EUROPEAN
COMMISSION

Brussels, 28.9.2016
SWD(2016) 315 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Report on the EU Export Control Policy Review

Accompanying the document

Proposal for a

Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items

(Recast)

{COM(2016) 616 final}
{SWD(2016) 314 final}

IMPACT ASSESSMENT REPORT

INTRODUCTION

The trade in dual-use items - goods, software and technology that can be used for both civilian and military applications and/or can contribute to the proliferation of Weapons of Mass Destruction (WMD) – is subject to controls to prevent the risks that these items may pose for international security. United Nations Security Council Resolution 1540, adopted on 28 April 2004, decides that all States shall enforce effective controls to prevent the proliferation of nuclear, chemical or biological weapons and their means of delivery. Efforts to prevent proliferation through international trade are also required under relevant international agreements, such as the nuclear Non Proliferation Treaty, the Chemical Weapons Convention and the Biological and Toxin Weapons Convention, and in line with commitments agreed upon in multilateral export control regimes.[1] An effective common system of export controls on dual-use items is therefore necessary to ensure that the international commitments and responsibilities of the Member States and of the European Union (EU), especially regarding non-proliferation, are complied with. Moreover, the EU Strategy against proliferation of Weapons of Mass Destruction of 12 December 2003 (EU WMD Strategy), as updated by the Council Conclusions of 21 October 2013 on ensuring the continued pursuit of an effective EU policy on the new challenges presented by the proliferation of weapons of mass destruction, calls for the strengthening of EU export control policies and practices.

The EU export control system is governed by Regulation (EC) No 428/2009 setting up a Community regime for the control or exports, transfer, brokering and transit of dual-use items ("the Regulation"). The Regulation provides for common control rules, a common EU control list and coordination of implementation. Controls apply to export – including electronic transmission - brokering and transit as well as, for some most sensitive items, internal transfer within the EU. The Regulation essentially transposes the commitments agreed upon in the multilateral export control regimes into EU law – e.g. the main control parameters and the EU list of dual-use items closely reflect decisions agreed upon in the regimes[2]. It is directly applicable throughout the EU and forms part of the common commercial policy under Article 207 Treaty on the Functioning of the European Union (TFEU). EU Member States nevertheless need to take certain complementary measures for implementing some of its provisions, e.g. in relation to licensing and enforcement, and may adopt, in some cases, specific national control measures[3].

As required by the Regulation, the Commission launched in 2011 a broad public debate[4] on the functioning of the EU export control regime and its future strategic options. The European Parliament and the Council, for their part, also called for a review and strengthening of export controls[5]. In a 2013 report to the European Parliament and Council[6] the Commission concluded that although the system provides solid legal and institutional foundations, it cannot remain static and must be upgraded in order to face new challenges and generate the modern control capabilities the EU needs for the coming decade and beyond. The report opened the way to a 2014 Commission Communication[7] outlining a long-term vision for EU export controls and announcing policy initiatives for their modernisation and adaptation to rapidly changing technological, economic and political circumstances. The Commission subsequently conducted an impact assessment of the review options outlined in this Communication to identify the most suitable regulatory and non-regulatory actions to bring them into effect.

The export control policy review has also been identified as an intiative under the Regulatory Fitness and Performance Programme (REFIT) and the Commission has in particular assessed the costs and benefits associated with the various options, notably as regards potential regulatory simplification and burden reduction.

CHAPTER 1 - PROBLEM DEFINITION: WHAT IS THE PROBLEM AND WHY IS IT A PROBLEM?

1.1 The problem: ensuring security and competitiveness in a changing world.

The EU export control system applies high standards of controls and serves as a benchmark for many countries around the world. The system is generally considered robust and provides solid legal and institutional foundations for the EU to fulfil its international obligations, and public consultations have demonstrated that stakeholders mostly agree that it reduces significantly the ability of states to proliferate by procuring sensitive items from European suppliers. In spite of this, denials issued by competent authorities and enforcement and violations of controls emphasise that risks remain acute. In this context, the primary challenge for the EU export control system is to continuously strike the right balance between the EU's overarching foreign and security policy objectives and its economic and commercial interests in a changing security, economic and technological environment. This is, in essence, why the export control system cannot remain static: its parameters need to be continuously adjusted to respond to evolving security risks, rapid technological developments and transformations of economic activity and it must be upgraded in order to face new challenges and generate the modern control capabilities the EU needs for the coming decade and beyond.

1.1.1 Risk that controls may not adjust to evolving security threats.

The last decade has witnessed dramatic shifts in the global security environment., and a first problem relates to the need for EU export controls to keep pace with evolving security threats and proliferation patterns at a time when the threat environment is dynamic and complex..Lessons learnt and stakeholder consultations show that the Regulation is not fully adapted to today's evolving security threats. Outdated or insufficient control provisions generate potential loopholes. For example, the application of the definition of exporter to natural persons is unclear in some situations. The determination of the competent authority is also unclear in certain specific situations and there are cases where the Regulation does not enable to clearly identify a single competent authority. Furthermore, controls on brokering and transit do not provide a clear basis for controlling items that maybe misused for terrorism or human right violations

Another aspect of the problem is that the Regulation essentially establishes a system for the control of legal exports, but lacks dedicated provisions to tackle illicit trafficking of dual-use items, which appears as an increasing threat. The Regulation also does not clearly address the risk of terrorism and misuse of dual-use items by non-state actors.

The problem is multifaceted and dual-use export controls are not the only security trade instrument in the EU's toolbox. Dual-use controls directly complement controls on arms exports and pursue largely similar objectives. Restrictive measures (sanctions) play an important role in combating WMD proliferation and terrorism, and also promote regional security and human rights. Regulation (EC) 1236/2005 (the "Anti-torture" Regulation) specifically addresses trade that could be misused for torture and capital punishment. Other regulations or directives e.g. on firearms, drug precursors or intra-EU transfer of defence material also play an important role in regulating the trade of sensitive items. However, each of those instruments deals either with a specific and different category of items and/or end-uses, or addresses different types of situations. Therefore, in spite of their importance as part of the overall EU response to evolving security threats, those instruments cannot address the 'dual dimension' of security.

1.1.2 Risk that controls may not keep pace with rapid technological and scientific developments.

Dual-use items are typically high-technology advanced items and the EU export control system therefore needs to integrate the security implications of an ever growing number of emerging technologies – e.g. cloud computing, Unmanned Aerial Vehicles (UAV), additive manufacturing, life sciences, nanotechnologies… - in order to ensure their peaceful use.

The problems is that the EU system lacks the flexibility and adaptability to keep pace with technology and ensure timely adjustments of controls. Thus, the list of items benefiting from EU General Export Authorisations can only be modified through a legislative procedure, thus making it difficult to adjust it to rapid changes in technology. The EU system is also constrained by limited technical capacity – expertise and resources - to assess the security threats associated with new technologies of concern and adapt accordingly. Thus, the EU has so far not issued any guidance on the control of emerging technologies, while for ex., some competitors like the US and Japan have clarified their approach, for the benefit of their operators, to the control of technology transfers through the cloud.

1.1.3 Lack of control on cyber-surveillance technologies.

Over the last years, the emergence and controversial export of new types of cyber-tools (e.g. spyware or malware and telecommunication and internet surveillance technologies - hereunder "cyber-surveillance technologies") have evidenced new threats for security and human rights and have fuelled a debate about the need for the EU to control the trade in cyber-surveillance technologies and its effects on human rights and security. The problem is that, although some initial steps have been taken to subject some cyber-surveillance technology to control, the Regulation does not fully address the risks associated with the burgeoning trade in cyber-surveillance technologies and does not clearly identify cyber-surveillance technologies as a new category of dual-use items. A particular aspect of this problem relates to the fact that "cyber-proliferation" is not as such covered by existing international arrangements, so that the EU needs to charts its own course in this area.

The lack of a robust legal basis for controlling exports of cyber-surveillance technologies hampers the EU's ability to prevent exports that may be misused for human rights violations or against the EU's critical infrastructure. The insufficient legal framework can also have dramatic consequences for EU companies: thus, one company is subject to a criminal court case in France and accused of complicity with human rights abuses in Libya[8].

1.1.4 Vulnerability of global supply chains and lack of level playing field.

Proliferation strategies evolve to exploit the vulnerability of the interconnected global trading and information systems. As a result, current EU controls, essentially based on physical geography (i.e. export from the EU customs territory) and focused on tangible goods, appear increasingly at odds with global supply chains and global data networks. The Regulation insufficiently address the specificity of intangible technology transfer - transmission of software and technology (e.g. technical data) by electronic media - which cannot be controlled by customs at the border, and for which individual licences appear ill-suited. The Regulation also insufficiently covers services such as technical assistance, which are increasingly integrated with trade in goods. For example, IT services, including maintenance and upgrades, are essential to the functioning of many cyber-surveillance technologies and as sensitive as the goods exported in the first place.

Moreover, the increasing foreign availability of dual-use items has become an important competitive factor in the absence of global control standard, as distortions of competition due to higher compliance costs and delivery delays sometimes put EU operators at a disadvantage vis-à-vis foreign competitors.

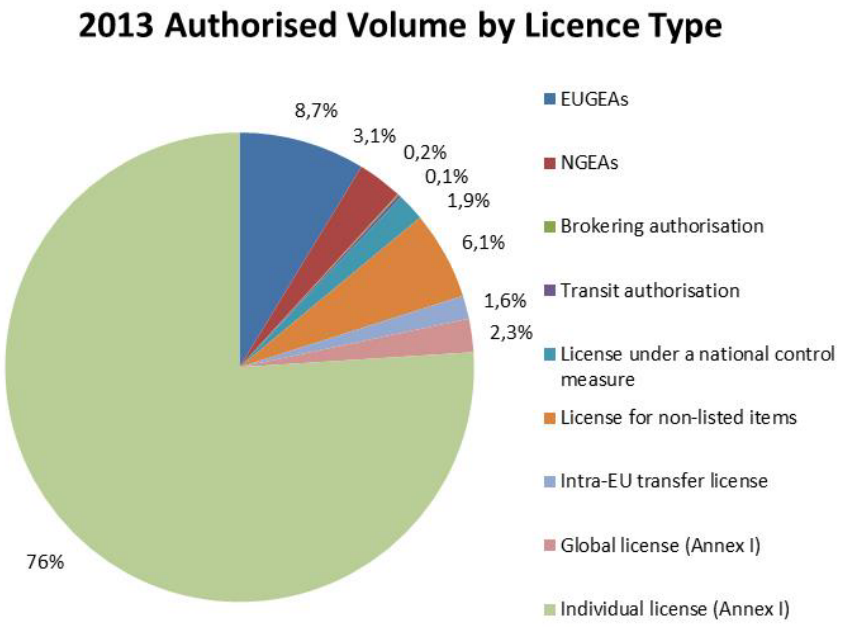
76% of surveyed industry associations affirm that current controls give rise to significant distortions of competition[9]. This may result from some key trade partners having more streamlined export control systems. For example, 2.4% of EU exports require a license[10] under the Regulation, as compared to approximately 1.0% under US regulations[11], which places a comparatively heavier burden on EU exporters. Distortions of competition may also appear as some competitors from countries that are not members of multilateral export control regimes produce and export dual-use items. For example, China, the EU's second biggest trade partner and a major producer of dual-use items, does not participate in all export control regimes and is therefore not bound by all their decisions. As a result, EU exporters are subject to comparatively higher requirements than their competitors. Against this background, the emerging bilateral dialogue with third countries does not, at this stage, sufficiently support regulatory convergence.

1.1.5 Excessive administrative burden.

Security has a cost, and export controls inherently have a cost. The problem arises when controls generate *excessive* administrative burden. Thus 81% of surveyed companies[12] complain that the administrative burden related to compliance with export controls is "heavy and time-consuming" especially due to complex procedures, licensing delays and lack of clarity of export denial[13]. For their part, surveyed licensing authorities identify challenges primarily in terms of insufficient staff resources and lack of specialised technical expertise[14].

In this sense, the licensing architecture in the EU appears sub-optimal, as 76% of EU authorisations take the form of individual licences (Figure 1)[15], with an inherent risk of delay and cost for exporters. Indeed, out of the four types of authorisations (individual, global and EU or national general authorisations), only individual licences require prior assessment of each single export , which can be time-consuming and can be problematic when just-in-time delivery of product to foreign customers or the real-time sharing of data and technology in research and development is required The divergent application of controls by competent authorities also generates costs within the Single Market, as operators are sometimes faced with accumulated delays and legal uncertainty. Also, certain specific controls under the Regulation result in exceptional costs.Thus, controls on intra-EU transfers of certain sensitive items (so-called 'Annex IV items'[16]) constitute a significant exception to the Single Market and an obstacle to the free-movement of goods.

Therefore, at a time when key partners[17] are reforming their systems with a view to reducing regulatory burden on companies, it is important for the EU to ensure that control processes under the Regulation do not unduly disrupt trade due to excessive administrative burden or legal uncertainty. The export control policy review is thus expected to contribute to a simplification of certain control procedures and a more clear and consistent application of controls throughout the EU, and has therefore been identified as a REFIT initiative.



`Figure 1: Comparative number of licences and authorisations per category (2013 data)

Furthermore, certain provisions of the Regulation give rise to legal uncertainty, which in turn adds to the cost of compliance since companies spend time and money finding out if and how they are affected. This is illustrated by complaints by exporters regarding the lack of clarity of "catch-all controls", which are applied by competent authorities on non-listed dual-use items, and for which little information is made available to exporters,

1.1.6 Uneven implementation and enforcement within the EU.

Important steps have been taken, under the Regulation, to support consistent implementation e.g. with the introduction since 2012 of a common IT infrastructure – the 'Dual-Use Electronic System' (DUeS[18]) – providing for some exchange of information between Member States and the Commission. However, divergences in the interpretation and application of controls continue to result in different export conditions, as well as a lack of legal transparency and predictability for companies and ultimately affect the effectiveness of controls and the level-playing field within the Single Market.

Exchange of information with Member States and dialogue with industry reveals problems associated with such divergences in the interpretation and application of controls in the EU. Thus, 60% of the industry associations declare that current export controls give rise to significant distortions between companies located in different Member States, and about 14 % of the companies declare that they have received a denial for a licence application when another exporter fulfilled the deal through an identical export from another Member State[19]. Catch-all controls offer, here again, a good illustration as the Regulation does not provide for a sufficient exchange of information regarding authorisation requirements, so that catch-all controls may be imposed by one Member States on the exporters established on its territory, while other EU exporters are not subject to the same requirement.

There are also reports that export authorizations issued by the competent authority of a Member State (where the exporter is established) have been rejected by other national authorities (typically when production is outsourced or sub-contracted in another Member State) thus obliging the exporter to

apply for another authorization and causing additional delays and a risk that the exporter be confronted with contradicting decisions.

1.1.7 – Design and implementation dimensions of the problem.

An important point to note is that the problems are linked both to the design of the regulation and its implementation. The design of the Regulation is associated with a series of problems, as some of its provisions are not entirely "fit for purpose" any longer. This applies e.g.to controls and provisions mentioned in Section 1.1.1, but also to the requirement for individual licences for intra-EU transfers within the Single Market, which stems directly from the Regulation and offers a good example of an outdated legal provision creating excessive administrative burden. In some cases, the design of the Regulation entirely fails to address an issue, as illustrated by the lack of clear legal provisions for controlling cyber-surveillance technology or for denying an export based on human rights considerations.

Problems also relate to the – uneven - implementation of the Regulation. For example, the Regulation's licensing architecture provides a good basis for controls, with four different types of licenses. However, it also leaves open the possibility for MS to introduce more flexible control modalities (such as National General Export Authorisations), thereby resulting in more favourable export conditions for some operators and a distortion of competition. The implementation of catch-all controls provides another example, since Member States who decide to control non-listed items do not need to inform other Member States or exporters, which inevitably results in "uneven implementation within the EU".

1.2 Identification of the problem drivers: What are the main drivers?

The following changes and trends have been identified as the main drivers resulting in the above mentioned problems:

1.2.1 Evolving and new security threats.

1.2.1.1 Changing proliferation patterns.

Export controls are a key instrument to counter WMD proliferation which is "one of the greatest security risks for the EU"[20] and has been in constant evolution over the last years:

- In recent years, the risk of nuclear proliferation has become multifaceted. A growing number of states are developing capabilities of proliferation concern. North Korea and Iran's nuclear and missile programmes have been a major international concern, while at the same time, global nuclear risks have increased with the emergence of additional nuclear threshold states, building a latent capacity for the leveraging of civilian nuclear power for potential nuclear weapons breakout capability. Additionally regional conflicts create chaotic situations that weaken states' ability to protect nuclear and radiological materials from theft or diversion[21], increasing the risk that they could be misused to build a "dirty bomb".
- With respect to chemical non-proliferation, the Syrian conflict revealed the first use of chemical agents since the 1980-1988 Iran-Iraq war. Moreover, there are concerns regarding possible covert chemical weapons programmes[22], potentially exploring new categories of dual-use chemicals with broad industrial and commercial applications. Evolving risks associated with trade in dual-use chemicals have become acute, as illustrated by the extradition in 2015 of an EU citizen to the U.S. to face charges of illegally exporting laboratory equipment, including items used to detect chemical warfare agents, to Syria[23].

- Biological weapons are complex and difficult to produce, but with the increasing mobility and accessibility of knowledge, the risk of developing new strains of dangerous viruses is of increasing concern. This was recently illustrated by the decision of the Dutch licensing authority, in June 2012, to subject to an export licence the publication of biological research on the transmissibility of H5N1 virus as part of an effort to discover a vaccine against the virus; the decision was recently confirmed by an appeal court in June 2015[24].

- Risks also result from advances in missile technology, including hypersonic missiles and the proliferation of missile guidance components. Experts report that 75 countries currently possess cruise missiles and 19 countries manufacture them[25]. The space security landscape also changes rapidly, with more countries and private entities joining the launch business.

- Importantly, WMD proliferation risks are not limited to states any longer, as non-state actors are increasingly involved in trafficking through clandestine procurement programmes, using sophisticated techniques to evade controls (such as complex procurement networks including series of front companies and deception techniques to hide the end-use, moving sensitive items through areas with weak domestic institutions and trans-shipment hubs etc). Experts highlight a confluence of transnational security threats involving drug organizations and crime groups in relation to nuclear smuggling and terrorism[26]. In 2015, the Associated Press reports at least four attempts in which criminal networks sought to sell radioactive material to extremists in 2015[27]. Also in 2015, the potential for terrorist use of chemical agents was illustrated by reports that the Islamic State (ISIS) used chemicals in military operations[28]. These are not isolated cases: a recent report found nearly 300 cases of export control violations by non-state actors supplying nuclear-related goods to Iran[29]. The December 2015 Plenary meeting of the Wassenaar arrangement "*underlined the importance of further strengthening export controls … to prevent the acquisition of … dual-use goods and technologies by terrorists*[30]".

1.2.1.2 Emergence of new risks of cyber-surveillance trade.

New risks are emerging and appear increasingly relevant to export controls. Since the Arab Spring in 2011, there have been numerous reports of cyber-surveillance technologies being exported to repressive regimes and/or in conflict areas, in some cases by companies based in the EU, and misused in violation of human rights. Moreover, over the last years, cybersecurity - sometimes described as the '4th dimension' of war - has emerged as a key security consideration and the threats that cyber-technologies pose to international security are an increasing concern. In particular, there is a risk that items with inherent dual-use capabilities may be misused against countries' critical infrastructures, or even to steal intellectual property from companies including trade secrets and confidential business information. A resolution of the European Parliament of 17 December 2015 thus emphasises that "the proliferation of certain surveillance and intrusion technologies around the world cannot only be detrimental to human rights but might also pose a significant threat to European strategic interests and our digital infrastructure"[31].

Cyber-surveillance technologies have legitimate and regulated law enforcement applications, but have also been used for internal repression by authoritarian or repressive governments to infiltrate computer systems of dissidents and human rights activists, at times resulting in their imprisonment or even death. As evidenced by numerous reports[32], the export of cyber-surveillance technology under such conditions poses a risk for the security of those persons and to the following fundamental human rights:

- Right to privacy
- Freedom of expression
- Freedom of association
- Freedom from arbitrary arrest and detention
- Right to life
- Freedom from torture, inhuman treatment and degrading treatment.

In certain instances, the Regulation may also affect certain other fundamental rights: in particular, controls of dual-use research need to respect academic freedom and the right to health.

The European Parliament has called repeatedly for the EU to ensure transparency and accountability of the trade in surveillance technology[33]. Most recently, the Parliament urged for action following the hacking of "Hacking Team", an Italian company that sells spyware all over the world, as revelations from leaked internal documents demonstrated that these tools were sold to the governments of countries whose human rights records the EU has criticised, in the absence of applicable legislation[34].

From a legal perspective, the EU has recognised the threat of illegal interception of electronic data transmission: Directive 2013/40 on attacks against information systems[35] provides that "*intercepting, by technical means, non-public transmissions of computer data … intentionally and without right, is punishable as a criminal offence…*". In December 2015, the European Data Protection Supervisor (EDPS) published an Opinion on *Intrusive surveillance technology*, and warned that "a*s the unregulated market for the trading and use of covert monitoring technology continues to grow, the EU must not underestimate the appetite for such technology. By addressing weaknesses in existing legislation and policies as well as developing new legislation, the EU legislator can help protect against the very real threat posed to our privacy and data protection rights."*

1.2.2 Rapid technological and scientific development.

The rapid spread of technological and scientific developments is a traditional challenge in many areas of control such as nuclear, chemical, and biological or aerospace. Some dual-use items such as semiconductors are at the heart of a myriad of innovative products such as computers or automobiles, wind turbines, solar panels or LED bulbs, but also have numerous military applications e.g. for night-vision cameras or missile guiding systems. Consequently, multilateral export control regimes devote considerable resources to the regular updating of controls so that they remain technologically and commercially current, and the EU, in turn, updates its control list each year[36].

Since the turn of the century, however, the emergence of new and advanced technologies with dual-use applications - such as additive manufacturing/3-D printing, cloud computing, nanotechnology, graphene research – increasingly add to the complexity of strategic controls. For example, research in synthetic biology supports the development of innovative medical solutions, but also raises the possibility that new pathogens could be created and creates a need for authorities to develop an understanding of the challenges it poses. As another example, additive manufacturing is also increasing the challenge posed by technology transfers: in the US, judiciary proceedings are ongoing after the publication of a 3-D printed gun was prohibited under export control legislation in 2013[37].

1.2.3 Transformations in global economic activity.

The rise of global supply chains means that the development and production of dual-use items happen in a series of steps across many countries and is increasing the risks associated with dual-use trade.

Expanding global trade and interconnected data networks increase the opportunities for state and non-state actors to acquire dual-use equipment and technology – legitimately or not. As a result, proliferation risks move across borders and jurisdictions along integrated value chains, as proliferators take advantage of their complexity and vulnerability. Proliferators mobilise increasingly sophisticated support networks characterised by the presence of unsuspicious legitimate operators (such as suppliers, service providers or transport operators unfamiliar with proliferation risks).

Global supply chains also mean that the volume of dual-use goods being trans-shipped via third countries is continuously expanding, thus increasing the risks of diversion to countries of concern (for example, EU exports to major trans-shipment hubs such as the United Arab Emirates have increased by 130% from 2004 to 2014, at a time when they were significant risks of diversion to e.g. Iran).

Moreover, as exports are increasingly 'transmitted, not transported', online trading platforms are transforming the nature of supply chains and making it possible for anyone, anywhere to act as a middleman or broker in a dual-use export transaction. Also, the greater diffusion of dual-use knowledge offers easier acquisition pathways as sensitive information – "intangible technology" - is easy to transfer via electronic means (e.g. plans for a nuclear bomb available on the internet).

