projects to implement these new requirements. There have also been a series of meetings on common risk management, led by the DG TAXUD. As a result, common risk criteria for entry (including transit) and export (including transhipment) were agreed.

The Community Customs Code creates a legal obligation to exchange security and safety related information between the Customs authorities in the EU in order to avoid diversion of illegal trade to other EU Member States. The exchange of risk related information is managed through the electronic EU Customs Risk Management System (CRMS), which enables Customs administrations to communicate identified risks to all EU Member States.

However, customs authorities can only share the information they own, not classified information they received from other services. In those cases, Member States can therefore be assumed to use bilateral

rather than EU-wide channels of communication. This may create gaps and opportunities for illegal exports of dual-use goods through those Member States that are not aware of the risks that have been identified in other Member States. At the same time, while a common risk strategy will enhance the effectiveness of the EU-wide regime, risks still need to be tailored to and prioritised at national level, reflecting trade flows, procurement patterns and industrial structures in the individual countries.

A common risk assessment in the **licensing** procedure is not currently considered, although such assessments have been discussed on an ad hoc basis. National interpretations and applications of Article 12 of the Dual-use Regulation vary considerably. A broader obstacle is rooted in the fact that export controls are also a reflection of states' foreign and security policy interests. Hence, harmonised export controls require fully harmonised foreign and security policy interests among EU Member States, which at present is not the case. Moreover, the outcome of risk assessments and acceptability of certain risks thresholds will also vary between countries and depend on a range of political and other factors.

In addition to common criteria, a common risk management would require common information on which to base decisions. Information essential to licensing decisions does not only consist of technical considerations related to the items, but also information about the end-user. Information exchange on end-users is currently limited to denials. Other end-user related information usually is based on intelligence information, which often neither customs nor licensing authorities are allowed to share. A common risk management framework in the EU therefore is not possible without closer cooperation and information exchange between intelligence agencies on the subject of dual-use trade controls.

4.2   Convergence of catch-all controls

Catch-all controls are also referred to as end-use controls (in particular in the UK) or controls for unlisted items. It is important to keep in mind that both listed and non-listed items can qualify as dual-use items, although they are controlled through different legal mechanisms. The basic principle is that, contrary to controls for listed items, non-listed items are not controlled based on their technical characteristics/parameters, but on their suspected or known end-use. This means (again contrary to the concept for listed items) that the same item may be subject to control for export to one country, but not another country, or even for one end-user in the same country but not a different end-user.

Catch-all controls of unlisted items were introduced to focus on the end-use of items, whether of old or new technology. For example, it became known that missile and nuclear weapon programmes specifically sought to obtain items just below the technical parameters of the control list to avoid control requirements. Catch-all mechanisms also help keep up with technological developments without impeding legitimate trade while enabling the prevention of dual-use items to sensitive end-users.

The way in which the catch-all provisions of the EU Dual-use Regulation are interpreted and applied across the EU varies substantially. This has led to concerns regarding distortion of competition within the EU, as well as the effectiveness of controls – for example, where the same item is subject to control (and likely denied the export if destined for certain countries) in one EU Member State, while it can be freely exported from another EU Member State. However, it is not clear whether this has actually been an issue exploited by those seeking to procure for WMD programmes, and thus whether it in fact poses a substantial security risk.

While many issues and challenges related to catch-all implementation are not EU-specific, but faced by governments and companies around the world, some aspects are unique to the EU common market context as they raise questions about fair competition and uniformity of application across the territory. This variance may be due to different access to intelligence information or risk assessments. This situation also raises issues regarding clarity and predictability for exporters, although this is a broader issue also applicable to listed items. Member States may take different licensing decisions for essentially identical

exports, or they may classify items differently, either as a listed or non-listed dual-use item, or as a dual-use or a military item. The latter has led to industry demands to make **common interpretations** of the control list mandatory.

The European Commission's proposal to 'harmonise the notion of catch-all controls across the EU' is an obvious one, therefore. How to do this in practice is less straightforward. A first step could be a common interpretation of the way the catch-all is translated into procedures and information is communicated to companies – formally or informally, and how narrow or wide the imposed licensing requirement is formulated. First, a catch-all may be published and apply to all producers of the same product, or only be delivered to a specific company. Second, it may apply to a whole destination country or only to a specified end-user. Third, it may be delivered in response to a shipment being stopped by customs, who request the company to apply for a licence with the competent authority, or the company may be notified in response to intelligence information, whether or not it was intending or attempting to export a certain product.

A second step would be increased information exchange through a catch-all database. Currently denials are exchanged, but not notifications. The Commission proposal to partly make catch-all information public will therefore need to be reviewed in light of this, as the sharing of information between Member States in some cases is already considered (too) sensitive. Moreover, the amount of information to be exchanged as a result is important, as are the consequences of receiving the information and next steps to take. A country may issue few catch-all notifications, based on rather certain information about a potential WMD end-use and thus normally result in a denial and entry of the information into the customs risk management system. If this country receives many notifications from a Member State that uses this tool as a precautionary measure for transactions that would in most cases not be denied, this could be confusing and result in unnecessary delays and controls.

A third element would be a reinforced consultation process in case of notified denials.

4.3 Intra-EU transfer of Annex IV items

The options proposed by the European Commission are a review of Annex IV to update the list and reduce it to the most sensitive items, and to introduce an EUGEA for intra-EU transfers. This would include technology transfers and be combined with post-shipment verification. Free intra-Community transfer of Annex IV items has been a demand notably from nuclear companies, who are most affected by these provisions. A review of Annex IV and its reduction to the most sensitive items seems uncontroversial. Concerns may be raised either in connection with international requirements on nuclear controls, notably those imposed by the IAEA, and by suppliers (such as the USA) that prefer to make decisions on the eligibility of certain EU Member States for certain transfers rather than treating the EU as one recipient. This is illustrated by the fact that the USA has excluded some EU Member States from certain export facilitation measures.

5 'Support effective and consistent export control implementation & enforcement'

This issue overlaps with the previous section in as far as effective export control implementation and enforcement is what an effective EU export control system is about, and competitiveness is also linked to consistency across the EU. However, while Priority 3 is aimed at creating a level playing field within the EU, Priority 4 is focused more on enabling practical implementation both by the authorities and by the private sector.

5.1 EU Export Control Network

Under the heading of developing an export control network in the EU, the Commission proposes a range of measures to: enhance the scope and depth of information exchange, both electronically and in person; strengthen cooperation between export control practitioners in the EU; and build capacity. It also raises the issue of enhanced consistency between the different export control related instruments and competencies in the EU and in the Member States. In fact, this priority probably has the most elaborate and detailed set of proposals.

5.1.1 Enhance information exchange and develop IT infrastructure

The Commission Communication proposes enhanced information exchange on licensing data and on other information (e.g. destinations, end-users, incidents and violations), and using the secure IT system DUeS for this purpose. It also proposes sharing information between and with enforcement agencies through an EU-wide information exchange system and developing standardised IT support tools and electronic licensing systems across the EU.

While substantial information is exchanged on denials, little information is publicly available or exchanged between Member States on dual-use licences granted or actual dual-use exports. In recent years, EU governments have begun exchanging some information on licences granted on an annual basis. These however are only broken down by the 10 categories of dual-use items, not more detailed control list categories, and moreover do not include actual exports. Figures on actual exports could possibly be derived from national customs databases. Whether this is possible, however, depends on a number of factors. Box 44 of the customs declaration (the Single Administrative Document SAD) is a multi-purpose field, which inter alia is used to declare that a dual-use licence is required for a given export (coded as X002). Whether the information in the databases can in fact be searched to identify dual-use exports depends on whether Box 44 is broken down into different sub-fields in the electronic customs system, including a dedicated box for X002. Correct sharing of this information also requires correct usage of the box by the exporter. Box 44 as a free text box is likely to be particularly prone to mistakes. Finally, whether national customs authorities are allowed to share this information with other national authorities or the European Commission may depend on fiscal secret and commercial confidentiality provisions. Lastly, with every information exchange it is essential that it serves a purpose and does not become an end in itself, since this may lead to information overload and strain on already limited capacities and resources. The question of who would actually use certain information should always be posed.

There is no systematic information exchange at present on sensitive destinations, end-users, incidents or violations. Incidents could include detections or interceptions of suspected violations, or transit shipments that are sent back because of a change of the declared destination, while violations could include investigated or prosecuted violations, which may result in compound penalties, administrative or criminal penalties if they result in a conviction. Importantly, this information exchange requires the

involvement of intelligence services, since customs authorities usually are not allowed to share classified information from their own or other countries' intelligence services with other customs agencies. These issues will need to be considered when exploring what information should be shared through DUeS, the EU's secure IT system for sharing information on dual-use export issues, and when setting up an electronic system for sharing information within and between enforcement authorities. Finally, in setting up intergovernmental information exchange mechanisms, it is important to keep in mind that the allocation of enforcement functions for dual-use export control varies substantially across the EU. While customs is commonly in charge of detection, auditing may also be dealt with by licensing authorities, or jointly with licensing authorities (or no dual-use specific audits may be in place). Police, intelligence, dedicated customs units or general investigation units may be responsible for investigations, depending on the EU Member State.

Many, but not all EU Member States, have electronic licensing systems. Many companies (especially larger ones) favour these over paper-based systems. Importantly, such systems must be compatible with electronic customs risk management systems. It also has to be kept in mind that they result in substantial IT maintenance costs for both administrations and industry.

5.1.2   Enhance strategic and operational cooperation with enforcement agencies

The Commission Communication proposes the integration of export control priorities in policy cycles; developing common risk management tools and framework; implementing joint operations; and enhancing the enforcement of transit and brokering provisions.

Article 24 of the Dual-use Regulation states that 'each Member State shall take appropriate measures to ensure proper enforcement of all the provisions of this Regulation'. It is striking that there is no dedicated EU forum for enforcement officers on dual-use issues. Rather, such sharing has taken place in multilateral regime meetings, on the fringes of seminars, and at technical assistance and cooperation missions to third countries.

Article 23 of the Dual-use Regulation provides for a Cooperation Group 'to examine any question concerning the application of this Regulation which may be raised either by the chair or by a representative of a Member State'. While there is thus a formal mechanism that could be used to share enforcement experience between Member States and across the EU, the meetings are usually attended by licensing officers, and enforcement officers are rarely included in the delegations. This may reflect (a) the chair of the group being DG Trade rather than DG TAXUD or DG HOME; (b) the agenda of the meetings; and (c) national budgetary priorities, since in principle only one delegate per Member State is funded by the EU (although some additional experts can be invited). Article 23 says that a 'Dual-Use Coordination Group chaired by a representative of the Commission shall be set up', and that 'each Member State shall appoint a representative to this Group'. A first joint meeting between customs and licensing authorities was organised by the Commission (TRADE and TAXUD) in September 2010. While some follow-up activity took place, this initiative has not been continued or institutionalised.

In EU Member States, the different enforcement functions of customs controls, risk management, company audits, and investigations and prosecutions might be divided between three or four different agencies such as customs or police. Also, depending on the size of the country and the organisation of the enforcement agencies, some or all of these functions may also be combined within one agency. The gathering of peers and functional counterparts and information sharing with and between enforcement agencies therefore requires understanding the institutional structures and allocation of responsibilities at the national level.

To involve all actors implementing and enforcing EU dual-use trade controls, this must involve not only cooperation of licensing authorities with enforcement agencies, but also among enforcement agencies.

There are regular EU meetings of dual-use licensing officers, but no systematic meetings of customs and other enforcement officers to discuss issues such as auditing, prevention/awareness-raising, and the detection, investigation and prosecution of EU export control offences. Currently, if at all, they meet at the export control regimes, international capacity-building events or US funded meetings. Regular meetings for enforcement officers, as well as joint meetings for licensing and enforcement officers, would substantially enhance the effectiveness of dual-use export controls in the EU through enabling and facilitating the exchange of information, experience and good practices. They would also enable the building and strengthening of both formal and informal networks that can be utilised when meeting daily enforcement challenges, which by definition have an international dimension and at times involve more than two EU Member States.

It is evident that a dedicated EU forum for enforcement officials on strategic trade controls would substantially enhance the effectiveness and coherence of the EU dual-use export control policy system. It would need to include all enforcement functions—prevention, risk analysis and profiling, detection, investigation and prosecution—but would provide opportunities to meet and exchange experience, good practice, information etc. This could be implemented in a number of ways: in parallel with the Dual-Use Working Party (with an option of joint meetings) or as a subgroup of the Customs Cooperation Group, for example. In such a forum functional counterparts would meet, and points of contact for individual enforcement functions would be identified. This solution would also address two challenges: language barriers, as interpretation is provided for official EU meetings; and shortage of resources, as lack of travel funds would no longer prevent enforcement officers from attending meetings. Since there are a number of different enforcement tasks, it would also be suitable to have both joint meetings and dedicated sessions for specific enforcement functions. There could also be sessions on specific topics such as the implementation of restrictive measures that involve different governmental entities, partly but not fully overlapping with those implementing export controls.

As a second step, **joint operations and exercises** could be developed, building on a joint exercise conducted in 2009, and more recently a table-top exercise conducted in 2014.[34] Lessons learned from a global exercise coordinated by the World Customs Organisations (WCO) on strategic trade controls could also feed into this process. Again, funding will need to be secured to enable implementation. This is essential to enable participation from all 28 Member States, given that not even those EU countries with a substantial number of dedicated dual-use enforcement staff are likely to have travel funds and budgets for joint exercises at their disposal.

The proposal to '**integrate export control priorities in policy cycles**' is an opportunity to highlight the importance of both top-level policy and mid-level management priorities for effective implementation and enforcement. The allocation of resources to dual-use export control enforcement varies substantially across the EU. More generally, the focus of customs has traditionally been on revenue collection and thus import control, not export control; and enforcement targets are often developed for cigarettes and drugs, but rarely on dual-use items, be it to enforce the dual-use regulation or other restrictive measures. Similarly, the focus of DG TAXUD has been on revenue collection and import control, but not on export control and international security issues.

More generally, there is a lack of awareness of enforcement-specific issues and challenges at the policy level across the EU. This is a critical shortcoming, as policy discussions need to be informed by an on-the-

---

[34]   See   <https://export-control.jrc.ec.europa.eu/News-Events/Conferences/Articles/ArtMID/525/ArticleID/234/Pilot-Export-Control-Simulation-Exercise-for-European-Union-EU-Customs-and-Licensing-Authorities>.

ground perspective so that policy decisions are taken with a clear picture of their implications for staff and financial resources, implementing procedures, institutional structures, laws, etc.