Furthermore, the growing importance of emerging economies, multinational companies and industrial processes within worldwide production networks and supply chains results in an increasing foreign availability of dual-use items. Foreign availability can be illustrated by economic data concerning some key dual-use sectors[38]. Thus, in the aerospace sector, world regional shares of global civilian revenues are projected as follow for 2020: 33% North America, 33% Europe, 15% Asia Pacific and the rest divided equally between Middle-East, Latin America and Africa. In the chemical sector, the total value of EU sales (EUR527 billion in 2013) has been continuously growing, but overall world chemical sales have outpaced that rate of growth and the EU contribution to world chemical sales between 2003 and 2013 dropped by 14.5%, from 31.2% in 2003 to 16.7% in 2013. In the machine tool sector, where the EU is still a leader with a production of EUR 19.8 billion, big producers now include China (EUR 12.9 billion), Japan (EUR 9.7 billion), South Korea (EUR 4.2 billion), the United States (EUR 3.7 billion) and Taiwan (EUR 3.5 billion). For its part, the Information and Communication Technology (ICT) industry is highly globalised, and European operators face stiff competition from other developed and emerging economies, particularly in Asia.

1.2.4 Asymmetric implementation of controls within the EU.

The EU system provides for a number of actions, especially with respect to implementation and enforcement, to be conducted by national competent authorities. This flexibility is inherent to the system and, to an extent, supports the effective implementation of harmonised EU controls thanks to the proximity of authorities to economic operators and their capacity to adjust to national economic conditions. This however also results in diverging interpretation/application of controls within the Single Market in relation to certain provisions of the Regulation (e.g. the determination of the competent authority), with respect to licensing conditions and requirements, and the application of catch-all controls on non-listed items.

In some cases, the Regulation itself provides, by design, for the possibility of national controls. In total, 12 Member States have introduced some form of national control measures. For example, seven Member States have National General Export authorisations (NGEAs)[39] These national measures sometimes cover a significant portion of licensed exports (approximately 6%): a total of over EUR 2.8 billion was exported under NGEAs in 2014. In other cases, the lack of detailed provisions open the door to diverging application of controls. For instance, the lack of indications regarding the validity of

licences or the licensing timeline result in greatly varying situations throughout the EU, with inevitable distortions of competition among exporters operating from the Single Market.

Differences between Member States also appear as regards the cost of controls. With approximately 39.000 applications and 28.000 individual licenses[40] granted in 2013 in the EU, the volume of licences processed highlights the fact that export controls represent a significant administrative burden for both companies and competent authorities.

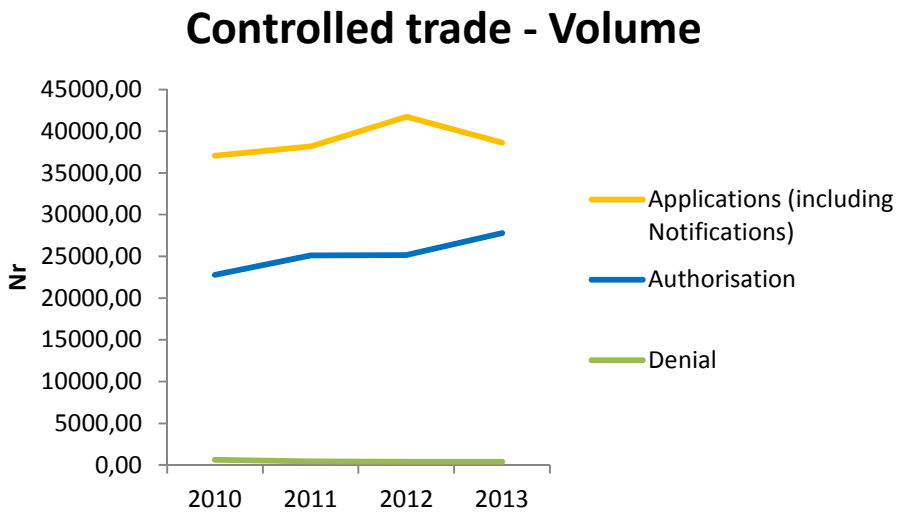


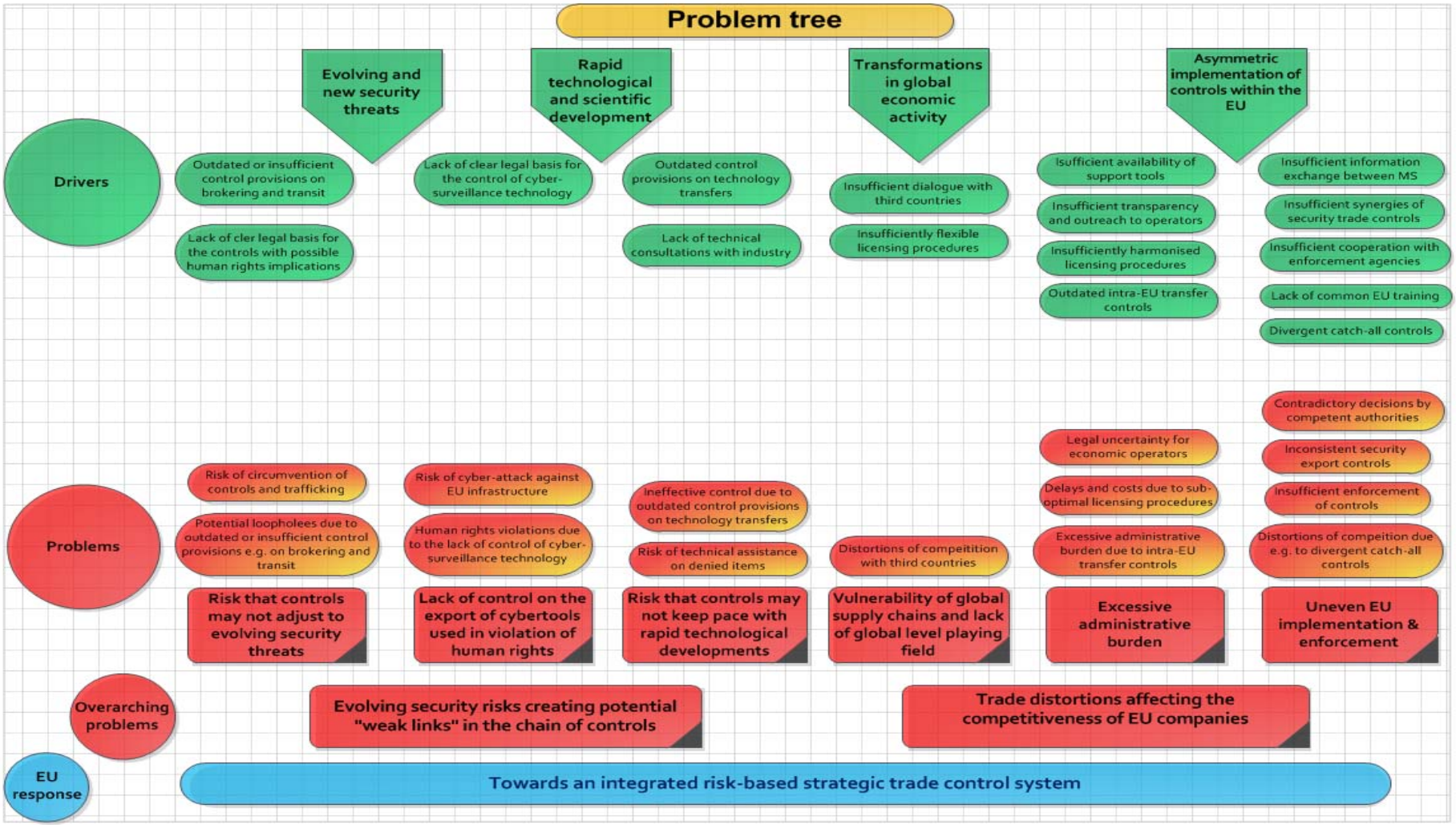
Figure 2: Volume of applications, authorisations and denials for (2010-2013)

In parallel to the asymmetric implementation of controls, the overall administrative burden relating to controls masks a variety of situations. Throughout the EU, resources and budgets allocated to export control differ markedly from one Member State to another, ranging from approximately EUR 100,000 up to EUR 6 million in 2014[41]. In practice, the administration cost of controls is not limited to licensing, which is only the tip of the iceberg as export controls require inter-agency cooperation involving various ministries as well as customs, intelligence and technical services, e.g. for international representation, technical expertise and enforcement.

With respect to economic operators, the administrative burden associated with controls essentially relates to compliance costs, licensing delays and legal uncertainty. Costs are mainly related to the classification of items (large enterprises can have thousands of items – including parts and components - potentially falling under dual-use lists or affected by catch-all provisions), but also to licencing procedures, dedicated IT infrastructure, training etc. Compliance costs vary greatly between companies and are not separate from other security trade measures (such as sanctions). From available data, it appears that, at central (headquarters) level, resources dedicated to controls remain limited: 77% of surveyed companies declare that they have up to 10 full-time equivalent (FTE) staff in charge of export control and that related costs can be as high as EUR 4 million per year for big companies. For SMEs, equivalent figures provided by companies were substantially below, often less than four FTE and approximately EUR 200,000 per year. Based on licensing data and consultations with key experts, it can be estimated that the overall yearly cost of licensing in the EU exceeds EUR 100 mln.[42]

Licensing delays appear as an important risk for economic operators, especially as they may in some cases lead to a cancellation of sales and thus cause a potentially large financial loss. On average, a few weeks are required for processing licence applications (UK published data report an average licensing time of 15 days), but this overall figures mask large variations in processing times - from a few days to several months in certain cases.

1.3 Problem tree.



1.4 Identification of the stakeholders: Who is affected by the problem?

1.4.1 Industry stakeholders.

A variety of economic operators in a variety of sectors are concerned by export controls, as they affect directly the freedom to conduct a business. This includes primarily exporters and manufacturers involved in the supply of goods, technology and services with dual-use applications in areas such as energy, aerospace, defence and security, transport and navigation, telecommunications, chemical and pharmaceutical industries, manufacturing and material-processing equipment, electronics, semiconductor and computing industries. While there is little authoritative data describing the "elusive dual-use sector", sector data may provide useful indications regarding key "dual-use industries" – i.e. industries affected, *to some extent*, by export controls – and their economic significance.

- The ***aeronautics, space, defence and security industries*** in Europe has a turnover of EUR 197.3 billion, invest EUR 20 billion in Research & Development (R&D), and counts over 3000 companies and 80,000 suppliers, many of which are SMEs[43]. According to the Aerospace Security and Defence association (ASD), much of its activity is affected by export controls.

- The ***machine tools industry*** is a key sector of modern manufacturing, with Europe as a global leader: European machine tools production reached EUR 19.8 billion in 2014 and exports reached EUR 9.1 billion. The sector is significantly affected by controls: the European association of machine-tool industries (CECIMO) estimates that more than 80% of European cutting machine tools are classified as dual-use[44].

- The ***electronics / semi-conductor*** industry supports around 200,000 jobs directly and more than 1,000,000 indirect jobs in Europe. EU exports of integrated circuits exceeded EUR 11 billion in 2014. Semi-conductors enable the generation of more than 10% of GDP in Europe and the world and the value of products comprising micro- and nano-electronic components represents around EUR 1,250 billion[45].

- The ***ICT industry*** is widely affected by controls since encryption (which is controlled at a certain level) is an integral part of most digital technology. In 2014, dual-use related exports of electronics were worth EUR 28.8 billion, dual-use related exports of telecommunications and 'information security' were worth EUR 32.5 billion, and dual-use related exports of computers were worth over EUR 15.6 billion[46]. Within the broader ICT sector, the size of the ***cyber-surveillance industry*** is difficult to estimate precisely, but estimates for the cyber-security industry indicate for example that it reached USD 75.4 billion in 2015.[47] Some studies offer insight into specific industry segments and indicate that the cyber-surveillance industry itself is significantly smaller in size – some NGOs estimate that it is worth USD 5 billion a year[48]. In its strictest sense, when targeting security firms that market highly-specialized systems of intrusion or surveillance to law enforcement and intelligence agencies, the market appears to be limited to a few small but highly mobile (companies may easily relocate in other countries) and global companies.

- The EU ***chemical industry*** ranks second globally, but is the leading exporter of chemicals in the world, with exports totalling EUR 139 billion. The sector is partially affected by controls with less than 10% of exports concerning dual-use chemicals[49].

- The ***civil nuclear sector*** generates 27% of the EU's electricity, representing half of the EU's greenhouse gas free electricity[50], and supports 217,589 direct jobs in the EU[51]. The civil

nuclear sector is almost entirely subject to dual-use controls, as nearly all of the principal items and components are listed.

Critically, dual-use controls affect emerging sectors which are key to the EU's Innovation capacity. For example, drones have a variety of civilian and military applications and appear as the most dynamic segment of the aerospace industry. The market for military drones is expected to almost double by 2024 to beyond USD 10 billion[52].

Naturally, industry stakeholders will only be affected by changes to export controls to the extent that they apply to the type of dual-use items they trade. For example, the chemical industry could be directly affected by changes to licensing processes for low-value shipments (since chemicals can typically be exported in samples) but would hardly be concerned by changes to encryption controls.

1.4.2 SMEs.

Industry stakeholders include multinationals and some of the biggest companies in the EU, but also a large number of SMEs. The example of the defence sector, which typically produces items with both military and civilian uses (i.e. dual-use), provides a good example. In 2012 there were around 1,184 firms operating in the defence industry in Europe[53], with a total turnover of more than EUR 17 billion and employing around 120,000 people. The majority were small firms: firms of less than 10 employees represented 76.7% of the total number operating in the sector in Europe[54].

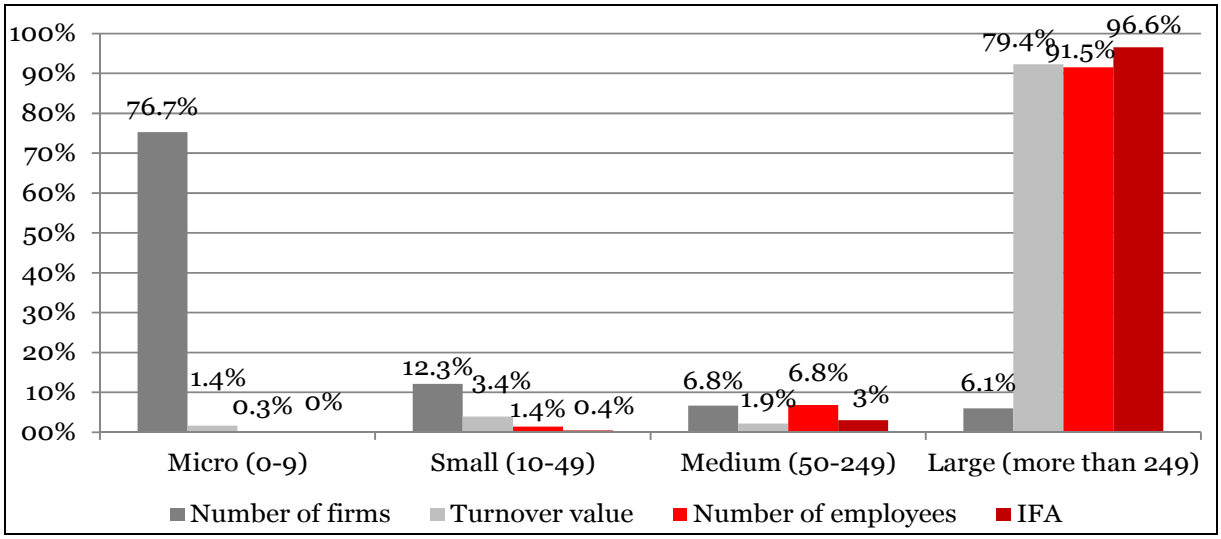


Figure 3. Distribution of the number of firms in the defence sector, with their respective turnover, number of employees and investments according to size, 2012[55].

1.4.3 Service providers and researchers.

Industry stakeholders also include service providers involved in dual-use trade - such as brokers, consultants providing technical assistance or resellers. Specific communities may be affected by specific aspects of controls e.g. Intangible Technology Transfers (ITT) controls particularly affect multinational companies and research institutes/universities. As another example, the internet security research community is concerned specifically by controls on cyber-surveillance technology.

1.4.4 Government stakeholders.

Member States have a direct interest in the initiative due to their responsibility in the negotiation of decisions on controls in multilateral regimes, and their administration, implementation and

enforcement at national level. Departments involved in managing, monitoring and enforcing export controls include licensing authorities, ministries of economy and trade, foreign affairs, defence as well as customs and intelligence agencies.

Third countries may also have an interest in the initiative, as it will affect bilateral trade and/or security (for ex. the export of dual-use items for military applications in one country may cause concerns in another country).

1.4.5 Civil society stakeholders.

Civil society has an increasing interest in export controls, in particular due to their positive impacts on human rights. For example, various NGOs formed in 2014 the Coalition Against Unlawful Surveillance Exports (CAUSE)[56] calling for the control of exports of cyber-surveillance technologies in order to prevent human rights violations.

The wider public may also indirectly benefit from increased security and competitiveness of EU dual-use industries, especially as export controls aim at preventing sensitive technologies from falling into the "wrong hands" and the broader security implications are of relevance for virtually all citizens. Exports of dual-use items may also affect fundamental rights, in particular those of people in third countries, such as the right to life and the prohibition of torture and inhuman and degrading treatment, the right to security[57], to health and to academic freedom. In addition, cyber-surveillance technology creates new risks to specific human rights (as outlined in 1.2.1.2.), and civil society in third countries – and in particular human rights activists and dissidents - may also benefit from enhanced controls.

1.5 Dimension of the problem.

Although there is little authoritative quantitative data on the 'dual-use sector[58]', the magnitude of the problem associated with the export control policy review may be approximated in relation to 1) the scope of the dual-use industry, 2) the importance of dual-use trade and 3) the extent to which problems are already addressed by the Regulation. Dual-use related data or partial/sectoral data may be useful to illustrate the importance of dual-use controls for the EU economy and to assess the dimension of the problem at a general level, while duly recognising the limitations of this exercise, in particular as the security and human rights dimensions of the problem are inherently not quantifiable, and considering the lack of data relating to specific control provisions.

1.5.1 The economic dimension: the EU dual-use industry.

The EU has an extensive dual-use industry that brings together thousands of small, medium and large companies providing high value-added jobs and know-how - including significant R&D work. Dual-use industries may be found in all Member States, but there is a degree of concentration of dual-use industries in certain Member States, with the top 4 exporters (Germany, UK, Netherlands and France) accounting for over 80% of dual-use exports in value.

Dual-use items are often high-tech products and include leading edge technologies that are crucial to the EU's drive towards innovation and competitiveness. For example, the semiconductor industry, is one of the most innovative industrial sectors in Europe and consistently ranked among the very top R&D intensive sectors. In reality, dual-use items have ramifications across a wide range of key sectors of the EU economy. The classification of dual-use items in the Regulation is as follows:

Category 0: Nuclear materials, facilities and equipment

Category 1: Special materials and related equipment

Category 2: Materials processing

Category 3: Electronics

Category 4: Computers

Category 5: Telecommunications and “information security”

Category 6: Sensors and lasers

Category 7: Navigation and avionics

Category 8: Marine

Category 9: Aerospace and propulsion.

A quantification of the dual-use industry based on production values would be useful to assess its share in the EU economy, but there are no dedicated statistics, and estimates can only be based on the corresponding production data for the largest relevant sectors. The size of the EU ‘dual-use *related* industries' –- that produce, inter alia, dual-use items - has thus be estimated at over EUR 600 billion[59]. This data usefully sheds some light on the economic context of controls, but presumably largely exceeds the actual size of dual-use production itself and cannot be used a reliable estimate when assessing the impact of specific review actions.

1.5.2 The trade dimension: dual-use exports.

Licensing data is probably the most direct and reliable measure for assessing the importance of the dual-use industry to EU trade. According to the 2013 data, the value of EU 'controlled exports'[60] reached EUR 85 billion, representing approximately 4.9 % of extra-EU exports. Authorised exports of dual-use items amounted to EUR 48 billion, representing 3.1**%**. By contrast, only a small portion of exports were actually denied: approx. 260 denials were issued in 2013, representing about 0,06% of the value of controlled dual-use exports in that year, and a negligible portion of total EU exports (Figure 4)[61].

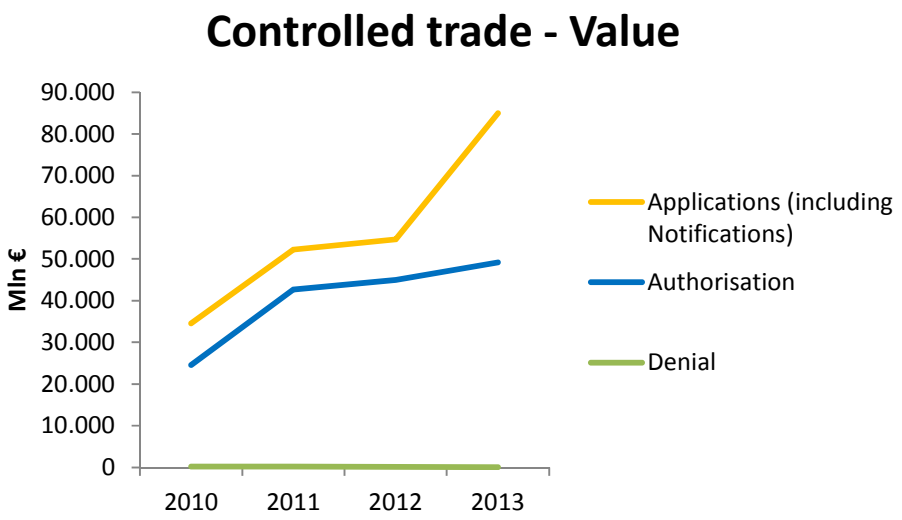


Figure 4: Value of applications, authorisations and denials for (2010-2013) (mln EUR)

In some cases, available licensing data shed some light on the importance of the problems relating to specific control provisions –such data is used, where available, in the assessment of concrete actions. It should however be noted that the low number and value of denials is not a reliable indicator of the

dimension of the problem or of the administrative burden placed on administrations and exporters, since export controls do not operate as a ban and are designed in a way as to minimise negative impact on trade, and most dual-use exports concern purely civilian operations.

The EU is a major exporter of dual-use items and trade in dual-use items is an integral part, and represents a significant portion, of trade with key partners (Figure 5).

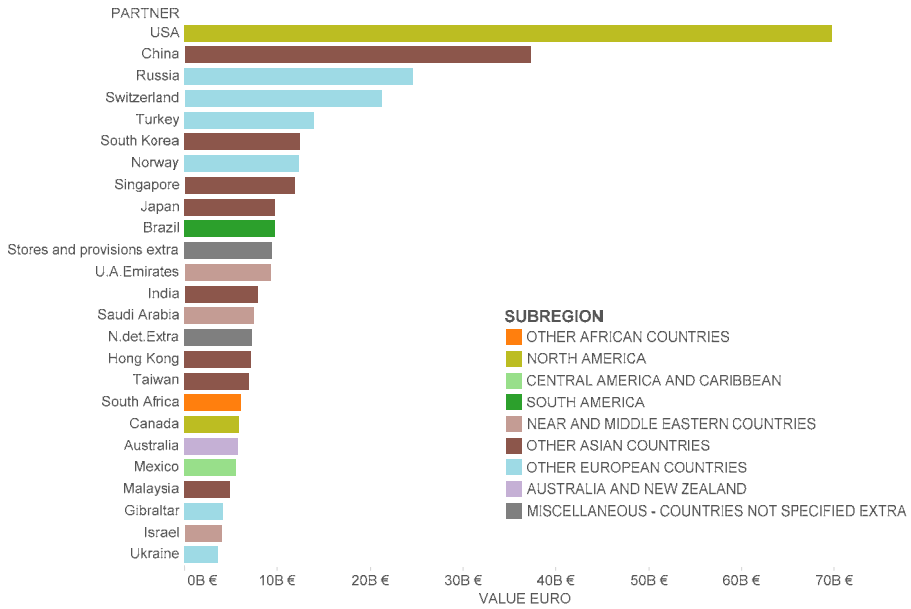


Figure 5: Destination countries and sub-regions for EU dual-use related exports in 2013[62].