Transit and transhipment controls have increasingly become accepted as an essential component of strategic trade controls. This trend has been reinforced by UN Security Council resolution 1540 of 2004, which made transit and transhipment controls for WMD-relevant items mandatory for all states. A number of other proliferation-related UN Security Council resolutions also require transit and transhipment controls for effective implementation. However, there are no standardised international definitions for these terms.[35]

In the EU Dual-use Regulation, transit is defined as the 'transport of non-Community dual-use items entering and passing through the customs territory of the Community with a destination outside the Community'. Transhipment, which is commonly understood to involve a change of means of transport, is not separately defined but understood as a sub-category of transit. Article 6 (1) provides that the transit of items contained in Annex I 'may be prohibited' if the items 'are or may be intended, in their entirety or in part' 'for proliferation of weapons of mass destruction or of their means of delivery'. It also explains that 'Before deciding whether or not to prohibit a transit' a Member State may impose an authorization requirement for the specific transit of a listed dual-use item. Member States may extend this provision to items not contained in the control list ('non-listed items'), not only in cases of a possible WMD end-use, but also to dual-use items for military end-use and destinations subject to an EU embargo.[36] The Regulation also includes an information exchange and consultation mechanism intended to prevent undercuts and differences in application. The EU Customs Code contains different definitions and provisions regulating transit and does not define transhipment either (Council Regulation (EEC) No. 2913/92, OJ L302, 19.10.1992, as amended).[37] Additionally, some EU Member States, such as Belgium, Poland and the UK, have specific national provisions defining and regulating transit, over and above the possible extensions to unlisted items and military end-use in the embargoed destination.

While enhanced enforcement of transit is important, it faces a number of practical challenges. These include:

- different ways in which the provisions are interpreted and implemented across the EU;

- a different definition of 'transit' in the EU Customs Code, which has led to confusion;

- often either insufficient information available on transit (substantially less than for export), or information that is not available to the right person at the right time;

- since transit/transhipment controls are often, or even mostly, intelligence based, the question of how the validity and credibility of the information can be assessed;

- technical reach-back, i.e. how to access technical expertise swiftly and possibly also during 'out of office hours'?;

- who is bearing the financial and the political costs when shipments are held up?;

---

[35] The 'International Convention on the Simplification and Harmonisation of Customs Procedures' (Revised Kyoto Convention) is the only international Convention that contains a definition of the terms transit and transhipment in its Specific Annex E. However, since the Special Annexes have only been ratified by a very small number of states, this can hardly be considered as a consensus international definition. See the WCO website <http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/conventions/pf_revised_kyoto_conv/instruments.aspx>.

[36] This only relates to EU embargoes that are formalised by a CFSP instrument, and therefore excludes the China embargo from 1989.

[37] See <http://ec.europa.eu/taxation_customs/customs/ procedural_aspects/transit/common_community/index_en.htm>.

- are customs officers sufficiently aware to be able to act upon suspicious activity, and are there specialised staff to support them?;

- how to conduct effective risk management without unnecessarily impeding trade, in particular given the narrow time window?;

- what can be done once the shipment has departed?; and

- are the legal powers of the relevant state authorities sufficient to implement national and international requirements?

Moreover, the horizontal nature of dual-use export controls and resulting cross-institutional competences also come into play here. Enforcement generally does not fall under the competence of licensing authorities but a range of authorities ranging from ministries of finance (customs) to ministries of interior (police, border police and intelligence services). Similarly, customs enforcement matters are usually discussed in the institutional context of TAXUD and customs cooperation within the EU (not within working groups under DG Trade), while judicial enforcement (investigation and prosecution) of dual-use export control offences could be discussed in the context of DG Home or working groups on investigation and judicial matters (but are not currently).

To conclude, export control is a cross-cutting issue that involves the coordination and cooperation of many actors. On this issue in particular, close coordination and integration of dual-use export control enforcement into existing efforts to develop and implement a common risk management across the EU is required.

Enhanced enforcement of brokering provisions faces different challenges. Such activity is unlikely to be detected through regular customs work at the EU's external or internal borders. Detection will usually require information sharing and co-operation with foreign enforcement or intelligence agencies. Brokering offences may also be detected during company audits.

The Dual-use Regulation 428/2009, which introduced EU-wide brokering controls for dual-use items, defines brokering services as 'the negotiation or arrangement of transactions for the purchase, sale or supply of dual-use items from a third country to any other third country, or—the selling or buying of dual-use items that are located in third countries for their transfer to another third country'. A broker is defined as 'any natural or legal person or partnership resident or established in a Member State of the Community that carries out services defined under point 5 from the Community into the territory of a third country'.

Ancillary services (defined as 'transportation, financial services, insurance or re-insurance, or general advertising or promotion') are explicitly excluded. The legal end-use construction is also used for the control of brokering activities. Brokering of listed dual-use items requires an authorization if the broker has been informed by the competent authorities that the items in question are or may be intended for a WMD end-use. When aware that listed dual-use items are intended for a WMD end-use, the broker must notify the competent authorities. A common form for licensing is provided as an annex in the regulation. The exchange of information on denials and undercutting for export decisions also applies to brokering licences.

While a common legal approach applies across the EU, implementation and enforcement fall within national responsibility. Moreover, the EU Regulation offers the possibility for Member States to extend brokering services on a national basis. This includes the extension to non-listed items and military end-uses, and the possibility to impose an authorisation requirement if the exporter has grounds for suspecting a WMD end-use.

In the dual-use area, companies that operate internationally often arrange brokered transactions as part of their normal business practices. Therefore, the EU chose a broad definition with a narrow control mechanism, which can be applied where necessary. Its introduction also has an important awareness raising function.

5.1.3 Improved coherence between different EU institutions and Member States, and identification of synergies between security-related trade control instruments

This review action is motivated by seeking coherence between different elements of the complex EU export control regime, which is complicated by the horizontal nature of trade controls.

The EU export control regime includes a range of instruments and measures, including: EU restrictive measures; the anti-torture regulation; customs coordination on risk management; the Joint Action on technical assistance of 2000; and arguably also arms export controls.

Arms export controls overlap with dual-use export controls in a number of ways: notably regarding the assessment of export licence applications for conventional dual-use items. The EU Dual-use Regulation specifically refers to arms embargoes in connection with the catch-all for dual-use items destined for a military end-use in an embargoed destination, thus highlighting the connection. It also refers to the criteria developed for arms exports from the EU (Art. 12, see section 2.1 above). On a more practical/operational level, in many states the laws, administrative procedures, agencies and staff that are responsible for controlling transfers of dual-use items overlap with those for conventional arms and for the implementation of restrictive measures (sanctions). This is important for common risk management, cooperation and information exchange, as well as for internal and external capacity-building. Additionally, there are technical linkages as some categories of goods and technologies appear on both conventional and WMD control lists, and some conventional arms can also be used to deliver WMD. Some items, such as machine tools and lasers, have both conventional arms and WMD applications.

This highlights the challenge of the horizontal, cross-cutting nature of dual-use export controls, which involves different legal instruments, policy areas and institutional competencies, in Member States as well as in the EU institutions. Even within the European Commission, dual-use export control aspects are also relevant for a range of DGs in addition to DG Trade, including DG TAXUD, DG Research and DG Home.

Currently proposed amendments to the Regulation 'concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment' would broaden the scope of application of Regulation (EC) No 1236/2005 by extending the definition of 'torture' and 'other cruel, inhuman or degrading treatment or punishment' and by introducing the control of brokering and technical assistance, as has already been done for dual-use items in 2009. Different types of authorisations and assessment criteria have also been proposed, a number of them building on experience from the Dual-use Regulation.

While it is not necessary or feasible to integrate all security-related controls into the same legal instruments, it is essential that they are closely coordinated and that a common policy framework ensures their consistency and carrying across of lessons learned.

5.1.4 Capacity-building within the EU

The Commission Communication proposes training/capacity-building (EU-wide capacity-building programme and training for officials and further develop EU pool of experts)

Currently no dedicated EU funds are available for EU internal training and capacity-building in the area of dual-use export controls. Moreover, a number of EU licensing authorities in EU Member States had to implement or are currently facing budget cuts and reductions in personnel, even as the range and complexity of the issues being tackled by export controls is increasing. Training events, which also serve information exchange purposes between licensing and enforcement officers (see 2.1.2 above), currently take place with US funding. This is limited to the 13 most recent Member States, although other EU Member States participate as speakers, which creates a peculiar situation between EU peers who otherwise meet in EU working groups. At the same time, the EU funds international capacity-building, in which licensing and enforcement officers from across the 28 Member States participate as experts/speakers.

The European Commission proposes EU internal training and capacity-building, which could redress this situation. In-reach and increased interaction will also facilitate more harmonised implementation across the EU.

Meanwhile, while an in-reach programme is indispensable for the system's effectiveness, it has resource implications since it requires systematic funding and must include not only legal, technical and licensing expertise but also enforcement functions to be effective, across the range of prevention, auditing, detection, investigation and prosecution. A feasibility study on an in-reach programme was produced for the European Commission by the German Federal Office of Economic Affairs and Export Control (BAFA) in 2010, but a decision to establish and fund such a programme has yet to be taken (BAFA, 2010).

5.2 Private sector partnership

The Commission Communication proposes clear private sector compliance standards for use of simplified mechanisms as a 'substantial benefit' for 'reliable exporters' through guidelines; transparency and coordinated outreach through publication of reports/non-sensitive control information, including guidance on good compliance practices; and promoting convergence with the AEO programme.

While the term **industry outreach** is still commonly used by export control officials, today's technological and scientific reality means that non-industry actors, such as academia and research institutions, also 'export' controlled items, both in tangible as well as intangible forms. Outreach by export control authorities has to therefore extend to a wider range of stakeholders, and also include start-ups and 'garage companies' or 'do-it-yourself' individuals in the biological area. The precise range of relevant actors in a given country or region depends not only on the industrial, research and academic structures, but also on the geographical situation in relation to trade flows – e.g. landlocked countries versus transhipment hubs, or those with major airports. It is of crucial importance to communicate the rationale of export controls to all stakeholders, and to support their compliance efforts by incentivising compliance and providing tools. Key stakeholders in addition to exporters also include universities, research laboratories as well as a range of actors in the supply chain. Each of these types of actors has different compliance requirements.

Even on the production side, the dual-use industry comprises a very wide and diverse range of industry sectors including: 'energy, aerospace, defence and security, lasers and navigation, telecommunications, life sciences, chemical and pharmaceutical industries, manufacturing and material-processing equipment, electronics, semiconductor and computing industries' (European Commission, 2014b).

Within these sectors, the organisational structures, ways of conducing R&D, extent of collaborating with academia and research institutes, business models and levels of awareness regarding security issues vary substantially. For example, the chemical industry is a very large industry comprising sectors such as printing, textile, plastics, pharmaceutical, food and cosmetics. The biological sector includes pharmaceutical and biotech industries, waste management, diagnostic laboratories (hospitals), agricultural and veterinary facilities. Importantly, it thus includes public and private sector actors and a range of entities that are not the target of traditional industry outreach activities. The nuclear industry in the narrow sense is tightly controlled and subject to detailed security and safety regulations. However, nuclear-related dual-use items with applications in a nuclear weapons programme (such as certain aluminium alloys) are produced in a wide range of industry sectors, many of which have mostly non-nuclear and civilian end-uses.[38] Companies producing dual-use goods, software and technology with applications in missile programmes and UAVs that could be used as delivery systems, come from different sectors, such as defence manufacturers, space technology and machine tools. Controlled items include specialised machines such as filament winding machines and isostatic presses, materials such as graphite and carbon fibre, as well as maritime navigation equipment and systems such as gyroscopes and accelerometers. Conventional dual-use items are particular in as far as they are covered by the dual-use regime but fall outside the scope of WMD related policies. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies maintains two control lists: one for conventional arms, and one for related dual-use items.

International transfers of biological agents notably include the exchange of materials within and between public sectors. One aspect of the global disease surveillance system is the need for diagnostic and reference samples to be transferred between countries, regions and continents on a regular basis, which is fundamental in scientific exchanges. Furthermore, the biotech service industries may present an additional layer of complexity as the steady decline of costs for basic and advanced biotechnological services has provided both the private and public sectors with an attractive alternative of outsourcing expensive and time-consuming work. While these international transfers are an essential element of risk mitigation, they simultaneously pose safety and security risks, especially when biological agents are transferred to regions where they are not common (or where a specific disease causing agent is not endemic) and thus present a higher risk which requires stricter containment infrastructure and controls (biosafety and biosecurity, see Clevestig 2009, 2014).

The transport sector provides many different types of service in addition to the physical transportation of a commodity, including customs processing and documentation. Certain aspects have to be kept in mind regarding compliance with transit and export control provisions. First, transporters (like traders) are not the manufacturer of the commodities and do not have expertise regarding the technical parameters of the commodity. Therefore, the transporter relies on information supplied by others, including the shipper from the country of export and the supplier or manufacturer. Second, transporters often deal with a large number of items and customs territories. The transporter therefore works with multiple jurisdictions and regulatory bodies. And third, the transporter rarely acts as exporter or has legal ownership over the commodities transported. And finally, due to the absence of legal responsibility in most cases, the transporter is likely to have little interest in the commodities transported.[39]

Identifying and engaging the full range of actors concerned, especially those that may be unaware of any licensing requirements, ideally requires a proactive approach. The alternative of sitting back and expecting companies to search for and find the relevant events and websites is a recipe for an

---

[38] On the specificities of the biological, chemical and nuclear sectors, see also Bauer, 2014.
[39] Thanks to Martin Palmer for information provided on the characteristics of transport sector.

incomplete compliance regime. Government must also tailor its engagement to the audience. This applies to the different product sectors as well as the different functions in the supply chain. However, identification of the entities concerned poses a major challenge for governments. Possible avenues include trade fairs, close cooperation with customs authorities, engagement with industry associations as well as compliance visits.

Generally, clear legislation and straightforward procedures, which take into account the integration requirements within the business systems of companies, are key enabling factors in compliance. To be effective, governments need to communicate the 'why' of export control, so that the rationale for control requirements is understood by industry, particularly since prevention is the real goal, not punishment. Even the best enforcement system is unable to capture all illegal transactions. It is also important to make the business case for export controls, highlighting that this will facilitate access to high technology and to commercial advantages such as trade facilitation (see the point regarding incentivising compliance below). Export controls can also open up new markets to foreign investment and technology transfers. Finally, it is in the interest of international companies to support their subsidiaries in meeting their export control obligations to protect the company's reputation and ensure security of supply.

Companies are motivated to put compliance systems in place by a variety of factors, including wanting to: avoid penalties; maintain a favourable image and avoid reputational damage; avoid delays in licensing application procedures and during export; be able to comply with licensing conditions; and prevent accidental contributions to WMD programmes. ICPs are also becoming increasingly important factors in entering into business along a supply chain.

Both options—the creation of EU-wide **legal ICP requirements** or mere **guidance**—are included in the Communication. In fact, the very term ICP, while frequently used, can lead to confusion, as it is often associated with a formal programme or sophisticated IT solutions. The term export compliance system may be more neutral. Moreover, regardless of the term used, compliance systems necessarily include a wider spectrum of issues and are not limited to the EU Dual-use Regulation or even dual-use export controls. EU-wide ICP requirements for dual-use export control will clearly benefit those companies that have a compliance programme in place and thus incur costs, while potentially facing competition from non-compliant companies. However, the challenge is in determining standards and requirements that fit a very diverse group of companies, representing different sizes, structures, sectors, functions and trading patterns. They will include actors such as transport providers (freight forwarders, fast-parcel operators, shipping lines, customs brokers etc.) and academia/research institutes. This is why many actors and many companies (notably SMEs) favour guidelines and tools over legal requirements. An internal compliance programme does not necessarily involve costly software. An ICP first and foremost involves awareness, knowledge and allocation of responsibilities within the company.