Here again, available licensing data do not precisely relate to the dimension of the problems identified in the review, but offer useful contextual elements. Some data more precisely relates to certain aspects of the problems. For instance licensing data on brokering controls or transit controls enable a more precise assessment of the dimension of those particular aspects of problems. Where available, such data is used when assessing the potential impact of review actions.

1.5.3 The social dimension.

Industry associations recognise that they are not in a position to assess the potential social dimension of the dual-use sector with precision, for lack of relevant data. In spite of the scarcity of data, it is clear that EU dual-use industries are important in terms of employment: in the period 2008-2012, between 7 and 8.5 million employees were active in dual-use *related* sectors, though, again, the number of employees working in *actual* dual-use enterprises is likely to be much smaller[63]. Considering that, across the EU, 31 million jobs, i.e. 14% of total employment, depend on exports [64], it can be estimated that extra-EU dual-use exports support approximately 1 million jobs[65]. It should be noted that dual-use industries, taking into consideration also production and intra-EU trade, support an even higher number of jobs.

Sector data may provide useful insight into the social dimension of controls in general - for example:

- the European machine tools industry employed about 135,000 people in 2013 and creates approximately an additional 600,000 jobs via its supply chain[66];
- chemical companies employed about 1.2 million people in the EU, and the sector generates a greater number of indirect jobs that is estimated to be up to three times higher[67];

- the aeronautics, space, defence and security industries employ close to 778,000 people[68].

As for economic and trade data, however, data cannot be disaggregated to the level of review options and actions, and offer more of a contextual information for the overall assessment.

1.5.4. The regulatory dimension.

The Regulation ensures that international commitments of the EU and its Member States are complied with, and problems arise only insofar as the Regulation does not sufficiently or effectively address and imperfectly adjusts to evolving risks or changing technological and economic developments. The review, by its very nature, will therefore essentially consist in adjustments to existing controls and the dimension of the problems will be limited to this need to adjust the system to changes in the environment..

Most review actions envisaged under options 2 and 3 of this report in fact aim at adjusting and refining *existing* controls: they seek to clarify, simplify or, in certain cases, possibly extend certain *existing* provisions of the Regulation. For example controls on brokering, transit or technical assistance are already in place under the Regulation, but e.g. differ among Member States or do not take into consideration specific aspects such as terrorism or human rights.

1.6 Analysis of the export control system: the case for a review of export control policy.

In light of the requirements of Article 25 of the Regulation, the Commission issued in 2011 a Green Paper[69] highlighting the development of the EU export control system over the last decade and launching a broad public debate concerning its functioning and future strategic options. The Green Paper marked the first step toward preparing the review required under Article 25 of the Regulation.

As a result, the Commission Staff Working Document[70] “Strategic export controls: ensuring security and competitiveness in a changing world" identified the main issues raised by stakeholders as regards the strengths and weaknesses of the EU export control system. It showed that most stakeholders agree that the EU export control system provides solid legal and institutional foundations, but also concur that it cannot remain static and needs to adjust to a changing security, technological and economic environment, to prevent the emergence of potential security gaps, and to avoid trade distortions affecting the competitiveness of EU companies.

As requested under Article 25.2 of the Regulation, the Commission then presented, in October 2013, a report to the Council and the Parliament[71], which recognized the need to upgrade the EU export control system and opened the way to the review of EU export control policy.

For their part, the European Parliament, the Council and the Commission have jointly agreed that a "modernisation and further convergence of the system is needed in order to keep up with new threats and rapid technological changes, to reduce distortions, create a genuine common market for dual-use items (uniform level playing field for exporters) and continue serving as an export control model for third countries"[72].

CHAPTER 2 - THE NEED FOR EU POLICY INTERVENTION: SUBSIDIARITY AND PROPORTIONALITY

As confirmed by the Court of Justice[73], dual-use export controls form an integral part of the Common Commercial Policy. The EU therefore has the right to act, based on exclusive competences under Article 207 TFEU.

Even so, according to the subsidiarity principle, the EU should act only where it can provide better results than interventions at Member States level. With due respect to Member States' prerogatives in the area of security, EU intervention is necessary as the security objectives pursued can only be achieved collectively, if competent authorities act in close collaboration and in accordance with the same principles so as to ensure that there is no "undercutting" of exports. Action at EU level is also necessary to address distortions of competition within the Single Market. Thirdly, EU intervention and dialogue with key trade partners is valuable to promote the level-playing field globally.

EU intervention is also necessary to protect fundamental rights in light of the Charter of Fundamental Rights, since a number of human rights have been identified as potentially affected by exports, in particular in relation to exports of cyber-surveillance technology, but also e.g. related to biological items[74].

EU legal acts must comply with the Charter of Fundamental Rights of the EU and, in line with the Better Regulation principles, an assessment of impacts on fundamental rights must be carried out when designing EU policies and legislation. The options identified in this document therefore comply with the principles of proportionality in so far as they are limited to what is necessary in order to attain the objectives laid down in section 3.

CHAPTER 3 – OBJECTIVES: WHAT SHOULD BE ACHIEVED?

3.1 General Objectives

According to Article 207 TFEU, the common commercial policy shall be conducted in the context of the principles and objectives of the Union's external action and in accordance with the EU's international commitments.

Accordingly, the EU export control policy review aims at supporting the overall policy objectives of the Union, as laid out in Article 3 of the Treaty on European Union, i.e. "contribute to peace and security, as well as free and fair trade and the protection of human rights". Modernised and effective export controls will also ensure that the EU and its Member States effectively comply with their international obligations, in particular with respect to WMD non-proliferation.

3.2 Specific Objectives

In light of the identified problems, the specific policy objectives of the export control policy review are to:

- Ensure that EU export controls adjust to evolving security risks and threats;
- Ensure that controls adjust to rapid technological and scientific developments;
- Prevent the export of cyber-surveillance technology misused in violation of human rights;
- Reduce the distortions of competition and administrative burden associated with controls;

- Promote a global level playing field;
- Support effective and consistent application of controls in the EU.

Overall, the review options and actions identified and assessed in this document aim at striking the right balance so that facilitating trade and reducing the administrative burden does not come at the expense of security or human rights. Ultimately, enhancing the security of the supply chain through robust export controls will protect legitimate trade and contribute to its development. Annex VI provides a detailed description of the links between problems, obectives and options.

3.3 Consistency with other EU Policies

The objectives are fully in line with EU foreign and security policies. The export control policy review will contribute to the European Security Strategy, and in particular responds to the 2013 Council Conclusions on ensuring the continued pursuit of an effective EU policy on the new challenges presented by the proliferation of weapons of mass destruction (WMD)[75].

The review options concerning "Human security" and the control of cyber-surveillance technologies could contribute to the protection of human rights globally as illustrated by the 2012 and 2015 Human Rights Action Plan and the EU's Guidelines for Freedom of Expression, which explicitly call for tightening controls on the export of such technologies.

The objectives are also fully in line with EU trade policy's aim to foster competitiveness and reduce distortions to trade, and with the 2015 "Trade for All" Communication's[76] announcement of specific proposals for *"an ambitious modernisation of the EU´s policy of export controls of dual-use goods, including the prevention of the misuse of digital surveillance and intrusion systems that results in human rights violations"*.

The export control policy review will also contribute indirectly to other EU policies e.g. proposals for fixing the vulnerabilities created by the trade in cyber-surveillance technologies are in line with the digital single market strategy. Since the export control policy review aims, in particular, to make EU law simpler and less costly and seeks for more effective ways to achieve its objectives, it serves the objectives of the REFIT programme.

CHAPTER 4 – POLICY OPTIONS: WHAT ARE THE VARIOUS OPTIONS TO ACHIEVE THE OBJECTIVES?

4.1 Identification and description of the policy options

In light of the initiatives envisaged in the 2014 Communication, five options have been identified which range from the continuation of the current export control system to its complete overhaul and full harmonisation, with other options between these extremes.

4.1.1. Policy Option no. 1 – "Baseline".

This option would leave the current legislation, administrative and IT arrangements unchanged, maintaining a well-known system in place. The current system would allow limited regulatory actions to take into consideration security, economic and technological evolutions e.g. since 2014 the EU list of dual-use items can be adjusted regularly through delegated acts. Similarly, limited cooperation and exchange of information between competent authorities is possible with the existing system, using current administrative resources, to support consistent implementation and enforcement.

4.1.2. Policy Option no. 2 – "Implementation and Enforcement Support".

This option would address problems associated with the lack of clarity and transparency and uneven implementation of controls, and with rapid technological and scientific developments. This option would combine a series of soft law, non-regulatory actions (avoiding regulatory changes and concrete support actions by national and EU administrations to develop the EU system and promote a consistent and effective implementation and enforcement of controls. The following actions are envisaged:

- ***Development of an EU export control network***. This action would focus on strengthening cooperation and coordination between the competent authorities of the Member States. Its operational objective would be to develop a more integrated and effective EU export control network. The action could be put in practice via the following measures:
  - Enhanced information exchange between competent authorities. The Commission and national authorities could develop structured exchange of information on key data (e.g. catch all controls, sensitive destinations and end-users, violations, global licence users), using and expanding, as necessary, the existing IT information-exchange system – the DUES. This would provide a common and robust information basis for risk assessments by competent authorities and thus support the effective and consistent implementation of controls throughout the EU;
  - Development of security export controls synergies. The EU implements various instruments (regulations, directives, decisions) to control the trade of various sensitive or strategic commodities (such as dual-use items, arms/defence items, firearms, 'torture goods', goods subject to restrictive measures/sanctions), conflict diamonds, drugs etc). These instruments rely on common principles and tools but are managed by different services, at EU and national levels. The action[77] could involve the pooling of expertise and the development of a common IT infrastructure to serve as a shared platform for exchange of information on controlled exports (possibly building on the existing DUeS IT platform);
  - Enhanced cooperation with Member State enforcement agencies. While enforcement is the responsibility of specific agencies of the Member States, cooperation and information exchange could be improved at EU level, e.g. through the setting-up of an "enforcement coordination centre" attached to the Dual-Use Coordination Group[78] and the development of synergies with other security & trade related programmes such as Authorised Economic Operators (AEO)[79] programme (in cooperation with customs);
  - Development of an EU capacity-building programme. This action would imply the development, by the Commission and national authorities, of a common training programme for officials of relevant authorities (primarily licensing and customs but also other enforcement agencies) – a so-called EU "Inreach" training programme - could be inspired by the ongoing "outreach programme" providing capacity-building to third countries[80].
- ***Transparency and partnership with the private sector***. This action is based on the observation that regulatory compliance and competitiveness are mutually reinforcing and would focus on the interaction between authorities and the private sector as the 'first line of defence' against evolving security risks. The operational objective is to enhance the security and resilience of the global supply chain and reduce the risk of corporate involvement in exports that expose

firms to penalties and wider reputational damage. It could be put in practice via the following measures:

- Transparency measures would expand outreach and information-sharing with operators, e.g. through the publication of informative annual reports by the Commission and of information supporting the application of controls (for example guidance for exporters on topical issues, "technical notices" laying out best practices helping companies to apply controls to new technologies[81]). Transparency would also enable the European Parliament and civil society organisations to fully contribute to the formulation and implementation of export control policy.
- The development of tools for operators. This would form another key element of the partnership and respond to industry's call for a common interpretation and application of rules. It would involve the development of e.g. EU-wide industry compliance standards for private sector, confidence-building measures such as codes of conduct for dual-use researchers. It could also include the introduction of electronic licensing systems in all Member States, based on the experience of those competent authorities that already operate such systems, thus providing for IT-based management of licensing processes and relations with economic operators.
- The development of a 'smart security' mechanism could take the form of "technical advisory committees", as inspired by US practice, bringing together key industry players with Government experts to engage in a dialogue on the technical parameters for controls. Such technical consultations would support regular updates of the EU control list and also pave the ground for EU coordinated inputs into discussions in multilateral export control regimes.

- ***Export control dialogue with third countries***. The action would involve the development of regular dialogues between the EU and key trade partners, and could consist of measures such as regular and reciprocal exchange of information, the possibility to negotiate agreements with third countries e.g. to allow for end-user verification programmes (whereby selected third-country companies could be granted special status of "Verified end-user" and obtain EU-wide recognition and facilitation of controls), mutual recognition of Internal Compliance Programmes (ICPs) etc. Its operational objective would focus on regulatory convergence and the global level-playing field.

4.1.3. Description of Policy Option no. 3 – "EU System Upgrade".

Drawing on "lessons learnt" from the implementation of various provisions of the Regulation, this option would address problems associated with lack of clarity and transparency, uneven implementation of controls and the risks associated with rapid technological and scientific developments and the interconnected global trading system. It would consist of various adjustments to the current regulatory framework, introducing amendments to the Regulation in order to simplify it and/or to make it more effective and efficient. It would essentially combine 4 actions:

- ***Modernisation of existing control provisions***. The operational objective of this action would be to clarify, simplify and improve the regulatory framework in light of "lessons learnt" and new developments. This could be put in practice via changes to various control provisions:
  - The clarification of key export control notions should reflect new realities. Thus, the definition of exporter in Article 2.3 of the Regulation reflects the original focus of controls on exports of tangible goods while the notion of exporter today extends to

e.g. service providers, researchers, consultants and even a person downloading "controlled technology". As another example, experience has evidenced difficulties with the determination of the competent authority in Article 9 of the Regulation, e.g. in situations where the owner of the controlled items is established outside of the EU. This provision also fails to capture the situation of natural persons, which may be "exporters", especially when it comes to technology transfers. Moreover, in order to avoid conflicting decisions by competent authorities, it is important to clarify that the determination of the competent authority applies to all control operations (incl. e.g. a decision on decontrol of items), and not only to the granting of a licence, as it currently does.

- 64% of surveyed industry associations see a need for a legal clarification of intangible technology transfers controls (ITT), especially as experts reports suggest that ITT, including technical assistance, plays an increasing role in proliferation. For example, an amendment to the Regulation is need to ensure the control of *technical assistance* where the supply of services or the transmission of technology involves a cross-border movement of persons, as this has become EU competence since the entry into force of the Lisbon treaty[82]. The action could also involve the introduction of references to ITT in various definitions, such as the definition of exporter;

- Tackling illicit trade: the Regulation sets up a system for controls of legal exports, but should be strengthened to counter the illicit trafficking of dual-use items – a dimension largely absent from the Regulation - and provide a robust basis for enforcement. Also, best practices from other security trade instruments, such as sanctions regulations, could be transposed in the export control area. For example, the Regulation applies controls on the export of items from the EU customs territory, which is ill-suited to intangible technology transfers and does not address the risk of circumvention by EU persons in third countries. In line with best practice in other trade security instruments (sanctions), it could be appropriate to apply controls throughout the EU jurisdiction – including on EU persons located in third countries. Similarly, it would be useful to introduce an anti-circumvention clause, i.e. a prohibition of actions which intentionally circumvent controls, thus establishing a solid EU-wide legal basis for the prosecution of export control violations.

- Strengthening of brokering controls: the EU controls brokering services for dual-use items where there are concerns about a particular transaction[83]. Experience however shows that the *definition of brokering* does not capture certain situations e.g. when the items are located in the EU or when the broker is resident outside of the EU. Moreover, brokering controls include *optional elements* regarding their extension to non-listed dual-use items and for military end-uses. These discrepancies create legal confusion and fragmentation of controls across the internal market, and increase the risk that controls are circumvented. In order to ensure the consistency and effectiveness of controls, it could therefore be appropriate to harmonise their application to non-listed items and military end-uses and to extend their application to terrorist use and human rights violations. It could also be envisaged to cover brokering of export from the EU to a third country, and to strengthen the control mechanism e.g. through the introduction of registration and/or reporting requirements for brokers.

- Consistency of transit controls: as transit is used by proliferators to mask the final destination of items and thus evade controls, the EU controls the transit of dual-use

items where there are concerns about a particular transit operation[84]. Based on lessons learnt, measures could be proposed to enhance the consistency and effectiveness of transit controls. For example, the Regulation contains *optional elements* for Member States regarding the control of non-listed items and of military end uses, which could be harmonised at EU level in order to ensure a uniform level of control, and thus avoid distortions of competition and the risk of weak links in the chain of controls. The control of transit could also be extended explicitly to terrorist use and human rights violations, which are currently only indirectly covered.

- ***Optimisation of EU licensing architecture.*** The operational objective of this action would be to further harmonise licensing processes and reduce the share of individual licences in favour of control modalities that do not disrupt commercial transactions such as general authorisations. It could be put in practice via the following measures:
  - Harmonisation of licensing processes: this could be achieved through common parameters for global and EU general authorisations (EUGEAs) e.g. validity period and conditions for use of the licences (registration, reporting requirements...). A standard requirement for authorities' transparency on licensing timelines could also be introduced with a view to reducing differences in licensing timelines.
  - While under the current system, a majority of transactions are authorised under individual licenses, a shift towards open licensing would support increased use of general authorisations to facilitate trade while ensuring a sufficient level of security through robust control modalities e.g. reporting, compliance audits of companies, etc. This could be achieved through the following measures:
    - a regular *review of NGEAs*, by Member States and Commission experts, to examine their possible transformation, where appropriate, into EUGEAs. National authorisations would thus remain in place in recognition of the fact that they are considered by some operators as a useful element of flexibility, but would be subject to regular review and, where appropriate, their benefit would be extended to all EU operators;
    - a *delegation of competence* for the Commission to modify destinations or items on existing EUGEAs and/or introduce new EUGEAs (including as a result of the review of NGEAs mentioned above);
    - the introduction of *additional EUGEAs* and/or new licence categories for trade with non-sensitive countries, such as:
      - Cryptography: the facilitation of controls for products containing cryptography could be especially useful to compete with license exceptions existing in non-EU countries and given the commercial importance and wide circulation of these items;
      - Low Value Shipments: this would facilitate controls for shipments under a certain value (currently that value is set, under national control rules, at EUR 5000 in Germany and GBP 6000 in the UK) provided the shipment and destinations are eligible and certain conditions are met;
      - intra-company technology transfers: this would address the growing importance of ITT by facilitating transfers of dual-use technology within a

company in other non-sensitive countries, in particular for R&D purposes, as long as the technology remains under the ownership of the company;

- Large-projects: this would adapt licences to the specificities and duration of large multiannual projects e.g. construction of a nuclear power plant, providing the benefit of one single licence for all related export operations, for the duration of the project, subject to certain conditions (e.g. reporting, auditing).

- **Convergence of catch-all controls**[85]. This action would address the lack of consistency of catch-all controls, which are imposed by national authorities without consultation or information of other authorities and thus result in distortions of competition and uneven implementation of controls. The operational objective would be to improve the convergence of catch-all controls at EU level, via the following measures:

  - Clarification and harmonisation of the definition and scope of catch-all controls: as experience shows that competent authorities introduce catch-all controls with widely different scope and parameters, this could clarify that a catch-all control should covers specific items (rather than entire ranges of goods) and specific entities (rather than entire countries);

  - EU-wide application and validity of catch-all decisions: a mandatory consultation procedure between competent authorities could ensure that a common approach is defined for the application of specific catch-all controls;

  - Regular exchange of information: the Commission and Member States could set up a 'catch-all database' recording catch-all licensing requirements, end-users and items of concern. Data could be shared with customs and other enforcement agencies. Additionally, the transparency of catch-all controls could be enhanced, with some information available to the public (e.g. watch list of items published as guidance) so that operators are aware of risks.

- **Re-evaluation of intra-EU transfers**. This action would aim at minimising the burden and the remaining barriers to trade in dual-use items within the Single Market, while ensuring sufficient control of intra-EU transfers on certain particularly sensitive items (Annex IV items). It could consist of the following measures:

  - Review Annex IV: the list in this annex should be revised in order to focus controls on an updated list of most sensitive items, taking account of technological and commercial developments;

  - EUGEA for intra-EU transfers: a general transfer authorisation for the updated list of most sensitive items in Annex IV could facilitate trade within the EU, allowing for free circulation under certain conditions (e.g. registration, reporting, auditing, post-shipment verification) ensuring the security of transfers.

4.1.4. Policy Option no. 4 - "EU system modernisation".

This option would introduce a new "human security" dimension to the EU export control system, recognising the links between security and human rights and addressing the specific problem posed by the insufficient control of cyber-surveillance technologies. Its operational objective would be to respond to the proliferation of cyber-surveillance technologies whose misuse poses a risk to

international security and the protection of human rights and digital freedoms in a globally connected world. This option would essentially consist of two series of actions:

- **A review of the general approach to 'dual-use'.** The human security approach moves beyond the traditional military and state-centred approach to security – which underpins current regulations - towards a wider approach also taking into consideration the security of the EU, its citizens and companies. This could imply, firstly, a review of the definition of dual-use items to extend it beyond purely 'military' and WMD proliferation-related end uses to address broader security implications, including effect on security of populations e.g. terrorism, human rights violations.

  A revised definition for 'dual-use items' could be combined with a review of the control criteria, explicitly providing for controls to prevent exports where there is a clear risk of human rights violations. It could also include a clarification that criteria apply to all controls e.g. also transit, technical assistance and brokering, as this is not explicitly mentioned in the Regulation.

- **An initiative to control exports of cyber-surveillance technologies**. This action would build on measures outlined above and introduce specific provisions for an effective and comprehensive control of cyber-surveillance technologies. It could take the form of measures such as:

  - A due diligence requirement for companies to ensure that their exports of cyber-surveillance technologies are not destined to be misused in violation of human rights and do not pose a risk to international security;
  - An EU autonomous list of cyber-surveillance technologies, which would list specific items to be subject to controls, with detailed technical parameters. This would allow for EU decisions to control specific other dual-use items of concern, where considerations regarding the EU's essential security interests or respect for human rights warrant it.
  - A catch-all control, either integrated in the general catch-all clause or taking the form of a dedicated catch-all control for cyber-surveillance technology, which would allow controlling non-listed items where there is evidence that they could be misused.

4.1.5. Policy Option no. 5 - "EU system Overhaul".

This option would imply radically changing the EU approach to export controls, including full centralisation and harmonisation of controls towards the establishment of a central licensing agency at EU level. It would likely bring considerable costs – administrative, financial as well as in terms of legal transition – while potential benefits appear uncertain and remote. Consultations show that it would also likely face strong opposition as there is little evidence of any stakeholder support, while on the contrary many stakeholders – in particular Member States, but also some industry associations and companies - highlight the need to preserve the 'optimal equilibrium' between the EU and national levels of the system. This option is therefore not assessed further in this report.

Options 2, 3 and 4 include actions that could be complementary e.g. guidance or IT support tools to support the implementation of legislation – while options 1 and 5 appear as purely alternative policy options.

CHAPTER 5 – ASSESSMENT OF THE IMPACT OF POLICY OPTIONS.