What else does an ICP involve? On this, a number of standards and guidelines have been developed, notably in the context of the Wassenaar Arrangement (2011) and the Nuclear Suppliers Group, which constitute useful references points in the EU discussion on developing guidance. First, it needs to be adapted to the size and structure of the company and integrated into standard procedures and business practices. Second, there are various issues to do with the scope and operation of an ICP, as discussed below.

An ICP has to consider the type of product (classification and potential uses), type of activity, the country of destination (in particular for the implementation of sanctions), the end-use, the end-user, and involved entities, as well as the resulting licensing requirements and prohibitions. Entities involved in a transaction may include the invoicing entity, receiving entity, banks, intermediaries and transit/trans-shipment points. Intermediaries during the transportation could involve freight forwarders, shippers, customs agents etc. Intermediaries and relevant parties in the recipient country may involve agents, distributors, brokers, joint ventures, subcontractors and subsidiaries. Applicable laws may concern multiple

jurisdictions, which may even be contradictory, and comprise regular export, transit, trans-shipment and brokering controls as well as sanctions and other restrictive measures (national, regional and international).

The processes and procedures necessary to establish and operate an ICP, include: measures to facilitate and enable compliance, monitor compliance (internal audits) and act if a compliance breach is detected; some form of infrastructure such as software, screening tools and specialized staff; awareness-raising and training of other staff; and possible support from external lawyers and consultancies (European Commission, 2011). An effective ICP also enables the company to communicate with the licensing authorities and facilitates swift processing of applications and queries, as well as regular contact with the authorities. An explicit company policy or written commitment is generally considered a key element.

The principle of **trade facilitation for 'reliable companies'** with solid internal compliance systems has been developed in a number of frameworks within the EU, both in the fields of military equipment and dual-use transfer controls. To what extent synergies between them can be exploited is the subject of current discussion.

Under the EU Dual-use Regulation, granting a global export authorisation to a specific exporter inter alia has to take into account whether the exporter has 'proportionate and adequate means and procedures to ensure compliance with the provisions and objectives of this Regulation and with the terms and conditions of the authorisation' (Art. 12).

The Intra-Community Transfers (ICT) Directive obliges EU Member States to introduce general and global transfer licences for the export of military equipment to other EU countries (OJ L146, 10 June 2009). To receive goods exported under a general transfer licence, companies must be certified by their national authorities. This in turn requires appointing 'a senior executive as the dedicated officer personally responsible for transfers and exports'. In addition, the company must provide a description 'of the internal compliance programme or transfer and export management system'. The description must include 'details of the organisational, human and technical resources allocated to the management of transfers and exports, the chain of responsibility within the undertaking, internal audit procedures, awareness-raising and staff training, physical and technical security arrangements, record-keeping and traceability of transfers and exports'. To assist with the harmonisation of ICP certification, an EU working group drafted recommendations setting common minimum standards, consisting of: questions and guidelines on the description of internal compliance programmes and subsequent assessment; a standard certification template; powers for monitoring compliance; corrective measures; suspension and revocation of certificates; and exchanges of information relating to certification (OJ L11/62, 15.1. 2011, p. 62). Given the level of detail they contain, these ICP recommendations could also be useful for the dual-use area and thus exploit potential synergies between different areas of EU policy. Lessons learned from this process could also feed into the dual-use area.

The Authorized Economic Operator (AEO) status was created by the 2005 amendments to the EU Customs Code (see section 4.1). The certification scheme came into force in January 2008. National authorities can award the status of AEO to any business that 'meets common criteria relating to the operator's control systems, financial solvency and compliance record' (Regulation (EC) No. 648/2005, OJ L117, 4.5.2005, p. 13). Manufacturers, exporters, freight forwarders, warehouse managers, customs agents and carriers are all eligible to apply for AEO status. Once awarded, AEO status is recognized across the EU and makes the recipient eligible for certain benefits, including simplified procedures at entry and exit points and simplified security- and safety-related inspections. However, this status has little relevance for export controls, and discussions about the benefits and disadvantages of a possible harmonisation are ongoing.

Finally, the goal of partnership with industry overlaps with that of optimising the licensing architecture in the area of facilitation measures (see section 3.1).

6 Further options to enhance effectiveness and coherence

6.1 Penalising offences[40]

Penal law has remained within national competence across all issue areas, including criminal procedural laws and the modalities for deciding whether to take a case to court. Depending on national legal traditions, penal provisions can be placed in specific legislation (such as foreign trade law or other acts regulating customs or dual-use related matters) or in the penal code. Article 24 of the EU Dual-use Regulation requires Member States to 'take appropriate measures to ensure proper enforcement of all the provisions of this Regulation' and to 'lay down the penalties applicable to infringements of the provisions of this Regulation or of those adopted for its implementation'. Article 24 also provides that penalties for breaches of the regulation be effective, proportionate and dissuasive. A similar wording is typically used in EU restrictive measures. However, the translation of this provision into national penalty systems differs considerably across the EU. For example, the maximum prison sentence for export control violations in Germany is 15 years—the highest in the EU. Elsewhere, the maximum sentence is 10 years in the UK (but 14 years for nuclear related offences), 6 years in the Netherlands, 6 years in Sweden and 12 months in Ireland (European Commission, 2005, 2006). Slovenia introduced criminal sanctions in 2008, and now provides for a maximum five-year imprisonment for WMD-related offences, as well as for illegal trade or brokering in other restricted items (Criminal Code of Slovenia, Art. 307). In addition, in 2012 Slovenia introduced provisions penalizing the violation of restrictive measures (Art. 374a). Administrative sanctions also vary considerably, and a number of EU countries do not provide for them at all, although in Sweden a parliamentary Commission in December 2014 proposed that such measures be introduced (Krigsmaterielexportöversynskommittén, 2014).

In addition to potentially facing penalties for infringements of the EU Dual-use Regulation, or for EU restrictive measures related to dual-use trade, suspects may also be prosecuted for violations of national legal provisions in relation to dual-use trade controls. Penalties for violating embargoes containing restrictions on dual-use items will also differ. This has increased in importance in court cases with the imposition of embargoes on Iran and the DPRK by the UN and the EU since 2006.

Numerous additional examples from across the EU could be added to illustrate the differing applications and interpretations of the terms 'effective', 'proportionate' and 'dissuasive'. This is reinforced by the fact that the interpretation and application of basic concepts in penal law such as aiding and abetting, attempt, support, negligence and intent, will vary across the EU. As will practices regarding the suspended prison sentences and parole.

The term 'proportionate' mandates that the scope of an offence and the penalty assigned to a breach has to fit the national legal tradition and system and be proportionate to the offence and to other offences. This criterion raises several questions. Should this criterion be assessed in relation to the seriousness of the crime, including its consequences or potential consequences? Should consideration be given to the subjective perspective, and thus the individual perpetrator, and in particular his or her intent? Or should appropriateness be considered in relation to other offences within the same legal system? This criterion refers to both, penalties for other offences such as fraud, theft, bodily harm or murder, and other trade or WMD related offences such as embargo violations. Countries may have very different penalties for dual-

---

[40] This section draws on Bauer, 2013b and 2015.

use trade offences related to chemical weapons (which are often specified in, or connected to, a Chemical Weapons Convention implementation act) and offences related to nuclear weapons, due to the different origins and context of the legislation.

The EU requirement for penalties to be 'dissuasive' relates to deterrence and prevention. Closely related to this is the issue of the appropriate deterrent for companies and individuals. Whereas fines, loss of property rights (confiscation) and privileges are obvious penalties for both companies and individuals, prison sentences clearly can only be applied to individuals. Prevention is a criterion for effectiveness. Effectiveness can also be interpreted to apply to the actual application of the penalties, and the effectiveness of the overall system. Where penalties only exist on paper but are known not to be enforced, they can hardly be considered effective.

The demand in the 2008 New Lines for Action (NLA) for the intensification of efforts to impede proliferation flows and sanction acts of proliferation leads to three fundamental questions, for which there are different answers.[41]

The first question relates to the way in which penalties are applied. As mentioned above, the range of penalties differs widely across the EU, including possible criminal and administrative penalties, their actual application by the courts, and the types of law used to prosecute proliferation-related offences. The competent authorities may choose to impose a fine without proceeding to prosecution. The procedures, modalities and competent authorities for this also differ across the EU. In Germany for example, since 2007 major WMD-related dual-use trade offences can be transferred to a specialized federal prosecution unit.

The second question concerns the acts to which penalties are applied. There is a wide range of possible acts of involvement in or contribution to proliferation. The focus in the Dual-use Regulation on the exporter can pose a problem from a prosecution perspective, since another actor may be the main or even the only perpetrator. Moreover, the range of actors and their types of involvement in offences has expanded considerably.

In addition, there are different degrees to a person's responsibility. Theoretically, the subjects of punishment could include those acting on their own initiative, organizing an illegal transaction, as well as those acting through negligence or a breach of duty of care. Whether in particular the latter two types of involvement can be subject to criminal prosecution, will again differ from country to country and may be highly controversial.

The third question relates to the 'proliferation'. There is no consensus legal definition apart from the provisions of the nuclear Non-Proliferation Treaty (NPT), which defines nuclear proliferation as the spread of nuclear weapons to states other than the five nuclear weapon-possessing states specified in the treaty. However, this term is rarely translated into or directly applicable in national laws. The term is therefore not justiciable in the EU, even though it has become commonly used in political discussions and in enforcement circles. There are, however, penalties for a range of WMD-related offences in national provisions.

However, it should be noted that different avenues and apparent differences may effectively lead to the same, or similar, results. In the Netherlands, Slovenia and the UK, both companies and individuals can be prosecuted. A company may for example be shut down or receive a monetary penalty. While prosecuting a company is not possible in Germany, fines or forfeiture may effectively lead to a company's closure.

---

[41] To sanction in English can also mean to condone, so obviously in the NLA it is intended to stand for punishing.

Due to the different legal systems, traditions, terminologies and procedures across the EU, a level playing field in terms of penalties is thus currently not feasible. While the 28 different ways of implementing and enforcing the EU Dual-use Regulation are based on one uniform law, investigation, prosecution and sentencing take place in 28 distinct frameworks. However, increased cooperation and exchange on legal as well operational approaches may lead to more consistency over time. Establishing a database of prosecution cases would also contribute to this end, and would be a useful source of information for investigators, prosecutors and judges who are rarely likely to deal with such cases. Finally, it is worth highlighting that the primary goal of an effective system is compliance rather than punishment.

6.2   Company audits

Company audits will help determine whether a company is reliable and has a robust system for internal compliance. Auditing a company's business and export records (in paper and electronic form) may identify previous unlicensed exports that were not detected, or other offences such as unlicensed technical assistance or brokering activities. Visiting a company also provides an opportunity to raise awareness and to obtain useful information that can feed back into the risk management system. As explained earlier, the introduction of trade facilitation measures such as general and global licences and access to simplified customs procedures requires methods to check that companies are compliant. One approach to verification is company audits specifically focused on export controls.

At present, most EU Member States do not have specialised foreign trade company audit strategies and procedures, and specialised staff to conduct those. Exceptions include Germany, the Netherlands, Sweden and the UK. Also smaller countries such as Slovenia conduct company audits that include dual-use exports. A shift towards more facilitated procedures will require enhanced auditing capacities. Already in the current context, in many EU countries, auditing capacities are not sufficiently used to prevent and detect illegal transactions.

While not specifically included, dual-use specific company audits build on some proposals made by the European Commission since they are relevant to internal capacity building and to facilitation measures combined with pre- and post-export controls. Training on specialised company audits could also be built into an EU internal capacity-building programme.

7   Conclusions and recommendations

The study concludes that there is clearly a need to adjust the EU's dual-use export controls by going beyond: the traditional military/civilian dichotomy; the traditional focus on export and exporter; and the focus on tangible goods. In doing so, it is highly important that EU policies and decisions keep in mind the following aspects, which have at times been neglected:

- the centrality of enforcement functions to an effective export control system, comprising prevention, auditing, detection, investigation and prosecution functions;

- the broad spectrum of actors in the supply chain, not only producers and exporters, but also academia, traders, the transport sector etc;

- the importance of matching policy priorities with operational resource. Policy goals must translate into operational targets, job descriptions and resource allocation in order to have practical relevance; and

- the external implications of EU changes, because many countries follow EU practice/standards.

The increasingly complex procurement patterns that are associated with illicit WMD programmes, the multiplication of actors involved, and technological developments that have made proliferation-sensitive

flows more difficult to control through traditional legal concepts, implementation approaches and enforcement methods.

This study suggests that the effectiveness of the system could be enhanced in a number of ways, requiring the mobilisation of political will at different levels and across different institutions in the EU and Member States, as well as enhancement of human resources, cooperation and internal and external capacity-building. Engaging with the whole range of stakeholders involved in the supply chain, and thus including transport providers and academia will be crucial to success. This will in turn require an understanding of the underlying purpose and concepts and the identification of constructive and practical solutions to an ever-evolving security, technological and economic challenge. Whether referred to as an internal compliance programme or export management system, the procedures, policies and infrastructure put in place have to be based on a culture of compliance in order to be effective. It can be argued that compliance efforts by industry are a part of corporate social responsibility, which also includes corporate responsibility for security. It can also result in cost reductions due to access to simplified export procedures and the reduced risk of illegal exports, thus avoiding penalties and protecting the brand/reputation, and attracting investors. While governments recognise the crucial role of industry, there is still some way to go to establish a true partnership between government and the private sector. In particular, compliance efforts need to be adapted to today's trading reality to effectively address the perceived risks and threats. To conclude, there is a need to facilitate legitimate exports while focusing efforts on preventing and detecting sensitive illegal transactions that may occur through ignorance, negligence or intent.

Key recommendations are therefore for the EU and its Member States to:

1. Allocate sufficient national resources for licensing and enforcement staff across the EU, also for international capacity-building, and include international cooperation in their tasks.

2. Establish a well-resourced EU in-reach programme comprising the whole range of licensing and enforcement functions.

3. Enhance the efficiency of licensing procedures through increased staff resources, targets for processing routine cases, and optimised procedures including electronic licensing.

4. Further review, create and use trade facilitation measures to enable authorities to focus on the biggest security risks.

5. Develop outreach measures, two-way dialogue and compliance tools tailored to different types of exporters and other supply chain actors.

6. Develop ICP guidelines tailored to different types of stakeholders (depending on the nature of the entity – e.g. company or academic institution), size of the entity, activity engaged in (export, transport, brokering etc.), building on those developed for the ICT Directive.