A thorough analysis was conducted to assess the impact of the different review options identified. Then, option 2, 3 and 4 were compared to option 1 – the baseline. The assessment is based on Commission services' own analysis and practical experience, on data and contributions provided by Member States, on the findings of an independent data collection study, and on the results of consultations of stakeholders, including an online public consultation in July-Oct. 2015.

The following potential impacts were identified:

	Economic & trade	**Social, incl. security & human rights**	**Environment**
Direct	• *EU dual-use exports* • *Level playing field (incl. trade barriers, distortions of competition)* • *compliance costs & administrative burden for economic operators* • *Legal clarity* • *administrative burden for public authorities*	• *WMD proliferation* • *Transfer of sensitive technology to countries/persons of concern* • *Terrorism* • *Human rights violations*	*N.A.*
Indirect	• *International competitiveness* • *Innovation & research / ITT* • *Investment & production*	• *Employment*	• *Poss. climate change, transport, resource use, waste generation, environmental risks*

Table 1: Overview of impacts.

The assessment of the economic, social and environment impacts requires some methodological precautions. Considering that the export control policy review is not about setting up a new regulatory system, but rather suggests changes to an *existing* system, review options can only produce a *marginal* impact that will depend essentially on the scope of the controls concerned and on the importance of the change introduced by the review actions.

As far as economic impact is concerned, it is also important to note that export controls affect a limited share of total exports so that the economic impact of review actions will necessarily be very limited in relation to the overall economic activity in the EU. Even so, export controls can have a direct impact on the trade performance of specific industries, but review actions mostly concern – and will impact - only a fraction of all stakeholders subject to controls.

Due to the fact that there are no official statistics on dual-use production and trade, the impact assessment is based largely on qualitative analysis, results of industry surveys conducted in the context of a "data collection project" and of the online public consultation conducted by the Commission, with supporting quantitative data where available. Quantitative data include licensing data collected by Member States, sectoral or company data provided by industry, and analysis of related trade flows derived from EU trade statistics[86].

The public consultation highlighted that most respondents did not foresee significant social impacts stemming from the review options. Social impact can therefore rather be assessed in terms of security and human rights, as the export of dual-use items may have direct consequences in this respect. It should however be noted that controls are only one of many instruments in the toolbox to address security and human rights– therefore, here again, the impact of review actions can only be partial.

No direct impact on the environment is noted. 70% of surveyed companies do not identify any environmental effects related to the trade of dual-use items. Some of the associations, however, take the view that the use and consumption of certain dual-use items – e.g. advanced micro-processors – might generate mainly positive environmental effects, e.g. on air pollution and emissions, and energy and resource use. Facilitating the trade in dual-use items might thus, albeit very indirectly, have positive impacts on the environment. Overall, however, environmental impacts appear to be so indirect as to be irrelevant to the detailed assessment of review actions and could not be assessed in line with the principle of proportionate impact assessment.

The impact analysis below therefore focuses on the economic, security and human rights impacts, as outlined in Table 1, that any of the proposed review actions identified under option 2, 3 and 4 would have for the stakeholders concerned. The impact of the various actions is analysed individually and then as a package or "review option". A detailed presentation of impacts for each option and action is presented in Annex 7.

5.1 Impacts of Policy Option 1 – "Baseline".

This option would present the advantage of stability, maintaining a well-known system in place and stabilising administrative costs for EU and national administrations. It would however also perpetuate the administrative burden and costs for operators and the distortions associated with certain elements of that system, as evidenced during stakeholder consultations. Economic impact is thus likely to be negative in the medium to long-term, especially as data shows an increase in the number of licensed transactions, and, consequently, of associated costs. The majority of rrespondents to the public consultation thus consider that the review could significantly enhance the efficiency of export control administration and EU companies' competitiveness. Specifically, most respondents consider that the export control policy review would "likely facilitate dual-use exports by SMEs".

The social impact of the baseline scenario is likely to be negative on jobs and production in the long term, as the competitiveness of EU exporters is gradually eroded by the lack of adaptability of the export control system. From a security perspective, this option would fail to take into consideration the challenges posed by a rapidly changing security, economic and technology environment. Problems would not only persist, but would in some cases increase, e.g. as transit volumes continue to grow and new technologies continue to emerge, while being imperfectly addressed by the Regulation. This assessment is supported by 86% of respondents to the public consultation, who agree that the review would improve the export control system, in particular with regards to its capacity to address evolving security risks and to respond to rapid scientific and technological developments. Lastly, the impact on human rights would be negative as the export of cyber-surveillance technology is not clearly

addressed. As the internet of things becomes more widespread, the risks associated with trade in cyber-surveillance items will become even more significant.

5.2 Impacts of Policy Option 2 – "Implementation and Enforcement Support".

5.2.1 The Development of an EU export control network.

This would imply, firstly, a series of practical measures for enhanced information exchange between competent authorities, which are likely to require additional administrative resources and to increase the administrative burden in a first stage, both at national and EU level, as procedures and systems need to be put in place. However, information exchange could be developed gradually and in a way as to minimise transition costs e.g. by systematically weighing the costs and benefits of specific proposals for additional information exchange rather than proceeding across the board. It will eventually support the efficient administration of controls, as decisions can be made more quickly and more consistently throughout the EU, thereby reducing the administrative burden for operators and national administrations alike. It could also be beneficial for operators in terms of competitiveness and trade, by addressing the fragmentation of controls across the EU and reducing trade distortions between exporters from different Member States. Likewise, it would bring benefits in terms of security, by reducing the risk of "license shopping" by dubious exporters seeking the most accommodating licensing conditions. Surveyed licensing authorities consider that it could have a slightly negative impact on staff resources, but a substantial positive impact on security and human rights.

The development of *synergies between various security export controls* can be expected to optimise the use of resources and increase the consistency and effectiveness of the instruments over time. For instance the development of a common IT infrastructure is expected to reduce IT development costs at national level, as compared to the development of different systems - but would require the mobilisation of additional resources at EU level. It would also bring benefits in terms of security, as data of different origins could be more easily accessed and compared by authorities, where necessary.

Measures to support *enhanced cooperation with Member State enforcement agencies* are also likely to have some resources implications and increase the administrative burden in the short run, both at national and EU level. However, beyond the short term transition cost, they can be expected to support the efficient and effective administration of controls at national level e.g. by providing customs with all the information they need to detain or release a suspicious shipment. Such actions would also be beneficial to legitimate operators, e.g. as the number of detained shipments – and related delays - could be reduced. They can also be expected to bring benefits in terms of security as enforcement agencies will be better equipped to respond to illicit trafficking.

The *development of an EU capacity-building programme* is likely to bring administrative and financial costs for authorities[87], both at national and EU level, but can be expected to enhance their capacity to make sound decisions in a timely and consistent manner, thus reducing, in turn, licensing delays and compliance costs for exporters and enhancing security. Licensing authorities consider that it would have a slightly negative impact on resources, but a substantial positive impact on security and human rights. 89% of respondents to the public consultation consider that this would be beneficial, and stakeholders repeatedly noted that, while the EU has been funding capacity-building programmes in third countries, there is thus far no common training programme for EU officials.

5.2.2. The development of a partnership with the private sector.

This action is supported by a large share of stakeholders: the quasi-totality of respondents to the public consultation and to the targeted consultations ran by SIPRI and ECORYS agree that enhanced transparency in the form of information-sharing with industry would be beneficial, especially as it could improve legal predictability and reduce the administrative burden for business. For instance, the clarification of controls of technology transfers through the cloud could help companies compete globally by taking the full advantage of cloud services[88]. It could also significantly improve security, e.g. by raising awareness of operators about specific risks known to the authorities, thereby empowering them to implement controls more effectively, and by raising awareness of specific sensitive sectors e.g. the dual-use research community.

The development of *tools for operators* is likely to have positive economic impacts. For instance, the development of *common industry compliance standards* would provide a basis for a level playing field within the EU, and for possible convergence with key trade partners. Most respondents to the public consultation (78%) thus agree that standard ICP requirements for global licence holders could enhance the level-playing field while containing compliance costs and administrative burden. It could also enhance security, as companies would follow a more structured approach to the detection of possible illicit transactions. Similarly, 78% of respondents to the public consultation note that the introduction of electronic licensing in all Member States would increase the efficiency of licensing processes and reduce licensing delays for both authorities and companies. It would also facilitate trade convergence as most key trading partners have such systems in place. Once established, it could in turn facilitate the interconnection of national IT systems and support enhanced exchange of information between authorities, and bring benefits in terms of security. The development of tools for operators would however have costs for administrations, also at EU level. For example, the introduction of electronic licensing can be expected to increase costs notably in the short run as the IT software needs to be developed (preliminary estimates are that it could cost approximately EUR 2-3 million for the EU budget) and maintain, even if these could be optimised by drawing on the experience of the Member States that already operate such systems.

Lastly, a *'smart security' approach* would initially entail some limited administrative costs for administrations – at both Member States and EU levels - and industry players as they would contribute resources (technical experts) to the consultation mechanism. However, it would benefit Member States that would otherwise not have access to the same level of expertise. Crucially, it would enhance the EU's capacity to bring controls in line with technological and scientific developments, thus reducing inefficient or outdated controls that represent an undue burden for operators and a competitive disadvantage where such items are not controlled in third countries. It could also have a positive security impact, as the EU could more actively contribute to discussions on control list updates in multilateral export control regimes. The large majority of respondents to the public consultation (circa 70%) thus agree that a "smart security approach", in the form of voluntary and regular technical consultations on dual-use items, would be beneficial.

5.2.3 Export Control dialogue with key partners

More active dialogue with partners would bring some additional administrative cost for the EU (50% of an FTE) and its Member States as resources would have to be devoted to those dialogues, but this could be limited by focusing on a few key partners. On the other hand, it would address surveyed companies' assessment that different rules between the EU and its trade partners have a 'strong negative economic impact'[89], and bring significant economic benefits in terms of regulatory convergence – e.g. as more countries use the EU list as a benchmark. It would also bring benefits in

terms of security, as partners could be made aware of denied entities and act accordingly to avoid dangerous exports.

All in all, Option 2 is likely to have positive impacts in terms of promoting consistent and effective application of controls and reducing distortions within the Single Market, and to promote the global level playing field, as well as on security, especially as controls could adjust more rapidly to technological developments. However, impacts on administrative burden are mixed. At national level the additional administrative costs are expected to mostly transitional in nature. At EU level, the development of the EU network and private sector partnership are likely to require 2-3 FTEs, though the level of resources could be scaled back once tools have been deployed to about 1-2 FTE. Option 2 can however be expected to generate efficiency gains and to thus reduce administrative costs in the long term, both for operators and administrations.

5.3. Impacts of Policy Option 3 – "EU System Upgrade".

5.3.1 Option 3 would involve firstly a ***modernisation of existing control provisions***, which impact can be assessed as follows:

5.3.1.1 The ***clarification of key legal provisions*** would streamline the export process and save exporters time and money by reducing confusion over definitions and legal concepts and improving legal clarity and predictability. Such legal revisions would not only be beneficial in terms of simplification of the rules , but should also bring benefits in terms of security, as potential loopholes can be closed. For example, the Regulation's provisions could be revised to ensure that a competent authority is always identified, including in situations when no license will be granted. Most respondents to the public consultation agree that a clarification of legal provisions would increase the effectiveness of controls, the level playing field and improve legal clarity.

5.3.1.2 A clarification of controls of ***intangible technology transfer*** (ITT) would not affect the scope of controls and would bring no additional administrative costs for authorities or operators, but could bring significant benefits in terms of legal clarity and competitiveness, effectiveness and security.

5.3.1.3 The introduction of ***specific provisions tackling illicit trade*** would generate some indirect administrative costs at national level to the extent that additional (illicit) situations would be captured by legislation. On the other hand, it would increase the effectiveness of controls and be beneficial in terms of security. In addition, the revision of the jurisdiction clause, to cover EU persons outside of the EU, could adjust controls to the reality of global supply chains and would also address the risk of circumvention of controls through third countries.

5.3.1.4 Changes to ***brokering controls*** could generate somewhat higher administrative costs for authorities and for brokers as new aspects of brokering are taken into consideration, but costs would remain low in consideration of the limited scope of brokering (only 30 licences, for a value of EUR 7 million in 2013[90]). On the other hand, they could eliminate discrepancies between Member States and bring benefits in terms of legal clarity and uniform application in the Single Market. They would enhance security and human rights, especially as controls would apply to situations not covered by current provisions e.g. when the brokering services are performed by an EU person situated outside of the EU or when it concerns certain non-listed items or terrorism or violations of human rights.

5.3.1.5 Changes to ***transit controls*** would likely bring the same type of benefits as for brokering controls - e.g. in terms of legal clarity, uniform application throughout the EU and enhanced security – while additional costs for the involved authorities can also be expected to remain very low due to the

small number of transit operations concerned (only 48 authorisations, for a value of EUR 108 million in 2013[91]).

5.3.2 Surveyed companies consider that **optimisation of the licensing architecture** would have a 'strong positive economic impact'[92] for economic operators as a clearer and simpler set of implementing rules will reduce divergent application of controls. Respondents to the public consultation overwhelmingly agree that it could minimize distortions of competition (86%) and reduce export control management costs, in particular for SMEs. Apart from a limited short term transition cost, simpler and more uniform licensing processes could also decrease the administrative burden for licensing authorities over time: indeed, surveyed licensing authorities consider that it would have a positive impact on staff resources and processing times[93].

Specifically, the ***introduction of new EUGEAs*** would reduce administrative burden associated with individual licenses in favour of simplified control modalities that do not disrupt transactions. It would reduce costs for economic operators and for authorities alike, and would be beneficial in terms of global level playing field as European companies would not have to incur delays due to licensing. Based on expert consultations, it appears that processing an export under an EUGEA would cost 4 times less than under an individual license for private companies, and up to 11 times less for licensing authorities. Figure 5 shows the specific areas where stakeholders support the introduction of EUGEAs.

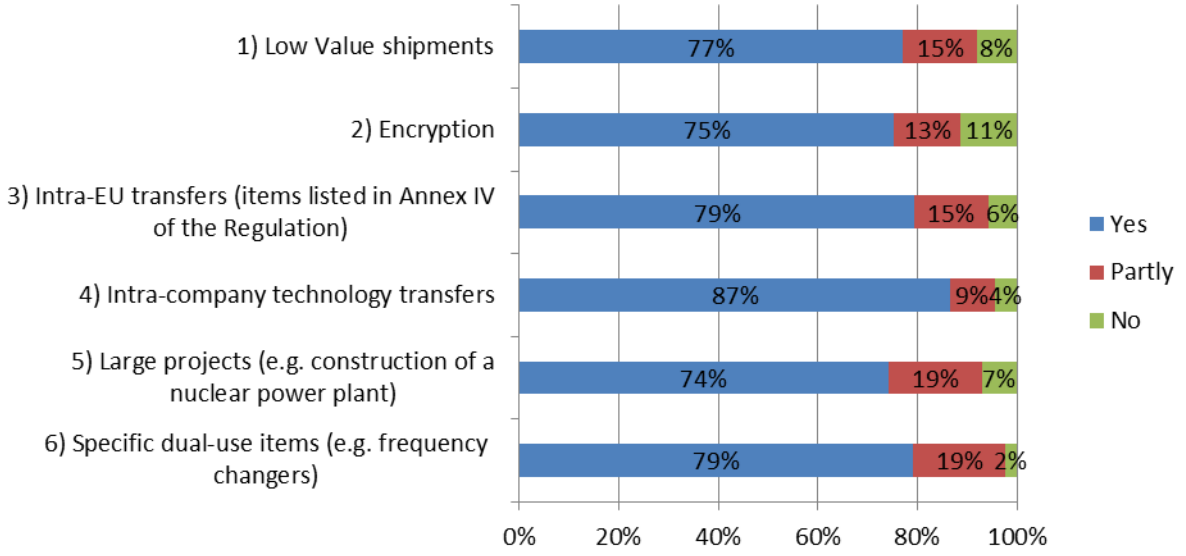


Figure 5: Responses to the question: "Would you support the introduction of any of the following EUGEAs?"

While there is no data available to quantify the potential impact of each and every action envisaged, it is possible to provide elements to estimate the impact of certain actions. Thus, from detailed discussions with industry, the following data could shed some light on the expected impact of an EUGEA on encryption: ESIA estimates that these represent approx. EUR 25 billion worldwide, and concern sectors as varied as banking, transport, mobile communication, smart infrastructure, pay TV etc. Surveyed licensing authorities however signal some concern that the introduction of EUGEAs could have a slightly negative impact expected on security and human rights[94]. This could be mitigated by ensuring that the conditions for use of EUGEAs enable robust monitoring of exports e.g. through company reporting or auditing.

75% of respondents also support the granting to the European Commission of a competence to modify, in consultation with experts from Member States, the parameters of EUGEAs, which would ensure that controls are updated and control modalities are proportionate to risks and thus enhance EU capacity to adjust to technological change. The implementation of this extended competence is expected to require about 50% of an FTE to manage depending on the number of modifications to EUGEAs that could be expected each year.

5.3.3 Convergence of catch-all controls. Surveyed companies consider that actions to increase the transparency and consistency of catch-all controls would have a 'strong positive economic impact'[95] as they can be expected to reduce distortions of competition caused by divergent decisions. This assessment is supported by available data, considering that approx.. 8000 licences were issued in 2013, for a value of approx. EUR 2.4 bn. Specifically, 74% of respondents to the public consultation agree that they could enhance legal clarity and predictability, reduce compliance costs and enhance the competitiveness of EU companies. Some additional administrative cost for EU and national authorities can however be expected from the development of an 'EU catch-all database', and surveyed licensing authorities fear a slightly negative impact on staff resources and processing times[96]. This impact should however be limited, especially as Member States have already started, since 2013, to exchange some information on catch-all licences. Importantly, surveyed licensing authorities anticipate a positive impact in terms of security and human rights, as greater consistency of controls would minimise risks of potential weak links in the EU control system.

5.3.4 Re-evaluation of intra-EU transfers. This action would reduce the remaining barriers to trade in dual-use items in the Single Market and thus reduce costs for operators. Although the impact cannot be predicted precisely, it could be noted that 696 licences for intra-EU transfers amounting to EUR 5.2 bn were issued in 2013; this trade could benefit from significant simplification thanks to the review. Depending on the detailed modalities, it can be estimated that the action would enable a reduction of the number of products subject to control on transfers within the EU by up to 40%. It would also improve the global level playing field, as EU operators would not be subject to comparatively more stringent controls than their competitors. Surveyed licensing authorities also anticipate a slightly positive impact on staff resources and processing times, while considering that the impact on security and human rights would be neutral[97]. The impact on security is indeed likely to be positive, as the list of most sensitive items could be updated taking account of technological developments, as underlined by 77% of respondents to the public consultation. In fact, the majority of respondents to the public consultation suggested that actions to review intra-EU transfer controls would at the same time enhance the effectiveness of controls and decrease compliance costs.

5.4. Impacts of Policy Option 4 – "EU system modernisation".

While some stakeholders – including the European Parliament and civil society organizations - have publicly called for the EU to bring exports of cyber-surveillance technology under control – others have expressed concern regarding the potential impact of a "human security approach" as envisaged under Option 4.

Specifically, there is concern that the **review of the general approach to 'dual-use'** envisaged under Option 4, which involves a broadening of the concept of 'dual-use items' beyond strict military and WMD applications, could result in an extension of the scope of regulations with potential associated costs e.g. in terms of additional licensing burden both for the affected industry and the relevant authorities. Indeed, categories of items that are normally not covered by the current concept (for example software that can be used for surveillance but has no military applications) could be subject to

controls under a revised definition. Similarly, the introduction of an explicit human rights criterion could potentially result in a negative impact on EU exports due to a greater volume of exports being subject to controls. However, controls in fact already incorporate considerations such as terrorism and human rights although they are not explicitly mentioned as criteria in the Regulation. For example the UK reports that in 2014, 18% of denied dual-use exports were related to human rights/internal repression grounds. Also, controls already apply to some items with no direct military or WMD applications – but recognised as 'sensitive' from a security perspective. In addition, the application of a human rights criterion is unlikely to have any significant impact for most dual-use items – e.g. integrated micro-circuits, pumps or valves, chemicals. Therefore, the real impact of an evolution of the dual-use concept in terms of administrative costs and on EU exports is likely to be marginal, as those actions would to a large extent clarify regulations and bring them in line with current practices.

Concretely, the option would essentially consist of the introduction of new controls on **exports of cyber-surveillance technologies**. Cyber-surveillance controls would, on the one hand, require highly-specialised expertise and would likely create some additional administrative costs (staff) both for economic operators – in particular in certain sectors of IT, telecommunications and electronics – and for administrations, both at national and EU level (1 FTE). On the other hand, new controls would likely have a positive impact on security and human rights: accumulated evidence regarding the misuse of European products in certain repressive regimes and/or conflict situations points to the need to control the export and end-use of such products and civil society organisations, in particular, consider that they are necessary to reduce the risks of human rights violations in repressive regimes and in conflict situations. However, industry has expressed concerns that cybersecurity controls, if not designed carefully, could have a negative impact on internet security, as academics and information security researchers use similar tools to investigate vulnerabilities in software and hardware in order to improve the security of technology (for example the use of penetration testing software is widely used by companies to secure their networks and counter intrusion software, exploits and vulnerabilities). There have also been concerns that controls may hinder access to encryption technology which is used to protect communications. Lastly, concerns have also been raised by law enforcement authorities who use these technologies and are concerned about the companies providing them moving abroad as a result of stronger controls in the EU.

In the face of such intricate economic and security considerations, impacts will largely depend on the selected control modalities and on the types – and number - of technologies brought under control.

- ***Control based on a list of technologies*** with clear technical descriptions would bring the benefit of legal clarity as operators – and authorities - know precisely which technologies need to be subject to controls. Importantly, a list could be agreed either at multilateral level (in the context of the Wassenaar regime) or at EU level. As evidenced by respondents to the public consultation, a multilaterally-agreed list would likely minimise risks that new distortions of competition are introduced, as operators from other countries would also apply the controls, and would have a positive impact in terms of level-playing field and competitiveness, as compared to other control modalities.

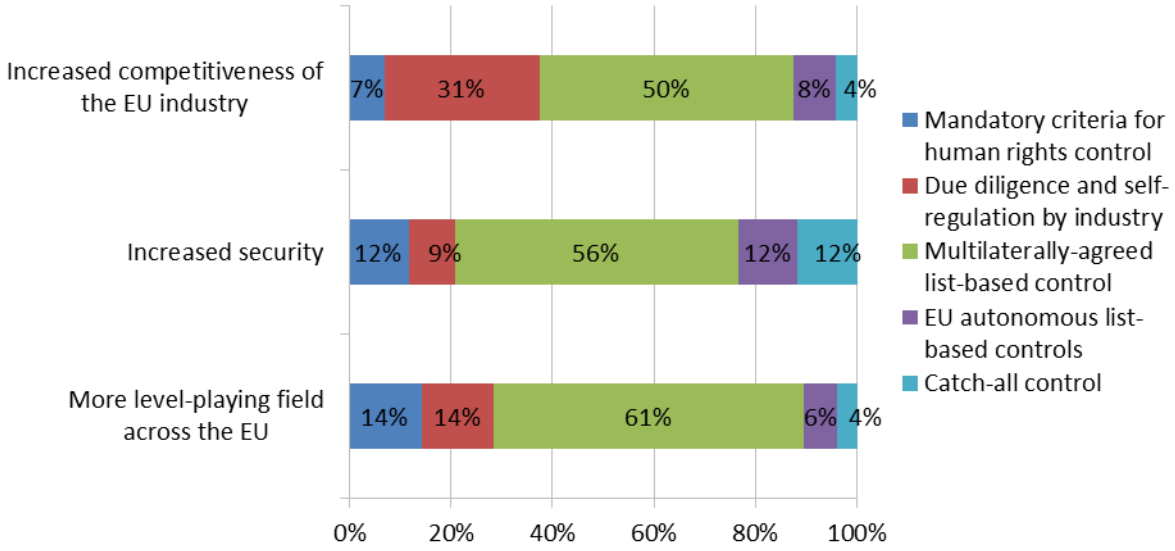


Figure 6: Would you agree that the actions to pursue the "human security approach" will likely have the following impact?