7. Conceptualise and implement an outreach and awareness raising strategy for academia.

8. Clarify current provisions on technical assistance and technology transfer and provide guidance for stakeholders across the EU.

9. Establish an EU forum for enforcement officers, with sub-groups or special sessions dedicated to the different enforcement functions: customs detection; company audits; investigation and prosecution, and including a peer review element.

10. Add informal workshops to the regular EU meetings (Dual-use Working Party and Dual-use Cooperation Group) to exchange experiences in a more informal setting.

11. Explore better use of Box 44 on the EU's customs declaration form to enable a) the verification of correct information regarding licensing requirements and the use of existing licences and b) enhanced information exchange among EU countries.

12. Establish an expert forum gathering academic, industry and governmental experts to discuss feasible and meaningful ITT controls.

13. Explore and seek to resolve EU-wide and international differences in terminology, in particular regarding terms such as dual-use, transit, transhipment and brokering.

14. Make common interpretations of the dual-use control list mandatory in the EU.

15. Clearly define the relationship between the EU Dual-use Regulation and the EU Common Position on the export of military equipment and technology.

16. Make control list amendments wherever possible in international fora.

17. Monitor developments in the field of cyber-surveillance technologies and adopt new control list items – as needed – at either the EU or Wassenaar Arrangement level. Where the latter is not possible, explore whether a complementary legal instrument could be created or a dedicated section be added through a separate Annex to the Dual-use Regulation.

18. Establish the range of human rights and security considerations that states should take into account when assessing licences for the export of dual-use goods.

19. Consider the adoption of catch-all controls for the export of unlisted cyber-surveillance technologies.

20. Develop guidelines concerning the technical specifications and governance frameworks for cyber-surveillance technologies.

8 Bibliography

ASD (AeroSpace and Defence Industries Association of Europe), 'ASD Position Paper on the Review of the Dual-Use Export Control System of the European Union', 22 Oct. 2014.

Anthony, I. and S. Bauer, 'Transfer controls', SIPRI Yearbook 2006: *Armaments, Disarmament and International Security*, Oxford: Oxford University Press 2006, pp. 775-797.

Bauer, S. (2013a), 'Arms trade control capacity building: lessons from dual-use trade controls', *SIPRI Insights on Peace and Security* 2013/2, Mar. 2013.

Bauer, S. (2013b), 'WMD-related dual-use trade control offences in the European Union: penalties and prosecutions', *Non-proliferation Paper* No. 30, EU Non-proliferation Consortium, July 2013.

Bauer (ed.), *Monitoring and Controlling the Import and Export of Chemical, Biological, Radiological and Nuclear Materials: An Introduction*, Background Paper for CBRN Training Workshop, CBRN Risk Mitigation Centre of Excellence Project No. 5 ('Import and Export Monitoring of CBRN Materials: Knowledge Development and Transfer of Best Practice on CBRN Import and Export Monitoring'), Frankfurt, 13–16 May 2014.

Bauer, S., 'Penalties for export control offences for dual-use and export control law: a comparative overview of six countries', April 2014, in *Skärpt exportkontroll av krigsmateriel – DEL 2, bilago, Slutbetänkande av Krigsmaterielexportöversynskommittén, KEX*, SOU 2015:72, Stockholm 2015, pp. 753-770, <http://www.sou.gov.se/wp-content/uploads/2015/06/1_SOU-2015_72_DEL-2_sid-1-818_webb.pdf>.

Bauer, S. and M. Bromley, 'V. Export Control Developments in the European Union', Dual-use and arms trade controls, *SIPRI Yearbook: Disarmament, Armaments and International Security*, Oxford: Oxford University Press 2013, pp. 457-468.

Bauer, S. and I. Micic, 'Controls on security-related international transfers', *SIPRI Yearbook 2010: Armaments, Disarmament and International Security*, Oxford: Oxford University Press 2010, pp. 447-467.

CAUSE (Coalition Against Unlawful Surveillance), 'A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation', June 2015, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>

Clevestig, P., *Handbook of Applied Biosecurity for Life Science Laboratories*, SIPRI: Stockholm, 2009.

Clevestig, P. 'Biological materials', in Bauer (ed.), *Monitoring and Controlling the Import and Export of Chemical, Biological, Radiological and Nuclear Materials: An Introduction*, Background Paper for CBRN Training Workshop, CBRN Risk Mitigation Centre of Excellence Project No. 5 ('Import and Export Monitoring of CBRN Materials: Knowledge Development and Transfer of Best Practice on CBRN Import and Export Monitoring'), Frankfurt, 13–16 May 2014.

Cindy Cohn, C. and Y. Jillian, Know Your Customer' Standards for Sales of Surveillance Equipment, Electronic Frontier Foundation, 24 Oct. 2011, <https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment>.

Council of the EU (2003), Fight against the Proliferation of Weapons of Mass Destruction: EU Strategy against Proliferation of Weapons of Mass Destruction, 15708/03, 10 Dec. 2003.

Council of the EU (2004), 2630th Council Meeting General Affairs and External Relations, Brussels, General Affairs, Press Release no. 15460/04, 13 Dec. 2004.

Council of the EU (2008), New Lines for Action by the European Union in Combating the Proliferation of Weapons of Mass Destruction and their Delivery Systems, 17172/08, 17 Dec. 2008.

Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code, *Official Journal of the European Union* L302, 19 Oct. 1992, as amended.

Criminal Code of the Republic of Slovenia, 2009 <http://www.policija.si/eng/images/stories/Legislation/pdf/CriminalCode2009.pdf>.

Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community, *Official Journal of the European Union*, L 146, 10 June 2009.

European Commission (2005), 'Sanctions imposed by EU member states for violations of export control legislation', Draft rev. 14, Sep. 2005.

European Commission (2006), Directorate-General for Trade, Working Party on Dual-use Goods, 'Report on the answers to the questionnaire DS6/2005 rev. 3 on existing sanctions—implementation of Article 19 of Council Regulation 1334/2000', DS 37/4/2005 rev. 4, 11 May 2006.

European Commission (2011), 'The dual-use export control system of the European Union: ensuring security and competitiveness in a changing world', Green Paper COM(2011) 393, 30 June 2011.

European Commission (2013a), 'Strategic export controls: enduring security and competiveness in a changing world. A report on the public consultation launched under the Green Paper COM(2011)393, European Commission Staff Working Document, Brussels, 17 Jan. 2013, SWD(2013) 7 final.

European Commission (2013b), ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, European Commission, June 2013.

European Commission (2014a), 'Communication from the Commission to the Council and the European Parliament, The Review of export control policy: ensuring security and competitiveness in a changing world', COM(2014) 244 final, Brussels, 24 Apr. 2014.

European Commission (2014b), 'Roadmap. Review of the EU dual-use export control regime – Regulation 428/2009', DG Trade F1, 15 July 2014, <http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2014_trade_014_dual_use_en.pdf>.

European Commission (2014c), Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1236/2005 concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment, COM(2014) 1 final 2014/0005 (COD), Brussels, 14 Jan. 2014.

European Commission (2015), 'Impact Assessment for the Review of the Dual-use Export Control Regime. Consultation Strategy', <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153627.pdf >, without date [2015].

Evans, S., 'Revising export control lists', Brussels: Flemish Peace Institute, Mar. 2014 <http://www.vlaamsvredesinstituut.eu/sites/vlaamsvredesinstituut.eu/files/files/reports/revising_export_control_lists_web.pdf>.

BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle/Federal Office of Economics and Export Control), 'Final report to the tender related to prepare a study setting out a technical training concept on dual-use export controls submitted by the German Federal Office of Economics and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle, BAFA)', without date [2010].

King's College London and Association of University Legal Practitioners, *Higher Education Guide and Toolkit on Export Controls and the ATAS Student Vetting Scheme*, 2015. <https://www.acsss.info/academia>

Krigsmaterielexportöversynskommittén, *Sanktionsväxling–effektivare sanktioner på exportkontrollområdet*, Delbetänkande, SOU 2014:83, Stockholm 2014.

Nuclear Suppliers Group, 'Good Practices for Corporate Standards to Support the Efforts of the International Community in the Non-proliferation of Weapons of Mass Destruction', (without date), <http://www.nuclearsuppliersgroup.org/images/Files/National_Practices/NSG_Measures_for_industry_update_revised_v3.0.pdf>.

UK Department for Business Innovation & Skills, 'Intrusion Software Tools and Export Control', 10 Aug. 2015.

UNDP, *Human Development Report 1994,* Oxford: Oxford University Press, 1994, <http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

Wassenaar Arrangement (2011), 'Best Practice Guidelines on Internal Compliance Programmes for Dual-Use Goods and Technologies', Dec. 2011 <http://www.wassenaar.org/guidelines/docs/2%20-%20Internal%20Compliance%20Programmes.pdf>.

Wassenaar Arrangement (2012), 'Wassenaar Arrangement public statement', Vienna, 11–12 Dec. 2012, <http://www.wassenaar.org/publicdocuments/index_PS_PS.html>.

Wassenaar Arrangement (2013), 'Public Statement 2013. Plenary meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies', 4 Dec. 2013, <http://www.wassenaar.org/publicdocuments/index_PS_PS.html/>.

WORKSHOP PRESENTATION

Improvement of the system against the backdrop of the European Commission's reform proposal

Speaking notes for European Parliament workshop on Dual-use Export Controls
Brussels, 17 June 2015

Sibylle Bauer
Director, Dual-use and Arms Trade Control Programme
Stockholm International Peace Research Institute (SIPRI)
(bauer@sipri.org)

1. Introduction

The workshop seeks to discuss *'the main issues to be addressed in the export control policy review, notably:*

- *shift in underlying control policy (e.g. human security dimension)*
- *technological relevance (e.g. list of goods)*
- *licensing architecture*
- *brokering, transit and technology controls,*
- *intra-EU transfer controls*
- *transparency and private sector implementation*
- *EU implementation capacity and*
- *global convergence'.*

The representative of the European Commission has already outlined the cornerstones of the reform proposal (including the state of play of the impact assessment), and Ian Stewart has given an overview of the state of play and the need for reform of EU export controls. I was asked to analyse 'the European Commission's review options and prospects for modernisation' as well as the 'impact of different policy choices'.

2. Improvement of the system against the backdrop of the European Commission's reform proposal

The title of the April 2014 Communication 'Ensuring security and competitiveness in a changing world' provides the overall rationale for export controls: balancing security (international, national and human security) and economic/trade interests. It also indicates what is considered an improvement of the system and its effectiveness. One could add a third dimension: academic freedom, the limits of which are currently under discussion in the context of the further clarification of controls of intangible transfers of technology (ITT).

Given the limited time frame here, I will only focus on some of the review options. Further detail will be provided in the written study and could be raised during the discussion.

2.1 Intangible transfers of technology (ITT)

- Technological developments (including 3D printing) have lead to substantial changes in export controls: not only export of goods but also transmission of technology through intangible means (such as electronic transfers), which

poses challenges inter alia for enforcement.

- ITT is central to normal business interactions (intra-company electronic transfers/shared server access; participation in meetings, bringing laptops with controlled technology etc.).

- ITT is central to academic research, exchange and publications (transmission of know-how at lectures, in academic publications, to foreign researchers – in the biological area also exchange of samples).

- Need for legal clarification and practical guidance/tools in the area of ITT.

2.2 Capacity-building within the EU and internationally

- In-reach: Currently no EU funds for training and internal capacity-building. EU internal training currently takes place with US funding (although limited to the 11 most recent Member States), while the EU funds international capacity-building. The European Commission proposes EU internal training and capacity-building, which has resource implications since it requires systematic funding and must also include enforcement functions.

- Outreach: International capacity-building not only contributes to international security but also to international convergence and thus to levelling the playing field.

- In-reach and outreach are mutually reinforcing, and essential for the effectiveness and credibility of EU dual-use export controls.

- In-reach and increased interaction will also facilitate more harmonised implementation across the EU.

2.3 Enhanced strategic and operational cooperation with enforcement agencies

- This must involve not only cooperation of licensing authorities with enforcement agencies, but also among enforcement agencies. There are regular EU meetings of dual-use licensing officers, but no systematic meetings of customs and other enforcement officers to discuss issues such as auditing, prevention/awareness-raising, and the detection, investigation and prosecution of EU export control offences. Currently, if at all, they meet at the export control regimes, international capacity-building events or US funded meetings.

- Proposal to 'integrate export control priorities in policy cycles': importance of top-level policy and mid-level management priorities for effective enforcement. Challenge of cross-cutting nature of dual-use export controls.

- Proposal to develop 'common risk management tools and framework': This is in process, but requires further increase in trust and information sharing. Joint operations and enhanced information sharing are also included in the Commission Communication.

2.4 Private sector partnership

- Importance of communicating the rationale of export controls to all stakeholders, and to support their compliance efforts (incentivise compliance and provide tools). Key stakeholders also include universities, research laboratories etc.

- Need to facilitate legitimate exports while focusing efforts on preventing and detecting illegal transactions (which occur through ignorance, negligence or intent).

- Possibility to create a technical advisory group on list changes at EU level.

2.5 Legal changes and clarifications

- Expansion/revision of the dual-use concept: beyond military/civilian dichotomy to include human security/human rights? While there is a clear need to address the issue, the challenge is to find the most appropriate instrument.

- Importance of keeping the international implications of EU legislative changes in mind: an increasing number of countries use EU legal provisions (including the control list) as a model/reference point.

- Current focus on export and exporter, while 'transiter' is not defined in the EU Dual-use Regulation. This is important given the complexity of the supply chain and of both legal and illegal dual-use transactions. The transport sector as the 'forgotten piece of export control regulations' deserves a stronger focus (the clarification of legal responsibility and the design of compliance guidelines and tools).

- Need to harmonise terms such as transit with the EU customs code.

2.6 Coherence between different elements of the EU export control regime

- Challenge of cross-cutting nature of dual-use export controls, involving different legal instruments, policy areas and institutional competencies; in Member States and in the EU. Dual-use export control aspects are also relevant for a range of other DGs (in addition to DG Trade), including DG TAXUD, DG Research and DG Home. Relevant elements include sanctions and anti-torture regulation.

3. Conclusions

Need to adjust dual-use export controls by going:

- beyond traditional military/civilian dichotomy
- beyond focus on export and exporter, although that is still the main activity around which control requirements revolve
- beyond a focus on tangible goods

Importance of:

- keeping external implications of EU changes in mind, because many countries follow EU practice/standards
- enforcement functions (prevention, auditing, detection, investigation, prosecution)
- engaging all actors in the supply chain, not only producers and exporters, but also academia, traders, the transport sector etc.
- matching policy priorities with operational resource, which requires allocation of sufficient resources for licensing and enforcement staff across the EU, also for international capacity-building. Policy goals must translate into operational targets, job descriptions and resource allocation in order to have practical relevance.

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES

POLICY DEPARTMENT

Role

Policy departments are research units that provide specialised advice
to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

Foreign Affairs

   Human Rights

   Security and Defence

Development

International Trade

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

Publications Office