However, due to the rule of consensus applicable in export control regimes and the fact that they do not address human rights, there is a risk that controls cannot be easily agreed in this context. Moreover, neither all EU Member States nor the EU itself participate in the 'Wassenaar' export control regime.

By contrast, an EU autonomous list of cyber-surveillance technologies would present advantages in terms of flexibility and capacity to react swiftly to technological developments. But from an economic perspective, it would not be in line with the objective of convergence within global supply chains and could create distortions of competition, as non-EU operators would not be subject to similar controls, at least initially. Also, creating a basis for EU autonomous controls of specific dual-use items of concern, where important considerations regarding security or human rights warrant it, would depart from long-established practice whereby controls simply mirror decisions made by Member States in multilateral export control regime. It would add a new dimension to the EU export control regime. That conclusion however needs to be nuanced, since, under the Regulation, this possibility already exists at national level: thus, two Member States have introduced national controls on specific cyber-surveillance technologies. In a sense, therefore, the introduction of EU autonomous controls would merely extend that possibility at EU level, with clear benefits in terms of level-playing field in the Single Market. EU-wide controls would also be more effective, since exports denied in one Member State could not occur from another Member State, thereby enhancing the impact on security and human rights.

- A ***"catch-all" control for cyber-surveillance technologies*** would bring significant benefits in terms of security, as catch-all controls act as an "emergency brake" and competent authorities would have a legal basis to stop any export where there is evidence that it may be misused. On the other hand, stakeholders are concerned that a catch-all could cause legal uncertainty since there is no prior indication of the items that could be subject to controls. This likely negative impact for operators could however be mitigated by focusing the catch-all control on specific types of technologies – a sort of hybrid approach, whereby controls could apply to non-listed items but only in so far as they correspond to a certain type of specially designed surveillance

technology. The application of controls would thus depend on the combination of technical factors and of evidence regarding end-use, thereby narrowing the scope of such targeted catch-all control and, in turn, any potential negative economic impact, especially as the impact is likely to be confined to a limited number of small companies active in the EU cyber-surveillance sector.

- A ***due diligence obligation*** for companies would cast a wider net and place the onus on the private sector to ensure, through internal management processes, that exports of cyber-surveillance technologies are not destined to be misused in violation of human rights and do not pose a risk to international security. While big dual-use exporters appear to have in place robust compliance management systems that could accommodate such requirement, it could represent a significant additional cost for SMEs. At the same time, risks associated with SME exports cannot be ignored, and due diligence would ensure that all economic operators fully play their role as the 'first line of defence" for the detection of transactions of concern.

The different control modalities envisaged above appear to have broadly similar impacts on human rights or security, i.e. any measure would produce a broadly similar level of control of the end-use of cyber-surveillance technologies. The combination of measures, however, would have a higher positive impact – allowing for example to target systematically and precisely (based on a list with technical parameters) the most commonly used technologies while keeping catch-all controls as "emergency brakes" in case there is evidence that an export may result in human rights violations.

In conclusion regarding Option 4, the introduction of a "human security approach" enabling to effectively bring exports of surveillance technology under control would bring some additional costs for administrations, both at national and EU level (1 FTE), and economic operators, but these costs could be kept manageable if controls could be targeted at specially designed surveillance items, thereby excluding other items with broader applications e.g. for the management of telecommunications networks. At the same time, the introduction of new controls is necessary to achieve the objectives of the review in terms of both security and protection of human rights.

CHAPTER 6 – COMPARISON OF POLICY OPTIONS: HOW DO POLICY OPTIONS COMPARE?

In light of the findings of the impact assessment process, certain conclusions can be drawn as regards the economic and administrative impacts, and the social, security and human rights impacts under the various options.

6.1 Comparison of policy options.

Policy option 1

The baseline scenario, in which the existing framework would be maintained, would not address the identified problems and would enable the EU to achieve only to a very limited extent the specific objectives of the review. In the long-term, problems are likely to get worse and result in increasingly negative consequences e.g. the distortions of competition would grow due to the lack of adaptability of the EU system, while key partners continuously revise their own systems[98]. This assessment is supported by the vast majority of respondents to the public consultation, who agree that a review of current rules would improve the export control system.

Policy option 2

When compared to option 1, Policy option 2 has the advantage to address some of the problems identified without legislative changes but its effectiveness would be limited. Option 2 would usefully contribute to some specific objectives e.g. as regards the need to adjust to rapid technological and scientific developments, to reduce the distortions of competition and to support effective and consistent application of controls in the EU. Option 2 would however leave other problems unaddressed – such as the lack of legal clarity of some provisions of the Regulation or the lack of sufficient control of cyber-surveillance technology and only partially achieve objectives. For instance, the development of guidelines can support the effective and consistent implementation of legislation, but cannot fully remedy its imperfections. Crucially, in terms of efficiency, its impact on administrative burden and simplification of regulations is mixed. Some of the actions envisaged under Option 2 – such as the development of guidance, IT support tools, capacity-building - would require the mobilisation of significant human and financial resources. Option 2 can thus be expected to have significant administrative costs in the short term, even if it can also be expected to optimise the functioning of the system and bring long-term benefits for both administrations and operators.

Policy option 3

Policy option 3 contributes to most of the specific objectives, and is likely to achieve significant progress with regard to the general objectives. It offers maximum potential for a reduction of the administrative burden for exporters – and in particular SMEs - and authorities (over time) in the REFIT context, and could help reduce distortions of competition with operators from third countries. However, it would not address the problems associated with the emergence of new types of cyber-surveillance technologies and would not provide the EU with a mechanism to address risks that such technologies may be misused in violation of human rights or that they may pose to international security. In the long term, this problem would be allowed to grow if nothing is done to control the burgeoning trade in cyber-surveillance technologies. Finally, it would also have certain resource implications for the EU as noted above.

Policy option 4

Policy option 4 addresses a specific objective, and is likely to achieve significant progress with regard to that objective. In terms of economic and trade impact, option 4 could result in a higher administrative burden for operators and authorities, both at national and EU level, since a new layer of control would be added, see above. Depending on the specific formulation of control provisions, it also involves a risk that new distortions of competition be introduced at global level, as it cannot be assured that other key technology suppliers (e.g. China or the US) would also introduce similar controls. However, to the extent that option 4 would focus on very specific technologies, negative economic impact would be limited to a specialised industry and would only affect a small trade volume so that the overall negative economic impact of this initiative would be equally limited. By contrast, option 4 would have a significant positive impact on security and human rights: it appears as an indispensable condition to prevent human rights violations resulting from the export of EU items in third countries and to address security risks, to the EU and its citizens, associated with new cyber-surveillance technologies.

6.2 Preferred option.

In summary, option 3 "EU system upgrade" appears as the most efficient and effective option to address problems identified and when comparing the advantages and disadvantages in light of economic and social (security and human rights) impact criteria, and in relation to the set objectives.

However, considering that Option 4 "EU system modernisation" is indispensable to address the problem associated with the lack of control of cyber-surveillance technology, it should also be retained. Therefore, the combination of Option 3 and 4 is recommended as the 'preferred option'.

In spite of its positive long term impact on administrative burden, Policy Option 2 would be relatively costly to implement in the short to medium term and could only be achieved with appropriate resources both at national and EU level and can therefore not be retained fully. However, considering the importance of administrative burden reduction in the REFIT context, a gradual implementation of some of those actions identified under Option 2 could be envisaged (e.g. development of e-licensing, technical consultations with industry) on the basis of a clear prioritisation of tasks and provided the necessary additional resources can be allocated, including joint commitments by relevant stakeholders such as Member States and industry.

Assessment criteria	Option 1	Option 2	Option 3	Option 4
Reduction of distortions of competition within the Single Market	-	+	++	+
Promotion of a global level-playing field	-	+	++	-
Reduction of administrative burden (operators)	0	+	++	-
Reduction of administrative burden (authorities)	0	-	0 (transition costs) / + (medium term)	-
Legal clarity	0	+	++	+
Prevention of WMD proliferation	0	+	++	0
Prevention of the proliferation of sensitive technology	0	+	++	++
Prevention of terrorism	0	0	+	0
Prevention of human rights abuses	0	0	0	++

Annex VII presents a detailed analysis of impacts by review option and action.

CHAPTER 7 - MONITORING AND EVALUATION: HOW WOULD ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The effectiveness of the changes introduced to the export control system by this initiative should be subject to monitoring and evaluation. In light of the policy objectives set out in section 3, the

following arrangements are proposed in order to set up an appropriate monitoring and evaluation framework.

7.1 Monitoring

Monitoring of implementation will be carried out in cooperation with Member States in order to ensure that competent authorities and exporters implement effectively and consistently the requirements of the proposed regulation.

While the fundamental limitations to data collection are likely to remain in the short term, implementation of some of the proposed actions will help addressing some of the data gaps currently hindering the analysis of impact. For example, while, in compliance with the principle of subsidiarity, relevant licensing information will continue to be gathered primarily by Member States, harmonised reporting conditions under general authorisations will provide more comparable and precise data and a more robust basis for capturing the volumes and values of dual-use trade. Regular dialogue and partnership with industry should also improve the information basis for monitoring, by providing anecdotic and evidence and concrete case studies regarding the application of controls. Moreover, further efforts will be made to continuously refine the statistical analysis of trade flows, and to improve the collection of open source export control information. Lastly, sources of data should also be expanded as a result of actions to enhance information exchange and enforcement cooperation.

The practice of periodic (annual) reporting[99] will allow for appropriate monitoring and evaluation of the implementation of the initiative and to inform the European Parliament and the Council regularly.

The table below gives an overview of the objectives tackled and a set of indicators to monitor the effectiveness of the proposed changes. They may be supplemented by other indicators found suitable for monitoring the changes introduced.

Objectives	**Indicator and unit of measurement**	**Source of data**	**Frequency of measurement**
Adjust to evolving security risks and threats	- Data on implementation and enforcement e.g. number, value and type of denials, reports of violations/seizures, questions on interpretation etc.	Member States and third countries, research institutions and Experts' reports.	- ongoing; - yearly (licence data).
Adjust to rapid technological and scientific developments	- Number and frequency of the adoption of specific EU control approaches dealing with new technologies, incl. publication of guidelines, reports of technical expert groups etc; -.Frequency of updates to the EU control lists and time gap with decisions	Reports of discussions with Member States and industry.	- ad hoc (publication of guidance notes or technical reports) - yearly (updates to EU control lists).

	adopted in export control regimes; - Existence and activity of Technical expert groups		
Control the export of cyber-surveillance technology	- Data on implementation of controls (e.g. number, value and types of licences, denials etc) - reports /complaints of human rights violations.	Reports from Member States, industry and civil society.	- ongoing; - yearly (licence data).
Reduce distortions of competition and administrative burden	- Data on implementation and enforcement, e.g. number of users of general authorisations, ratio individual/general licences,, more even processing times number of operators with ICPs, volume and value of trade subject to intra-EU transfers,... - Economic situation of dual-use exporters.	Member State reports. Stakeholder surveys Trade statistics (e.g. evolution of trade flows).	- yearly (annual report, incl. trade data) - ad hoc surveys of stakeholders.
Promote the global level playing field	- Number and frequency of multilaterally and bilaterally agreed control rules; - Number and frequency of EU coordinated proposals in the regimes; - Number and frequency of bilateral decisions on convergence of controls.	Reports from multilateral export control regimes. Reports of dialogue with trade partners Industry feed-back.	- ongoing.
Ensure effective and consistent application of controls in the EU	- Introduction of support tools, e.g. e-licensing systems, adoption of guidance… - Number and frequency of reports on the ineffective/inconsistent application of controls - Organisation of outreach events and number of relevant stakeholders	Member States reports Reports from relevant events, incl. DG TRADE dual-use webpage Reports / position papers by industry.	- ongoing. - yearly (annual reports)

	attending outreach events - Organisation of dedicated operations / actions e.g. training, joint exercises with Customs etc - Availability of more implementation and enforcement data.		

Table 3: Monitoring - objectives and indicators

7.2 Evaluation

The Commission should undertake an intermediate evaluation of its new initiative five years after its entry into force in order to assess the actual economic, social, and environmental impacts and evaluate its efficiency and effectiveness and the extent to which its results are consistent with the objectives. The evaluation results will be used for decision-making needs on the future of the policy, and for amendments to the regulatory framework, if appropriate. The Commission will communicate the evaluation results to the European Parliament and the Council.

List of acronyms

AEO	Authorised Economic Operator
ASD	AeroSpace and Defense Industries Association
BAFA	German licensing authority
CAUSE	Coalition Against Unlawful Surveillance Exports
CECIMO	European Association of the Machine Tool Industries
CEFIC	European Chemical Industry Council
DUeS	Dual-Use Electronic System
DUCG	Dual-Use Coordination Group
ESIA	European Semi-conductors Association
EUGEA	European General Export Authorisation
FTE	Full Time Expert
ICP	Industry Compliance Programme
ICT	Information and communication Technology
ISIS	Islamic State
IT/ICT	Information (and Communcation) Technology
ITT	Intangible Technology Transfers
NGEA	National General Export Authorisation
OPCW	Organisation for the Prohibition of Chemical Weapons
R&D	Research and Development
UNSCR	United Nations Security Council Resolution
WMD	Weapons of Mass Destruction

ANNEX 1: PROCEDURAL INFORMATION

The Impact Assessment was led DG TRADE, unit F1.

The Impact Assessment process was launched in the second semester of 2014. The Impact Assessment roadmap is available on the DG Trade Dual Use webpage at the following address:

http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2015_trade_027_duxc_en.pdf

Five Impact Assessment Steering Group (IASG) have been called in the course of the Impact Assessment. The following DGs and services were invited to the IASG: Energy (ENER), Taxation and Customs Union (TAXUD), Joint Research Centre (JRC), Internal Market, Industry, Entrepreneurship and SMEs (GROW), Health and Food Safety (SANTE), Migration and Home Affairs (HOME), Research and Innovation (RTD), Communications Networks, Content and Technology (CNECT), International Cooperation and Development (DEVCO), Competition (COMP), Informatics (DIGIT), Employment, Social Affairs and Inclusion (EMPL), Eurostat (ESTAT), Legal Service and Secretariat-General (SG), as well as the European External Action Service (EEAS).

The Impact Assessment included a data collection project, commissioned to external consultants. The result of the data collection project, targeted at outlining the economic and trade profile of the EU dual-use industry, is attached in Annex V. The information included in the report relies on the sources and the methodologies outlined in Annex IV.

The dual-use sector, for its intrinsic characteristics, remains difficult to "quantify" with precision: however, the results presented in the Impact Assessment report and summarised in Annex V do represent, at this point in time, the most far-reaching and methodologically robust endeavour in this direction.

The Regulatory Scrutiny Board expressed its positive opinion regarding the Impact Assessment Report. A number of comments were transmitted to DG TRADE. The table below illustrates how such comments were taken into account in the current version of the report.

	RSB comment	**Revisions to the IA report**
1	**Clarify the policy context of the export control regime and describe the link with international EU obligations in the area.**	- Revised introduction - Clarification regarding other security trade instruments in Section 1.1.1. - Clarification regarding which elements of the control regime are defined at international, EU, and national level in the revised introduction - Analysis of the effectiveness and the efficiency of the existing EU export control in Section 1.1, and comment regarding the low number of denials in Section 1.5.2. - Clarification of the margin for EU action, given already existing international arrangements in Section 1 and 1.1.3 (for cyber-surveillance technology).
2	**Improve the problem definition, including by enhancing the focus on**	- Revised sections 1.1

	issues specific for the export control of dual-use items. **Demonstrate the magnitude of the problem, underpinning it with available evidence.**	- Revised Problem Tree - Revised section 1.5.2 on the magnitude of the problem, incl. comment on denials as an indicator of the trade dimension, and reference to specific licensing data. - New section 1.1.7 to distinguish issues linked to the design of the regulation from those linked to the implementation of the regulation, and revisions to 1.2.4. - additional and revised element son trafficking in Section 1.2.1.1 - diverging situations in Member States and the EU internal market elaborated in Section 1.2.4
3	**Improve the intervention logic and the linkages between different parts of the report (problem – objective – options).**	- Revised section 3.2 and new Annex VI – Table linking problems, objectives and actions - distinction between the complementary and alternative elements in the composition of the policy options – see revised Section 4.1 - The pros and cons of option 2 (and therefore of the integration of elements in the preferred option) are clarified in Section 6.1
4.	**Deepen the analysis of impacts, quantifying them wherever possible.** **In particular, strengthen the REFIT conclusions – i.e. in relation to the cost-efficiency, simplification/burden reduction potential and SME impacts of the initiative.**	New Annex VII –Detailed presentation of impacts by review option and action. - Impacts have been quantified where possible, including data on some specific controls (see additional data under 5.3.3, 5.3.4). - See revised section 1.1.5 on administrative burden, and revised sections 6.1 and 6.2 on the selection of policy options, as well as additional references to REFIT in 3.3 (consistency with other policies), some additions to 5.3. - Additional explanations regarding the data quantification limitations are included in Section 1.5.
5.	**Better plan monitoring and evaluation**	- evaluation indicators are aligned with policy objectives in Section 7.1. - Revised Section 7.1 includes additional explanation of actions to address data gaps.
6.	**Procedure and presentation**	The presentation of the report has been revised in an effort to make it more legible and additional information placed in annexes where possible.

ANNEX 2: STAKEHOLDER CONSULTATION

Introduction

The European Commission has actively engaged with stakeholders and conducted wide-ranging stakeholder consultations to support the EU Export Control Policy Review. The Consultation strategy included online public consultation, dedicated export control conferences and seminars, and regular outreach to key stakeholders. Moreover, a data collection project which included *i.a.* targeted surveys of key stakeholders was commissioned to feed into the impact assessment.

This report summarizes the consultation activities carried out and their main results.

1. The preliminary phase: the Green Paper consultation (2011-2013)

Art. 25 of the Regulation calls on the Commission to review the implementation of the Regulation 428/2009. In order to initiate such review, a Green Paper (COM(2011) 393 final) was published on 30.6.2011, inviting stakeholders to express their views about the EU export-control regime and the potential need for its review. Exporters, business associations and authorities from the Member States, as well as research institutes and other civil society organizations took part in the consultation. The Commission reported on the outcome of this process in the Staff Working Document "Strategic export controls: ensuring security and competitiveness in a changing world – A report on the public consultation launched under the Green Paper COM(2011) 393" (SWD(2013) 7 final, 17.1.2013). This was complemented by the presentation of a Report from the Commission to the Council and the European Parliament on the implementation of Regulation (EC) No 428/2009 (COM(2013) 710 final, 16.10.2013).

The Staff Working Document and the report to the European Parliament and Council emphasise that stakeholders call for various improvements and updates to the EU export control system in order to adapt it to rapidly changing technological, economic and political circumstances and opened the way to the review of export control policy. Stakeholders views were thus taken into account in the preparation of the Commission Communication 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, 24.4.2014) in which the Commission outlined a number of key initiatives to modernize the system.

2. Export control conferences and seminars – regular dialogue with stakeholders.

As the export control policy review proceeded, the European Commission organized, jointly with the rotating presidencies of the European Union, regular conferences in order to develop a dialogue with key stakeholders from dual use industry, civil society and Member States, and collect their views on the review:

- On 26 June 2013, the first "Strategic Export Control Conference" gathered more than 300 representatives from industry associations, companies, civil society, academia as well as member States authorities, who identified possible areas to upgrade the existing rules and formulated options for a more risk-based, targeted and effective EU system;[100]
- The Export Control Industry Forums of 24 October 2014[101] and 7 December 2015[102] , gathering Member States authorities, as well as c. 150 stakeholders, stakeholders, including representatives

to discussion different aspects of the review options identified in the Commission Communication. Detailed reports of the Forums are available on DG TRADE Dual Use webpage.

3. Targeted outreach to key stakeholders

Besides the formal periodic events organized in Brussels, the Commission services have conducted targeted outreach to key stakeholders including key business associations and civil society organizations, essentially responding to invitations to participate in industry or civil society events. Meetings were thus held with key industry associations such as the Aerospace and Defense Industry Association, the European Semiconductor Industry Association, Digital Europe etc. and civil society organizations such as the "CAUSE coalition" to discuss specific review issues in more detail and Commission services participated in some key export control events such as the "World ECR conference" or the Berlin export control seminar in October 2015.

A number of industry associations and some civil society organizations have formally adopted "position papers" with respect to the review options identified in the 2014 Communication. 13 substantive contributions were received from companies and industry associations representing stakeholders in the fields of ICT, semiconductors, nuclear energy as well as aeronautics, space and defense. More homogenous implementation of controls in the EU, the introduction of new EUGEAs as well as timely updating of the EU Control List to ensure adaptation to technological advances were among the most quoted demands by the industry. Two papers were submitted by civil society organizations, concerning the relationship between EU export of surveillance technology and violations of human rights in third countries.[103] Position papers submitted in the context of the public consultation are available at http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_154004.pdf.

4. Data collection and analysis project

In order to support the Impact Assessment, the Commission contracted an external consultant to collect relevant data about the EU dual-use industry and, to the extent possible, about the likely impacts of review options. In addition to wide-ranging desk research, the consultants have run online questionnaires for business associations, companies and licencing authorities of Member States, as well as interviews with key stakeholders among EU industry associations, academics and research institutes, NGOs, and Member States authorities. C. 250 companies, 50 industry associations as well as 14 Member States licensing authorities took part to the data collection project. The final report is available at http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190.

5. Online open public consultation on the EU Export Control Policy Review

On 15 July 2015, the European Commission launched an open online public consultation with a view to collecting stakeholders' input on the EU Export Control Policy Review ("the Review"). Stakeholders were invited to respond to 38 questions covering the range of themes and options outlined in the Communication (2014)244, including the modernization of controls, the optimization of licensing architecture, harmonization of controls at EU and global level, controls of technology transfers and the development of a "human security" approach taking into consideration the links between security and human rights.

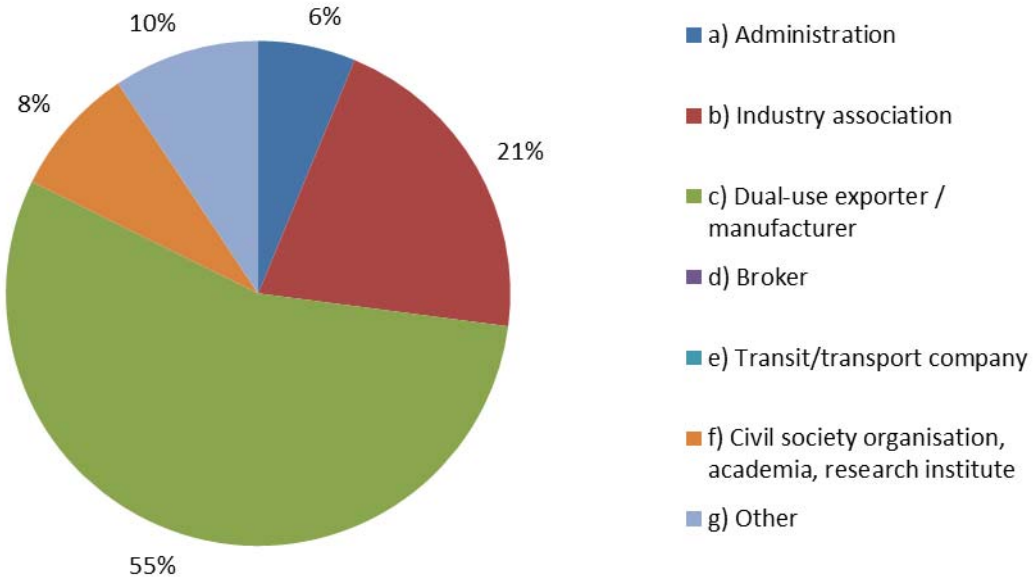
The Commission received 97 responses to the online public consultation, coming mainly from industry associations and civil society. Stakeholders' responses have been published online according to the Commission applicable rules.[104] They can be found together with a list of contributors via: http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190

The results of the online public consultation will be complemented with the stakeholders views collected in the other consultation activities.

5.1 Overview of respondents

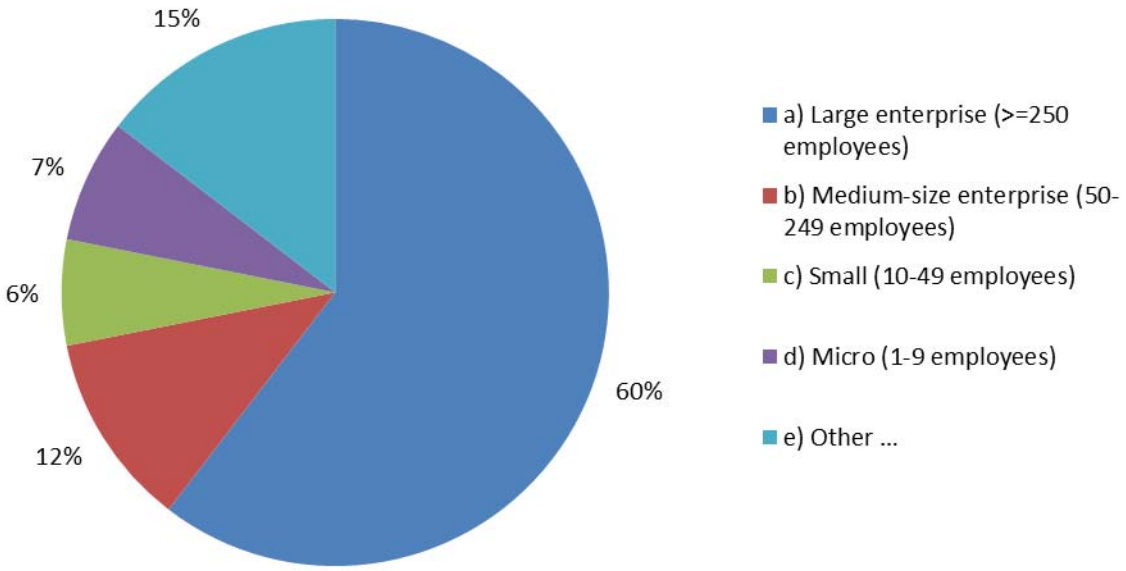
97 responses were received.[105] They were submitted mainly by dual-use exporters and manufacturers (55%). Industry associations (21%), civil society representatives (8%) and Member States Authorities (6%) also took part in the consultation.[106]

Figure 1: Breakdown of respondents by category



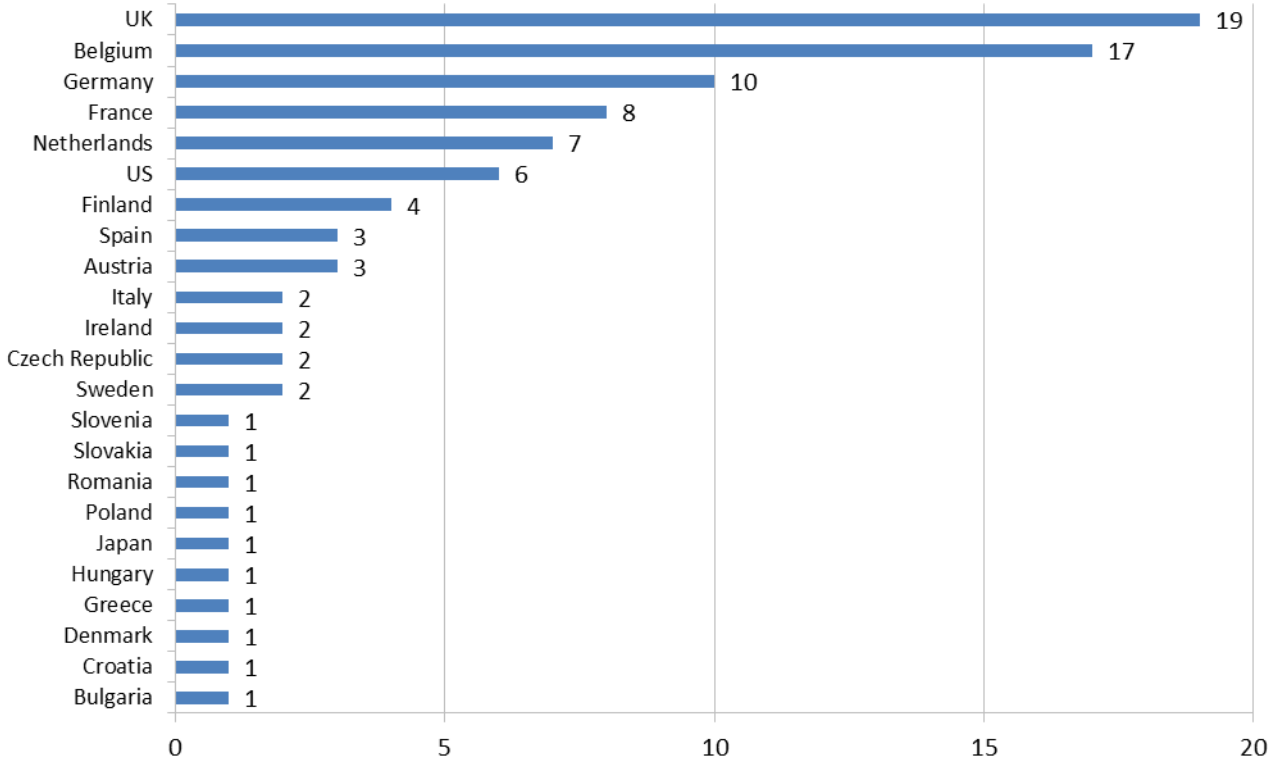
The key dual use industries took part in the consultation, with a strong representation from the industrial goods sector (including machinery and equipment) and the computer/electronics sectors (27% and 15% respectively). Other reported sectors included energy including nuclear (9%), space/aeronautics (8%), telecommunications (7%) and chemicals (2%). Most of the respondent companies were large organizations[107] (i.e. enterprises with at least 250 employees, 60%), but about one quarter of the respondents were SMEs (24%)[108].

Figure 2: Breakdown of respondents by size[109]



Finally, in terms of geographical distribution, most industry associations which replied to the questionnaire are based in Belgium, but are expected to represent operators from all over Europe. Three EU Member States – UK (20%), Belgium (17%) and Germany (12%) – accounted for almost half of total respondents. 7% of replies came from stakeholders established outside of the EU, namely the United States of America and Japan.

Figure 3: Breakdown of respondents by country



5.2 Summary of the respondents' contribution by issue

5.2.1 Baseline scenario, objectives and review options.

The large majority of respondents (86%) agreed that a review of current EU export control rules would improve the export control system, in particular with regards to its capacity to address evolving security risks such as WMD proliferation and terrorism (according to 62% of respondents) and to respond to rapid scientific and technological developments (58%). According to the majority of respondents, the Review would also significantly enhance the efficiency of export control administration (55%) and enhance EU companies' competitiveness (49%). On the other end, most participants did not foresee significant environmental or social impacts (including on the job market) stemming from the Review (respectively 71% and 80% of respondents). 34% of respondents suggested that the Review could support the prevention of human rights violation in third countries; on the contrary, 25% disagreed with this statement.

5.2.2 Impact of review options

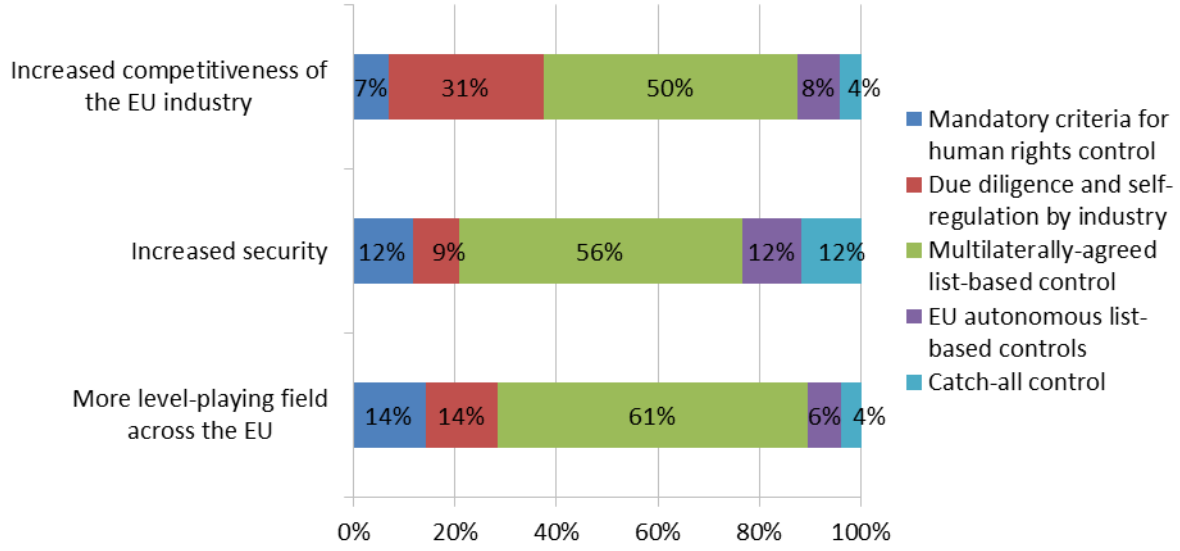
5.2.2.1 Human security approach

Respondents expressed diverging views on the introduction of provisions based on the concept of human security in the EU export control regulation.[110] A significant share of respondents (c. 40%) did not believe that the adoption of a human security approach would improve EU security and decrease the risk that EU exports of cyber-surveillance technology could be misused in human rights violations. In particular, 40% of respondents did not deem the inclusion of a human rights control criterion as an effective instrument to reduce the misuse of dual-use items to commit human rights violations. 45% of respondents suggested that reviewing the definition of dual use items would not reduce this risk either.

On the other hand, 31% and 30% of respondents, respectively - most of which were representatives of civil society - supported the opposite views.

Figure 4 shows the views of respondents on the effectiveness of different possible applications of the human security approach in the areas of competitiveness, security and the level playing field. While civil society representatives preferred mandatory criteria for human rights control as the most effective action, the overall set of respondents supported a broader set actions, in particular the introduction of multilaterally agreed list-based controls.

Figure 4: Would you agree that the actions to pursue the "human security approach" will likely have the following impact?



5.2.2.2 "Smart security" mechanism and modernisation of trade controls

The majority of respondents agreed that a "smart security approach", in the form of voluntary technical consultations on dual-use items (c. 70%), yearly updates of the EU control list (66%), regular consultations with industry and development of guidelines (92%) and coordination of the EU position in multilateral export control regimes (69%), would be beneficial for the EU export control policy.

Furthermore, a significant share of respondents agreed that clarifying the definition of exporter, the criteria for determination of the competent authority, the jurisdiction clause to control transactions between third countries involving EU persons, and the scope of brokering, technical assistance and transit controls in the EU would increase the effectiveness of controls (58%), the level playing-field (60%) and improve legal clarity (75%).

The analysis of responses did not highlight any significant divergence of views among different categories of participants.

5.2.2.3 Strategy for "immaterial control"

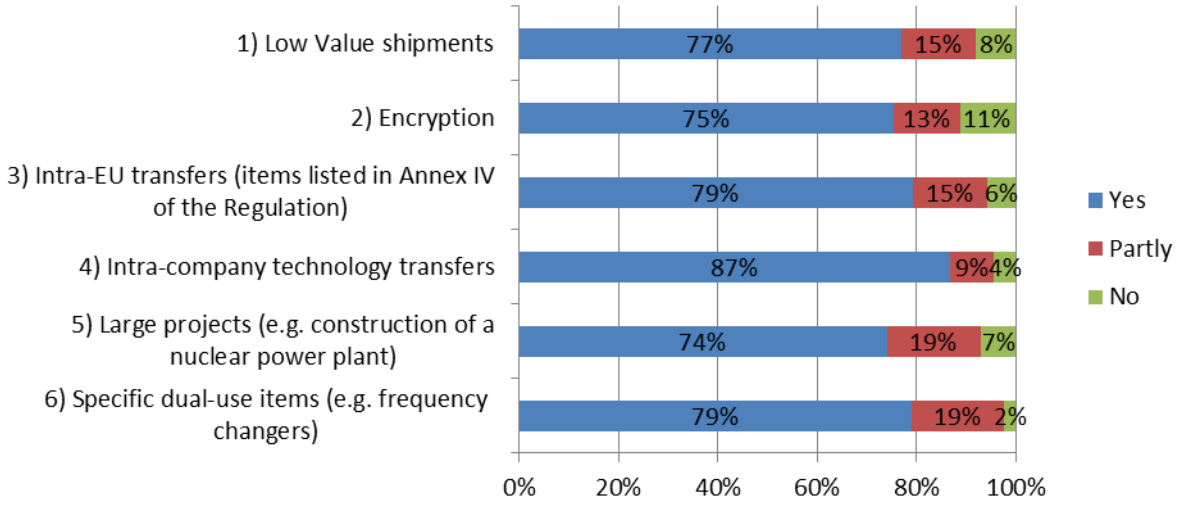
With regard to the strategy for immaterial control outlined in the Communication (2014)244,[111] 85% of respondents supported the introduction of an EU General Export Authorization (EUGEA) or global license for intra-company technology transfers. While industry associations and companies supported the introduction of new types of EUGEAs, civil society expressed concerns over possible misuses of such authorizations. 76% of respondents also supported outreach to industry and academia in the form

of public guidance for technology transfers and dual-use research aimed at enhancing the enforcement of controls while preserving academic freedom.

5.2.2.4 Optimisation of the licensing architecture

Respondents agreed on the utility of further harmonization in EU export authorizations to minimize distortions of competition (86%) and reduce export control management costs, in particular for SMEs (66%). They also supported the shift from "paper-based" ex-ante controls on transactions to pre- and post- transactions controls on companies to enhance controls' effectiveness (66%). In particular, with regard to the specific export control options, 75% of respondents agreed that granting the European Commission the competence to modify, in consultation with experts from Member States, the list of EUGEAs and their content could help ensure an efficient and effective use of EUGEAs. Figure 5 shows the specific areas where respondents supported the introduction of EUGEAs.

Figure 5: Would you support the introduction of any of the following EUGEAs?



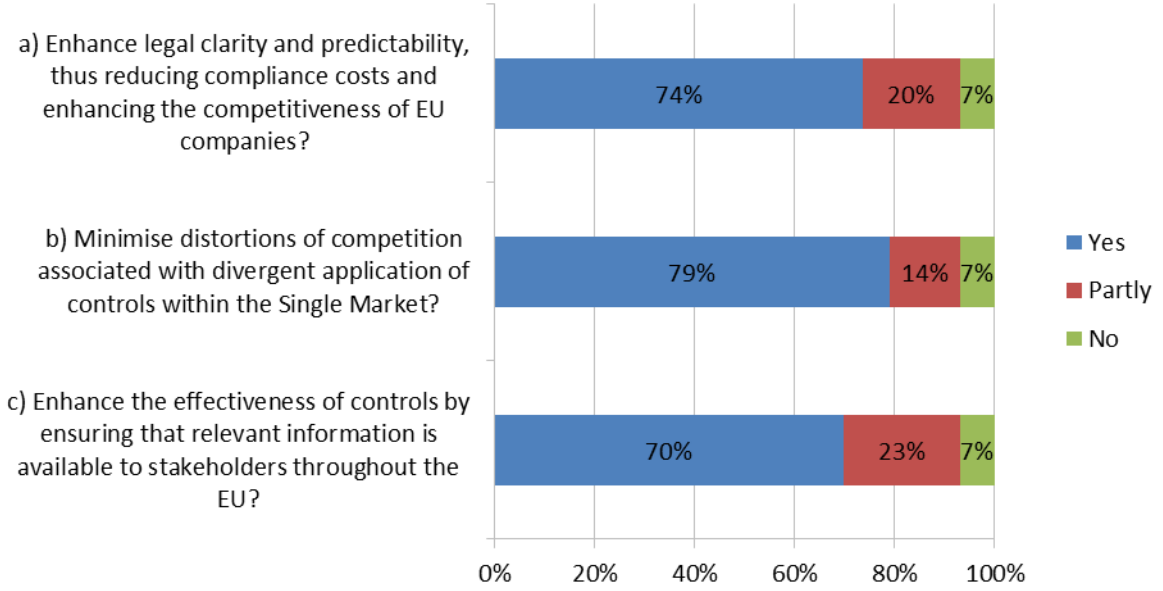
A significant share of respondents (74%) also suggested that a regular review of existing national general export authorization (NGEAs) should be carried out with a view to transforming them into EU general export authorizations (EUGEAs).

The analysis of responses did not highlight any significant divergence of views among different categories of participants.

5.2.2.5 Convergence of "catch-all controls"

A large majority of respondents expressed interest in further developing the concept of catch all in the Export Control Policy Review.[112] Figure 6 highlights the benefits that, according to respondents, could be produced by a greater convergence of catch-all controls in the EU.

Figure 6: Would you agree that actions to promote a greater convergence of catch-all controls could:



In order to achieve the above-mentioned targets, respondents suggested to harmonize the definition and scope of catch-all controls (e.g. regarding destinations, end-users and items covered by the catch-all control) (86%); to introduce a mandatory consultation process between licensing authorities to support uniform EU-wide application of catch-all controls (61%); and to enhance transparency with exporters – including the possibility of publication of catch all requirements (75%).

The analysis of responses did not highlight any significant divergence of views among different categories of participants.

5.2.2.6 Critical re-evaluation of intra-EU transfer controls

With regards to intra-EU controls, 77% of respondents agreed that updating the list of items in Annex IV to the export control regulation could help bringing controls in line with technological developments and commercial availability. Furthermore, c. 60% of respondents suggested that the actions to review intra-EU transfer controls, including the review of the list of most sensitive items in Annex IV and/or the introduction of new EUGEAs associated with new possibilities for controls (e.g. post-shipment verification), would at the same time enhance the effectiveness of controls and decrease compliance costs.

The analysis of responses did not highlight any significant divergence of views among different categories of participants.

5.2.2.7 Development of an EU export control network

Another area where respondents' views were relatively homogeneous is the one regarding the development of an EU export control network. 78% of respondents agreed that the development of a common IT infrastructure (including e.g. the introduction of electronic licensing for all competent authorities) could usefully contribute to consistent and efficient implementation of controls within the EU. An even larger share (89%) suggested that the introduction of EU-wide capacity-building and training for officials from licensing and other relevant administrations, and outreach to industry and academia would be very beneficial for the enforcement of EU export controls. Reducing the fragmentation of controls across the EU and reducing the risks of "license shopping" were quoted as the most valuable objectives achievable through the implementation of an EU export control network.

The analysis of responses did not highlight any significant divergence of views among different categories of participants.

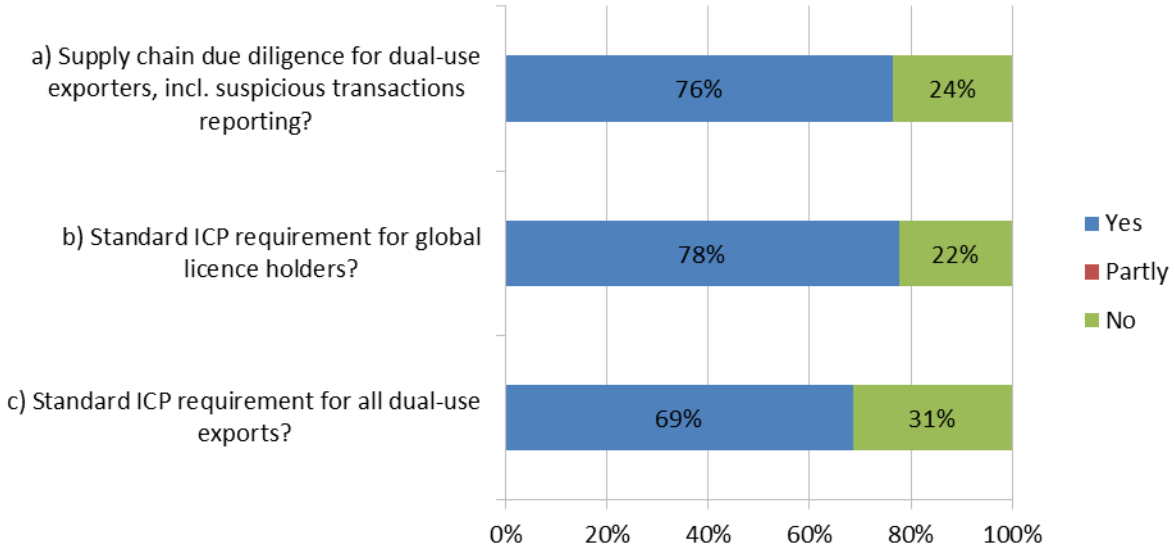
5.2.2.8 Private sector partnership

A very large share of respondents suggested that developing a private sector partnership, as outlined in the Communication, would be helpful in promoting the level-playing field within the Single Market (73%), promoting the global convergence of controls (75%) and enhancing the effectiveness of controls (77%).

In particular, Figure 7 outlines respondents' views on the effectiveness of possible options for introducing industry compliance standards.

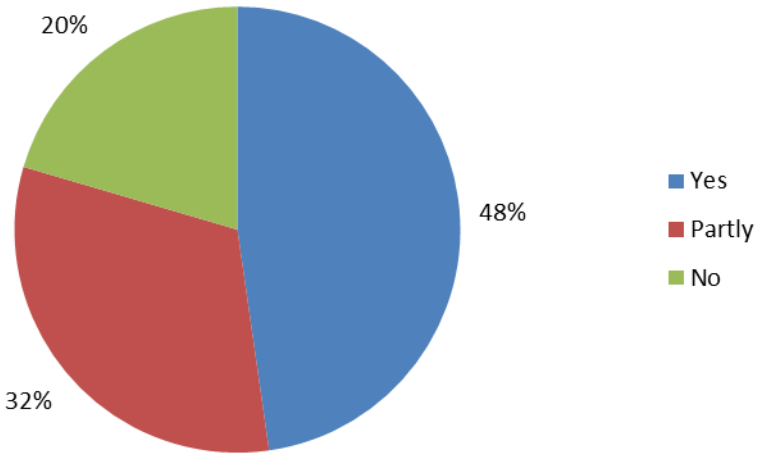
The analysis of responses did not highlight any significant divergence of views among different categories of participants.

Figure 7: Would you consider that the following options for introducing industry compliance standards, would enhance the level-playing field while containing compliance costs and administrative burden:



70% of respondents also indicated that guidelines and structured outreach activities to the private sector would improve the effectiveness of the EU export control system. With regard, to SMEs, Figure 8 summarizes respondents' views: c. 50% of respondents supported the introduction of standard compliance requirements in order to reduce the costs of compliance, thus increasing SMEs' capacity to export dual use items.

Figure 8: Would you agree that the development of a "private sector partnership", through standard compliance requirements containing compliance costs, could support SMEs' capacity to export dual-use items?



5.2.2.9 Global convergence

Views of respondents were less homogeneous on the possible introduction of "end-use monitoring" (i.e. verification of the end-use directly at the premises of the end-user in a third country). While 44% of respondents supported the idea, 40% did not show confidence in its effectiveness. On the other hand, 66% of respondents agreed that EU participation in all multilateral export control regimes would appropriately reflect the EU's role as a key security and trade actor, and would allow the EU to better promote its interests and represent its export control system. Similarly, 79% of respondents supported EU outreach efforts towards third countries so as to disseminate EU best practices and improve the level-playing field.

The analysis of responses did not highlight any significant divergence of views among different categories of participants.

ANNEX 3. WHO IS AFFECTED BY THE INITIATIVE AND HOW

	Policy Option 3: EU system upgrade				Policy Option 4: EU system modernization	
Action / Stakeholder	**Modernization of existing control provisions**	**Optimization of EU licensing architecture**	**Convergence of catch-all controls**	**Re-evaluation of intra-EU transfers**	**Review of the general approach to Dual Use**	**Controls on cyber-surveillance technology**
Citizens	More legal clarity would lead to better compliance and higher security.	Streamlining licensing procedures would allow competent authorities to devote more time to suspicious transactions and decrease the incentive for illicit exports. Security would be improved.	A more uniform application of catch-all controls would increase compliance and reduce illicit exports. Security would be improved.	The further operationalization of the EU Single Market for dual-use would allow licensing authorities to focus on dual use exports towards third countries, where the risk for security and violation of fundamental rights is higher.	Further operationalizatio n of existing controls based on human rights concerns, as well as a broader definition of dual-use items, would increase security and respect of human rights in third countries by preventing the export and misuse of dual use items.	Human rights abuses linked to the misuse of cyber-surveillance technology would be more difficult. With regards to the specific new technologies subject to controls, global security would be improved. On the other hand, the introduction of new controls may favor the relocation of producing companies outside of the EU and reduce the information flows among researchers and academics working in

						the field of internet security.
Licensing authorities (LAs)	LAs would receive less questions and complaints from exporters regarding the interpretation of the export control rules. Changes on controls on intangible technology transfers as well as on brokering and transit could marginally (the volume of these transactions being low) increase administrative costs in the short-term. Security and enforcement would be improved in the medium term.	The move towards open licensing would significantly reduce the administrative burden in terms of staff resources and processing times.	LAs would face short term increases in their administrative costs, as they would need to share on more systematic basis information on catch-all controls. In the medium term, the gains from access to better and more complete information would offset the short-term costs.	The reduction in the remaining barriers to the Single Market would decrease the administrative costs and improve processing times for licensing requests.	LAs would face only marginal increases in their administrative burden: human rights are already included in the current regulatory framework, although not explicitly, as a criterion for export controls. Their inclusion as a distinct control criterion should not substantially increase the number and complexity of existing controls. The broadening of the definition of "dual use" items could increase the administrative	LAs could face higher administrative costs, as they would need to train highly specialized teams able to evaluate specific types of cyber-surveillance technology.

					burden by expanding the scope of existing controls.	
Exporters	Exporters would need to devote fewer resources to compliance. They would be able to assess the legal implications of their exports more easily and with greater predictability.	Exporters would get their licenses faster. The introduction of new EUGEAs would extremely facilitate exports and reduce the costs of compliance.	Exporters would face a more uniform application of export control, and will be able to better predict the requirements and control criteria adopted by LAs in different Member States.	Exporters would benefit from a better level playing field, with no distortion of competition among companies established in different Member States.	Expanding the definition of "dual use" items would broaden the scope of dual use export controls, and thus introduce new items in the scope of Reg. 428/2009. Similarly, the introduction of a specific human rights criterion may marginally increase the number of export denials and thus decrease the exports to third countries.	Exporters of cyber-surveillance technology would need to apply for licenses in order to export their products to third countries. The intangible transfer of encrypted data and of information concerning the vulnerabilities in software may also become more difficult.
Large corporations	A company with branches in different Member	A multinational company could export more easily its	Companies operating across different Member States, or	Large corporations operating in different Member States would	Large corporations exporting goods	Large corporations exporting newly controlled items would

	States would know, for each transaction, which is the relevant competent authority entitled to issue or refuse them a license.	products (especially semi-finished) to its foreign branches. The transfer of encrypted data would also be easier. Companies operating on the supply chain of IT products (e.g. producers of frequency changers) would export their products more easily.	having branches all over the EU would be able to predict the criteria for the application of catch-all controls by LAs of all EU Member States.	face more uniform and predictable rules across the EU.	that – although not being directly linked to military and WMD applications – would classify as "dual use" under a new, broader definition would face proportionally additional administrative and compliance costs. The introduction of a human rights criterion should only marginally shrink the exports of large corporations, as implicit controls based on human rights concerns are already applied under the current regulatory framework.	face additional administrative burden. As the list of controlled cyber-surveillance technology is expected to be very specific, the additional burden is should not be heavy.

SMEs	SMEs devote less resource to compliance: more legal clarity would significantly reduce the legal and administrative costs of compliance.	SMEs operating in specific market niches (such as frequency changers, IT products, encryption) covered by new EUGEAs would benefit from easier export procedures.	SMEs devote less resource to compliance, and it is more difficult for them to interact and with LAs of Member States other than the one where they are established. Higher predictability of catch-all controls would be particularly beneficial for SMEs, as it would reduce the cost of controls for them.	A better EU-level playing field is particularly beneficial for SMEs, who operate mainly within the EU level.	SMEs would face the same benefits and challenges as large corporations.	The impact of stronger controls linked to human rights could significantly impact those SMEs that produce and export exclusively some specific cyber-surveillance technologies. Some of them may choose to relocate in third countries with looser rules.

ANNEX 4. QUANTITATIVE DATA ON EXPORT CONTROLS.

1. Licensing and denials data

Dual-use items are civilian items that can have military applications. Due to this hybrid nature, distinct data on dual-use production (size of the dual-use sector, dual-use related jobs) as well as on dual-use trade (exports of dual-use items) are not easily derivable from public statistics, but need to be estimated. Over the last years, the Commission – in partnership with the Joint Research Centre - has put into place a number of initiative aimed at improving data collection and analysis in this area.

At this moment in time, the following types of data sources on EU dual-use sector trade and production profile are available:

1. A statistical methodology has been developed in 2013 to assess trade flows, based on the DG TAXUD correlation table, which links dual-use items to customs codes: this allows for a quantification of trade flows including dual-use items.[113]

2. Licensing data have been collected since 2013 and aggregate values published in a yearly Commission annual report. Data on export denials are also shared by Member States through the IT platform "Dual Use Electronic System". Although for security and commercial reasons these data are not public, the aggregate figures on the volume and values of licenses application and authorizations, as well as of denied exports are made publicly available on a yearly basis by the Commission, based on the obligations outlined in Reg. 428/2009.

3. Some data can be gathered from open sources, e.g. from specialised publications on specific sectors. Similarly, the private sector sometimes provides data on dual-use trade and production on a voluntary basis in the context of dialogues organised by the Commission. Although useful, these data are difficult to use as a basis for generalizations and for the purpose of the Impact Assessment. In fact, they often describe specific sectors globally, without providing a clear and replicable methodology to discern between dual use and non-dual use-specific figures.

In the absence of official statistics capturing dual-use production and trade, based on the sources outlined above it is possible to identify some figures that – subject to the *caveats* above – can provide an estimation of the overall economic and social (i.e. job-related) dimension of the dual use sector in Europe. In particular, the following data are available and presented in this Impact Assessment Report:

- Estimate of the dual-use related trade
- Volumes and values of licenced/controlled exports
- Volumes and values of denials

As part of the impact assessment, a dedicated data collection project was commissioned to SIPRI and ECORYS (see Annex 5) which validated the data collection methodology developed by the Commission since 2013 and provided further details e.g. on trade flows and on specific sectors. The SIPRI/ECORYS data collection project gathered data on the basis of: a) public statistics on trade, production, employment and the number of enterprises; b) licencing and export data provided by Member States in the annual data exchange process; and c) data obtained from the private sector through interviews and online surveys.

2. Administrative burden

As part of the ongoing effort to quantify the impacts of the Export Control Policy Review, the Commission has also developed a methodology to estimate the cost of licensing dual-use items. The exercise has been conducted on the basis of the following data sources:

- Members States' licensing authorities have provided their estimation of the average time for a national authority to issue an export license, as well as the hourly cost of one labour unit.
- The companies which took part to the public consultation provided their estimation of the average time that an exporter needs to file a request for an export authorization, as well as the hourly cost of one labour unit.

Based on these data, it was possible to estimate the aggregate cost of an export license, and the savings that derive from the streamlining of licensing activities through, for instance, the introduction of new EU General Export Control Authorizations.

Total cost of dual use export control licensing in the EU in 2013

Licence Type	Typical Tasks	Estimated cost for licensing authorities (man-hours)[1]	Estimated cost for exporters (man-hours)
Individual	**End User Certification**: • Preparation • Request from End User and associated follow up communications • Problem resolution • Document Retention **Licence Application:** • Preparation and pre-submission checks • Submission (OELAS) • Problem resolution **Licence Management:** • Record retention • Continuation sheets • Internal controls & checks • SAD Review and forwarder control • Risk Management and audit controls	12 man-hours * €87,5 = **€1,050**	18 man-hours * €100 = **€1,800**
EUGEA	**End User Certification:** • Generally not required **Licence Application:** • Aside from first time use, no licence application required **Licence Management:** • Record Retention • Internal Controls & Checks • SAD Review and forwarder control • Risk Management and	1 man-hour * €87,5 = **€87,5**	3,6 man-hours * €100 = **€360**

[1] The HR and Budget unit of DG TRADE estimated the daily cost of a senior expert as €800 in private companies and €700 in public administrations. The time needed for licensing and EUGEAs applications has been estimated as the median value of the data points provided by Member States licensing authorities as well as by some major dual-use exporters which took part to the online public consultation.

	audit controls		

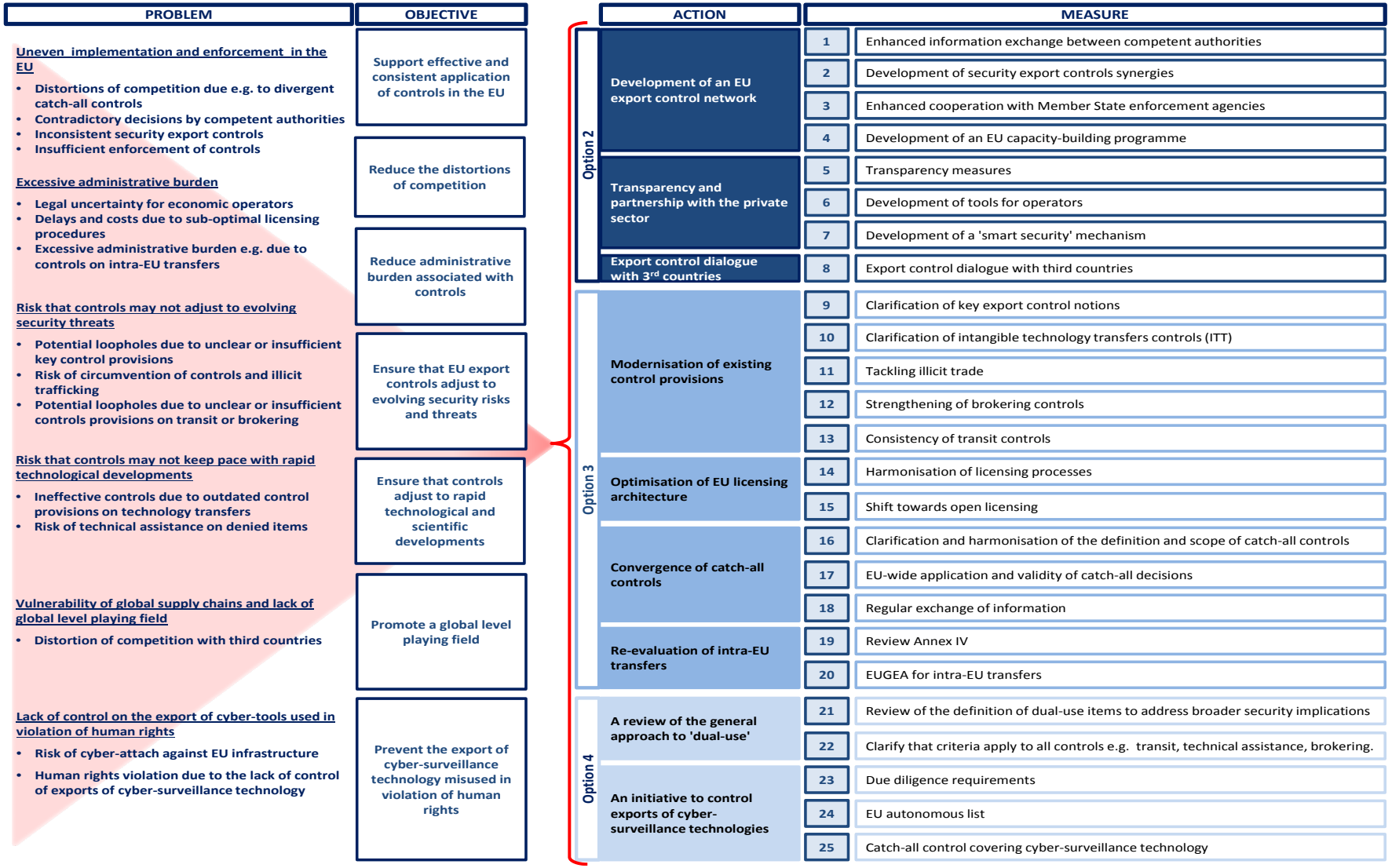
Total cost of applications:
Number of individual license applications in 2013: **34,926**
34,926 * (€1,050+€1,800) = **€99,5 million**

Total cost of licenses
Number of individual licenses issued in 2013: **27,807**
27,807 * (€1,050+€1,800) = **€79,3 million**

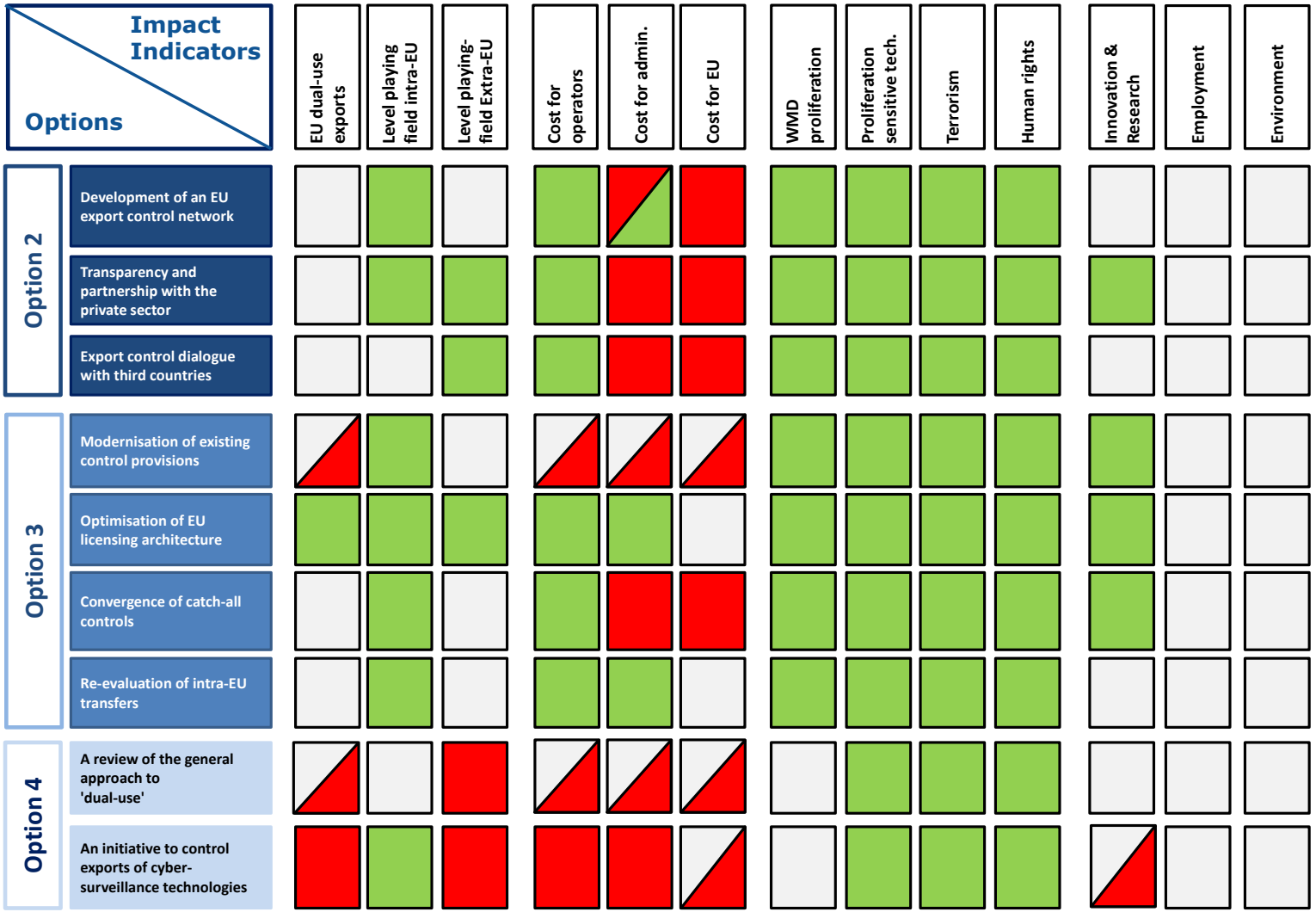
ANNEX 5 – SIPRI/ECORYS DATA COLLECTION REPORT.

The SIPRI/ECORYS report is available at the following link: http://trade.ec.europa.eu/doclib/html/154962.htm.

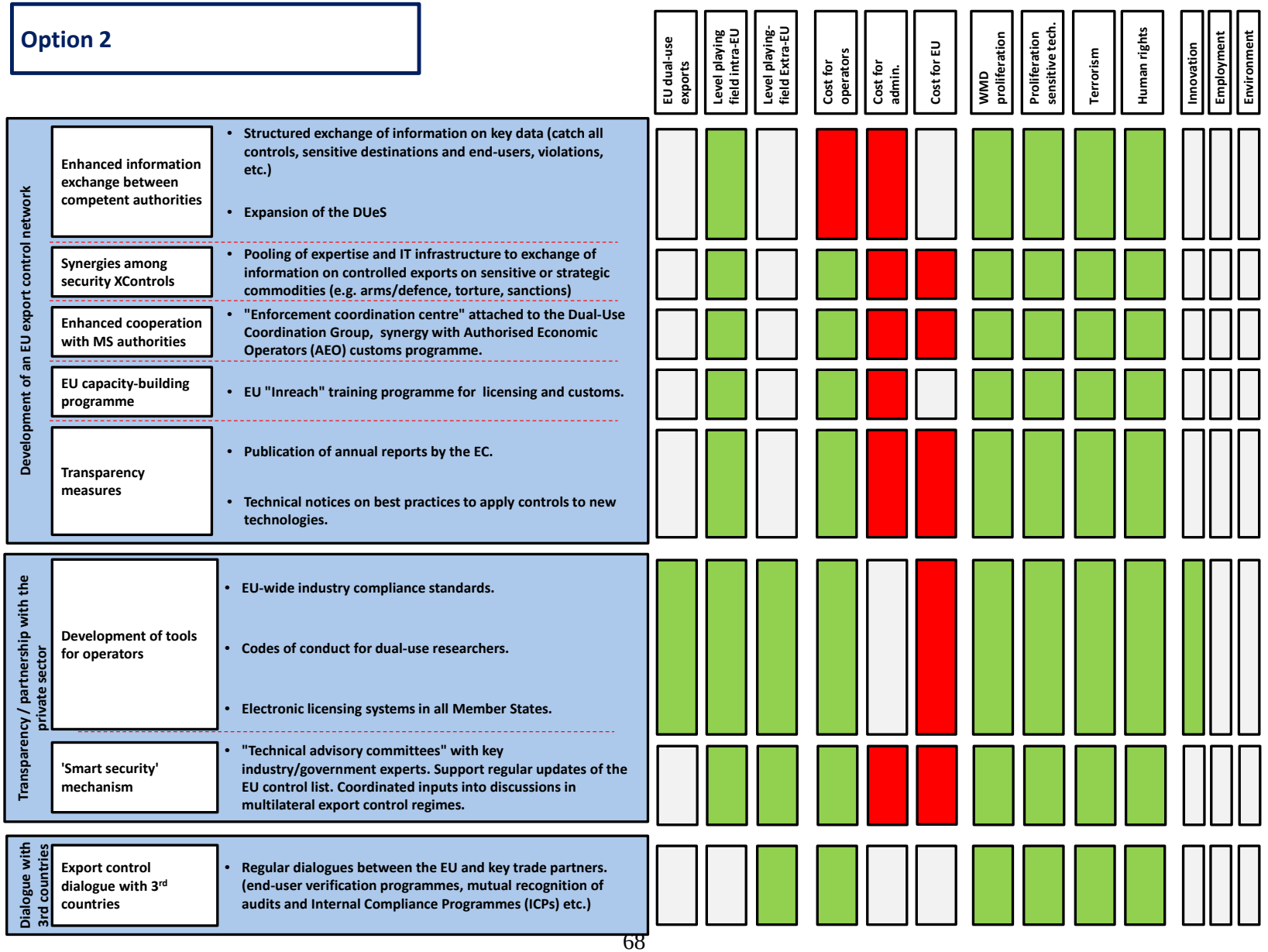
ANNEX 6 – INTERVENTION LOGIC: LINK BETWEEN PROBLEMS, OBJECTIVES AND OPTIONS.



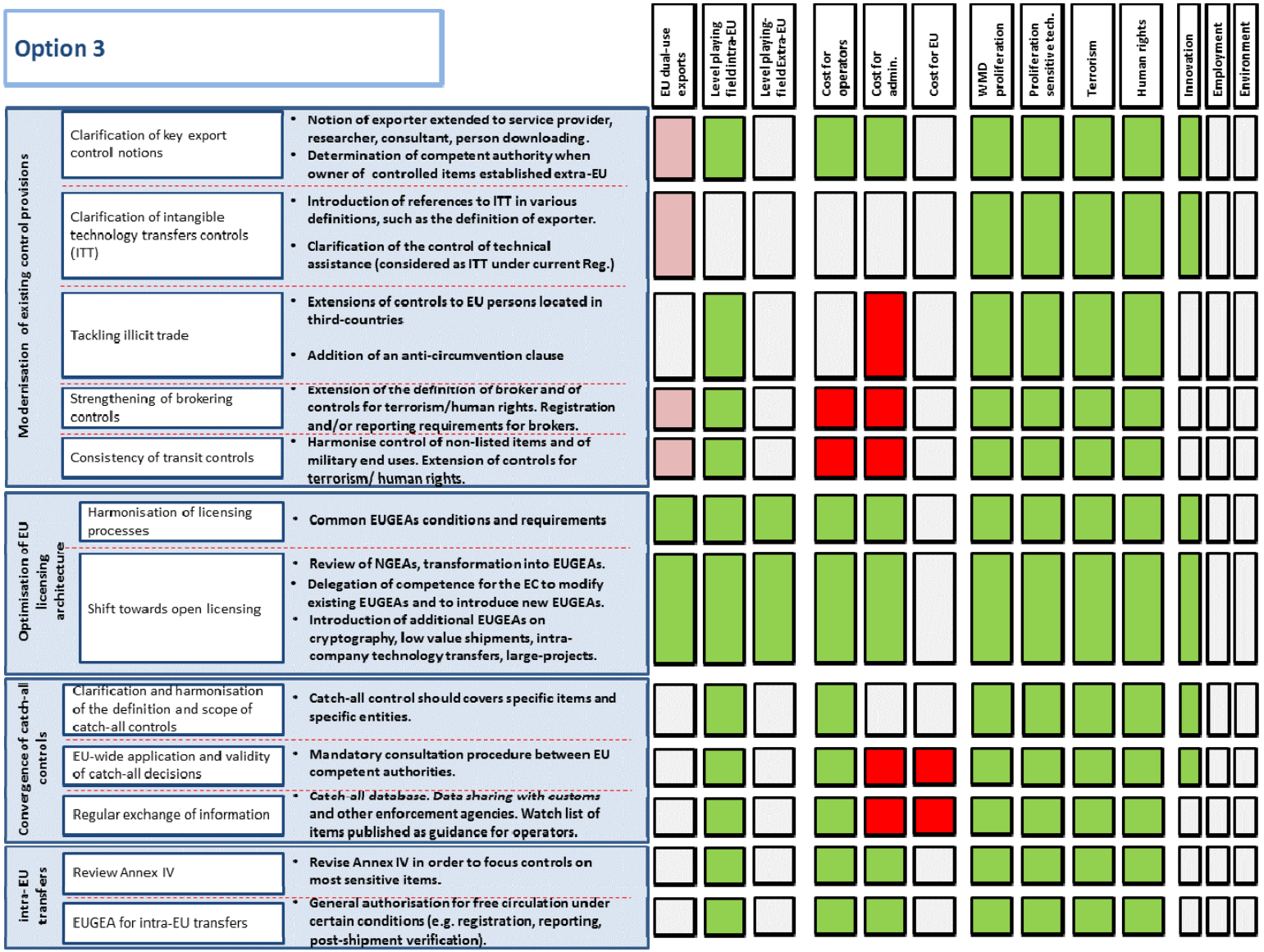
ANNEX 7 – DETAILED PRESENTATION OF THE ASSESSMENT OF IMPACTS OF REVIEW OPTIONS AND ACTIONS



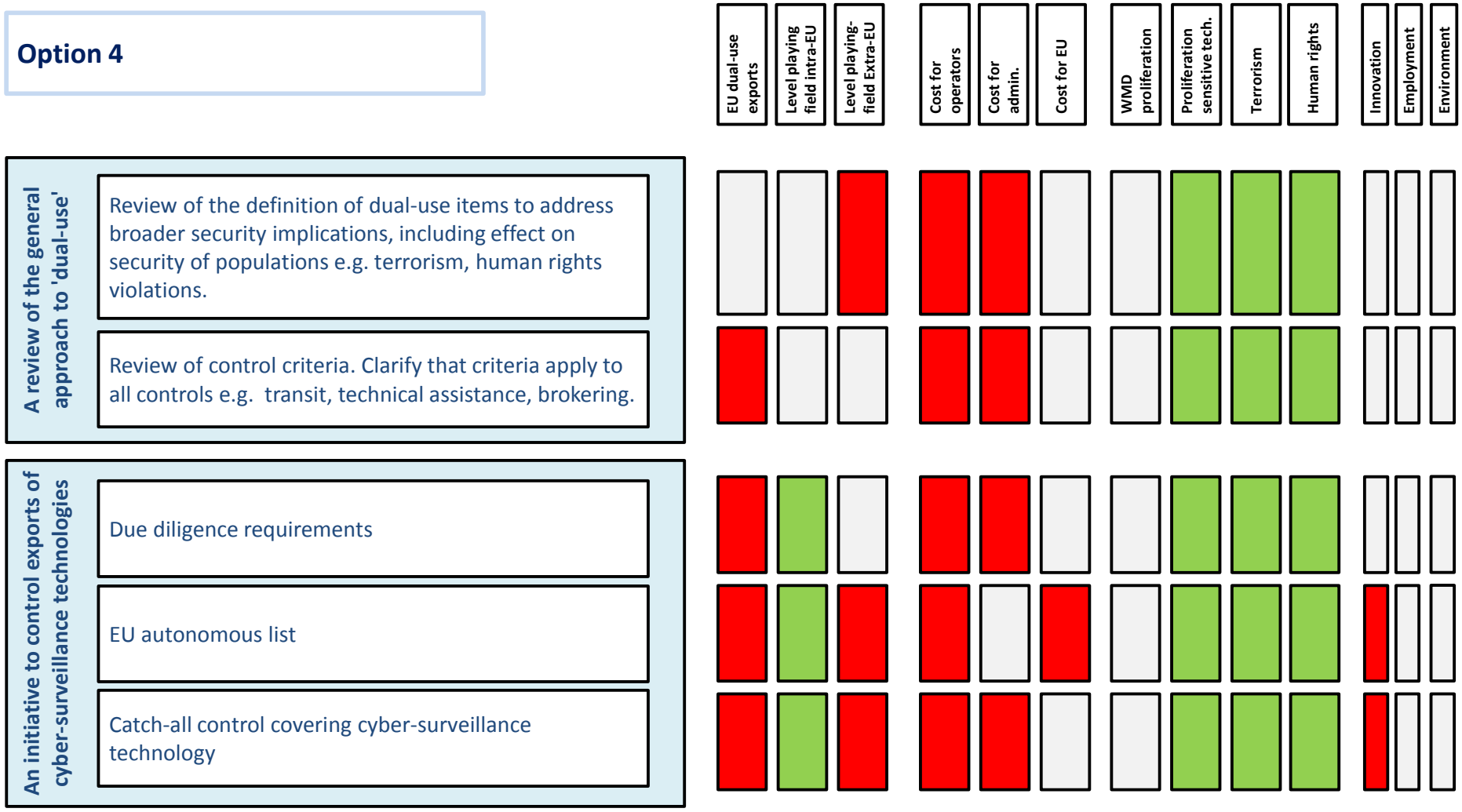
Option 2


EU dual-use exports
Level playing field intra-EU
Level playing-field Extra-EU
Cost for operators
Cost for admin.
Cost for EU
WMD proliferation
Proliferation sensitive tech.
Terrorism
Human rights
Innovation
Employment
Environment
Development of an EU export control network
Enhanced information exchange between competent authorities
• Structured exchange of information on key data (catch all controls, sensitive destinations and end-users, violations, etc.)
• Expansion of the DUeS
Synergies among security XControls
• Pooling of expertise and IT infrastructure to exchange of information on controlled exports on sensitive or strategic commodities (e.g. arms/defence, torture, sanctions)
Enhanced cooperation with MS authorities
• "Enforcement coordination centre" attached to the Dual-Use Coordination Group, synergy with Authorised Economic Operators (AEO) customs programme.
EU capacity-building programme
• EU "Inreach" training programme for licensing and customs.
Transparency measures
• Publication of annual reports by the EC.
• Technical notices on best practices to apply controls to new technologies.
Transparency / partnership with the private sector
Development of tools for operators
• EU-wide industry compliance standards.
• Codes of conduct for dual-use researchers.
• Electronic licensing systems in all Member States.
'Smart security' mechanism
• "Technical advisory committees" with key industry/government experts. Support regular updates of the EU control list. Coordinated inputs into discussions in multilateral export control regimes.
Dialogue with 3rd countries
Export control dialogue with 3rd countries
• Regular dialogues between the EU and key trade partners. (end-user verification programmes, mutual recognition of audits and Internal Compliance Programmes (ICPs) etc.)

Option 3


EU dual-use exports
Level playing field intra-EU
Level playing-field Extra-EU
Cost for operators
Cost for admin.
Cost for EU
WMD proliferation
Proliferation sensitive tech.
Terrorism
Human rights
Innovation
Employment
Environment
Modernisation of existing control provisions
Clarification of key export control notions
• Notion of exporter extended to service provider, researcher, consultant, person downloading.
• Determination of competent authority when owner of controlled items established extra-EU
Clarification of intangible technology transfers controls (ITT)
• Introduction of references to ITT in various definitions, such as the definition of exporter.
• Clarification of the control of technical assistance (considered as ITT under current Reg.)
Tackling illicit trade
• Extensions of controls to EU persons located in third-countries
• Addition of an anti-circumvention clause
Strengthening of brokering controls
• Extension of the definition of broker and of controls for terrorism/human rights. Registration and/or reporting requirements for brokers.
Consistency of transit controls
• Harmonise control of non-listed items and of military end uses. Extension of controls for terrorism/ human rights.
Optimisation of EU licensing architecture
Harmonisation of licensing processes
• Common EUGEAs conditions and requirements
Shift towards open licensing
• Review of NGEAs, transformation into EUGEAs.
• Delegation of competence for the EC to modify existing EUGEAs and to introduce new EUGEAs.
• Introduction of additional EUGEAs on cryptography, low value shipments, intra-company technology transfers, large-projects.
Convergence of catch-all controls
Clarification and harmonisation of the definition and scope of catch-all controls
• Catch-all control should covers specific items and specific entities.
EU-wide application and validity of catch-all decisions
• Mandatory consultation procedure between EU competent authorities.
Regular exchange of information
• Catch-all database. Data sharing with customs and other enforcement agencies. Watch list of items published as guidance for operators.
intra-EU transfers
Review Annex IV
• Revise Annex IV in order to focus controls on most sensitive items.
EUGEA for intra-EU transfers
• General authorisation for free circulation under certain conditions (e.g. registration, reporting, post-shipment verification).

Option 4


EU dual-use exports
Level playing field intra-EU
Level playing-field Extra-EU
Cost for operators
Cost for admin.
Cost for EU
WMD proliferation
Proliferation sensitive tech.
Terrorism
Human rights
Innovation
Employment
Environment
A review of the general approach to 'dual-use'
Review of the definition of dual-use items to address broader security implications, including effect on security of populations e.g. terrorism, human rights violations.
Review of control criteria. Clarify that criteria apply to all controls e.g. transit, technical assistance, brokering.
An initiative to control exports of cyber-surveillance technologies
Due diligence requirements
EU autonomous list
Catch-all control covering cyber-surveillance technology

ENDNOTES

[1] There are four "multilateral regimes" bringing together key technology suppliers: the Australia Group (chemical and biological items), the Nuclear Suppliers Group (nuclear technology), the Missile Technology Control Regime (rocket and other unmanned air vehicle delivery systems) and the Wassenaar Arrangement (sensitive items that contribute to the development of military capabilities).

[2] Most EU Member States participate in all of the four multilateral export control regimes in order to exchange relevant information, discuss control approaches and adjust the lists of sensitive items. The EU directly implements those decisions, but the control modalities are determined, to an extent, at EU level.

[3] An overview of national measures is published at regular intervals – see OJ C51/8, 13.02.2015, p. 8.

[4] COM (2011) 393 of 30.6.2011 and SWD (2013)7 of 17.1.2013.

[5] See respectively: European Parliament resolution of 8 September 2015 on 'Human rights and technology:

the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI)) and Council Conclusions of 21 October 2013 on ensuring the continued pursuit of an effective EU policy on the new challenges presented by the proliferation of weapons of mass destruction (WMD).

[6] COM (2013)710 of 16.10.2013. This report was required under Art. 25.4 of the Regulation.

[7] COM 2014)244 of 24.4.2014.

[8] https://www.fidh.org/IMG/pdf/note_affaire_amesys_fr.pdf.

[9] SIPRI/ECORYS Data collection project, p. 122.

[10] This figure includes individual licences, global licences, intra-EU licences, and licences under national controls.

[11] US Department of Commerce, Bureau of Industry and Security.

[12] "surveyed companies" refers to industry associations and companies surveyed by the consultant in the context of the data collection report.

[13] SIPRI/ECORYS Data collection project, p. 118.

[14] SIPRI/ECORYS Data collection project, p. 129.

[15] COM (2013)710 of 16.10.2013.

[16] Annex IV of the Regulation is a subset of Annex I, which contains the EU list of dual-use items.

[17] See for example the US Export Control Reform: http://export.gov/ecr/index.asp

[18] The DUeS is an electronic system that allows for the secured exchange of information between Member States and the Commission, e.g. on denied exports.

[19] SIPRI/ECORYS Data collection project, p. 101.

[20] Council conclusions, 21 October 2013

[21] http://www.nti.org/analysis/opinions/greatest-terrorist-threat/

[22] http://www.australiagroup.net/en/agm_june2015.html

[23] https://www.ice.gov/doclib/news/releases/2014/140423philadelphia.pdf

[24] http://www.sciencemag.org/news/2015/07/dutch-appeals-court-dodges-decision-hotly-debated-h5n1-papers.

[25] Summary Report of the 2015 EU Non-Proliferation and Disarmament Conference.

[26] See for example: http://www.cfr.org/weapons-of-mass-destruction/likely-nuclear-terrorist-attack-united-states/p13097.

[27] https://www.washingtonpost.com/world/europe/ap-investigation-nuclear-smugglers-sought-terrorist-buyers/2015/10/06/cc398ffe-6c90-11e5-91eb-27ad15c2b723_story.html.

[28] Various press articles reported in October 2015 that ISIS militants used mustard agent in Northern Iraq.

[29] King's College London, "Iran's procurement activities", 30 June 2015.

[30] http://www.wassenaar.org/.

[31] RR\1079477EN.doc.

[32] http://www.globalcause.net/resources/cause-calls-eu-update-dual-use-regulation-protect-human-rights.

[33] European Parliament resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI)).

[34] European Parliament resolution of 17 December 2015 on arms export: implementation of Common Position 2008/944/CFSP (2015/2114(INI)).

[35] OJ L218/8 of 14 August 2013.

[36] For latest update: see Commission Delegated Regulation C(2015) 6823 final of 12 October 2015.

[37] See for example: https://nakedsecurity.sophos.com/2015/07/14/us-government-takes-aim-at-3d-printed-guns/.

[38] Data collection project, p. 235. Data provided by relevant industry associations.

[39] NGEAs are national measures allowing the export of certain dual-use items to certain destinations subject to certain conditions. NGEAs (and EUGEAs) represented facilitated control mechanisms, as there is no need for an authorisation ('individual licence') prior to the export.

[40] 2014 Annual Report (http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm). The difference between applications and licences correspond to decisions that items under consideration do not meet the technical parameters of the EU list, to yearly adjustments and, for a small number, to denied exports (denials).

[41] SIPRI/ECORYS Data collection project. This data may cover other export controls e.g. on arms exports and sanctions. On the other hand, this data does not capture staff from other government departments, agencies and ministries in relation to the implementation and enforcement of the Dual-use Regulation.

[42] See Annex 4 for an explanation of the underlying methodology.

[43] Source: ASD.

[44] Source: CECIMO.

[45] Source: ESIA.

[46] Calculcation by the Joint Research Centre, Statistical Trade Analysis, 2014 data.

[47] 'Cybersecurity Market 2015-2025" *MarketWatch*, 22 June 2015, <http://www.marketwatch.com/story/cyber-security-market-2015-2025-leading-companies-in-network-data-endpoint-application-cloud-security-identity-management-security-operations-2015-06-22>.

[48] CAUSE report, June 2015. Vernon Silver, 'Spies Fail to Escape Spyware in $5 Billion Bazaar for Cyber Arms', Bloomberg, 22 December 2011.

[49] CEFIC statistics include Switzerland, Norway, Turkey, Russia and Ukraine.

[50] Source: EU Energy in Figures: Statistical Pocketbook 2015, publisher European Commission

[51] Source www.Foratom.org

[52] Report, IHS Jane's Intelligence Review, October 2015.

[53] Source: Technopolis, Study ENTR/172/PP/2012/FC.

[54] It should however be noted that large enterprises, representing 6% of the total number of firms, actually account for 79.4% of total turnover, thus revealing the strong concentration of this industry.

[55] Source: Technopolis, Study ENTR/172/PP/2012/FC. Calculations based on Eurostat SBS for the number of firms and turnover and on Amadeus for the number of employees and Intangible Fixed Assets (IFA).

[56] The CAUSE coalition brings together Amnesty International, Digitalle Gesellschaft, FIDH, Human Rights Watch, Privacy International, Open Technology Institute, Reporteurs Sans Frontières, and Access.

[57] The ECJ held that "Article 6 of the Charter lays down the right of any person not only to liberty, but also to security" in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, § 42.

[58] Some stakeholders take the view that there is no such thing as a 'dual-use sector'. The Commission, for its part, has referred to the 'elusive dual-use sector' in its communications.

[59] SIPRI/Ecorys Data collection report, p.

[60] This figure includes values of licence applications and notifications under General Export Authorisations. The difference between applications and authorisations consists essentially of "zero notices", i.e. applications for licence by exporters that are not sure about the classification of the items and ask for a determination of the licensing authorities, without a licence being eventually issued. The difference also includes a small proportion of export denials.

[61] In 2013, denied exports amounted to 0.003% of total exports. This value is however highly variable from one year to another.

[62] 2013 Annual Report, calculation by the Joint Research Centre.

[63] Source: SIPRI/ECORYS Data collection project, p. 75.

[64] http://ec.europa.eu/trade/policy/in-focus/trade-and-jobs/

[65] Considering that dual-use items represent roughly 3.1% of EU exports (2013 data),

[66] Source: CECIMO.

[67] Source: CEFIC.

[68] Source: ASD.

[69] COM (2011) 393 of 30.6.2011.

[70] SWD (2013)7 of 17.1.2013.

[71] COM(2013)710 of 16.10.2013.

[72] OJ L173/82 of 12.06.2014, p. 82.

[73] See case C-70/94 and C-83/94.

[74] See in particular Articles 2, 4, 13 and 35 of the Charter.

[75] Council Conclusions on ensuring the continued pursuit of an effective EU policy on the new challenges presented by the proliferation of weapons of mass destruction (WMD), 21 October 2013.

[76] COM(2015)497 of 14.10.2015.

[77] Similarly, a key objective of the US export control reform launched in 2010 by President Obama consists in the development of common rules and a single system for arms and dual-use export controls.

[78] The Dual-Use Coordination Group, created by Art. 23 of the Regulation, brings together experts from the Commission and Member States to monitor and coordinate implementation of export controls.

[79] Operators can be accredited by Customs as AEOs when they prove to have high quality internal processes that will prevent goods in international transport to be tampered with. The AEO programme is key to ensuring the integrity of global supply chains and securing the international trade flow.

[80] Over the last 10 years, the EU has funded an "Outreach Programme on Dual-Use Export Controls" for third countries. The 2013-2014 programme supported outreach to 28 countries, with a budget of EUR 3 million.

[81] For example, the US and Japan have issued guidance on the control of technology transfers on the cloud.

[82] Technical assistance involving a cross-border movement of persons is thus far controlled by Member States based on a Council Decision.

[83] The basic principle underlying EU brokering controls is that they may result in a licence requirement only in special circumstances, when there is a clear risk of WMD or military end-use; in other words, there is no systematic control of brokering of dual-use items.

[84] The basic rule underlying EU transit controls for dual-use items is that it can be prohibited by competent authorities in specific cases in relation to a WMD end-use; in other words, there is no systematic licensing requirement for the transit of dual-use items

[85] Catch-all provisions allow a competent authority to control items not listed in the EU control list. It is often described as an "emergency brake" as it provides the authorities with the ability to respond swiftly to unexpected risks by applying greater scrutiny and, where necessary, by preventing exports of concern.

[86] EU experts regularly update a correlation table linking dual-use items with customs code, but the correlation remains limited, since both classifications fundamentally differ.

[87] A 2012 study estimated training costs at between EUR 1.5 and 2.5 million per year depending on the training format, and confirmed the demand from authorities for an EU training programme.

[88] Some key trade partners (US, Japan) have issued guidance which clarifies the application of controls on technology transfers through cloud computing for the benefit of their operators.

[89] SIPRI/Ecorys Data collection project, p. 128.

[90] 2014 Annual Report.

[91] 2014 Annual Report.

[92] SIPRI/Ecorys data collection project, p. 128.

[93] SIPRI/Ecorys Data collection project, p. 137.

[94] SIPRI/Ecorys Data collection project, p. 137.

[95] SIPRI/Ecorys Data collection project, p. 128.

[96] SIPRI/Ecorys Data collection project, p. 137.

[97] SIPRI/Ecorys Data collection project, p. 137.

[98] US Commerce Undersecretary for Industry and Security Eric Hirschhorn, commenting the ongoing US export control reform, said the "rolling review" is a key component of the constant refinement of export controls… because technology, threats and industry understandings and misunderstandings evolve, the regulations needed to evolve alongside of them". (*www.InsideTrade.com* - November 6, 2015).

[99] Annual reports on the implementation of the export control regulation, including licensing data, have been published since 2013.

[100] The results of the discussion are summarised at:
http://trade.ec.europa.eu/doclib/docs/2013/july/tradoc_151594.pdf

[101] The results of the discussion are summarised at:
http://trade.ec.europa.eu/doclib/docs/2014/october/tradoc_152858.pdf

[102] The results of the discussion are summarised at:
http://trade.ec.europa.eu/doclib/docs/2015/december/tradoc_154041.pdf

[103] The reports are publicly available at https://www.fidh.org/IMG/pdf/cause_report_final.pdf and https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf

[104] In accordance with paragraph 3 of the Specific Privacy Statement of the Online Public Consultation on the Export Control Policy Review, all the contributions received, together with the identification data of the respondent, have been published on the Internet, except for those where respondents expressed explicit objection in the questionnaire.

[105] Two responses were not related to the consultation topic and will not therefore be included in the following analysis.

[106] The remaining 10% included individuals as well as companies and associations declaring not to be part of any of the abovementioned categories.

[107] For the purposes of the questionnaire, large enterprises are defined as those with at least 250 employees.

[108] In detail, the breakdown between small, medium and micro enterprises was respectively 6%, 11% and 7%.

[109] The category "Other" includes four Member States licensing authorities, one individual and nine industry associations.

[110] As outlined in the Communication 2014(244), the "human security approach" intends to place people at the heart of EU export control policy, in particular by recognising the interlinkages between human rights, peace and security. See http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf

[111] The development of a strategy for "immaterial control" would be aimed at moving beyond the current focus on tangible (goods) transactions towards electronic movement of data that can be used to modify and produce unlimited quantities of sensitive items. Concretely, this would entail addressing the challenge posed by Intangible Transfers of Technology (ITT), including the need to clarify the control of 'dual-use research', while avoiding undue obstacles to the free flow of knowledge and the global competitiveness of EU science and technology.

[112] "Catch-all controls" apply to items that are not listed in the Dual Use Regulation when there are indications that they pose a risk of proliferation or military application. A summary of the basic concepts of Dual Use Export Controls can be found at the link: http://trade.ec.europa.eu/doclib/docs/2014/february/tradoc_152181.pdf

[113] For a detailed explanation of the methodology, see Versino C. Dual-use trade figures and how they combine. JRC97664, EUR 27514 EN, ISBN 978-92-79-52715-9, doi:10.2789/439924, 2015 (2015).