BDI
Bundesverband der
Deutschen Industrie e.V.

POSITION PAPER

EU Dual-Use Reform: EC Proposed Regulation COM(2016) 616

April 2017

On 28 September 2016 the European Commission adopted the reform proposal COM(2016) 616 final, which envisages extensive changes to the EU Dual-Use Regulation. The European Parliament and the Council will now debate the European Commission's proposed Regulation. The main areas covered by the proposed Regulation go beyond the stated goals of the reform. This could have a negative impact on the future of Europe and Germany as technology locations. The European Parliament and the Council must now exercise good judgment in the legislative process and provide answers to open questions.

- **A revision of the proposed Regulation is urgently needed**

  The proposed Regulation fails to strike a balance between effectiveness and efficiency in core areas. The *Impact Assessment* of the European Commission is incomplete. The reasons provided for the introduction of new rules are insufficient. It is therefore not in line with the important efforts to reduce bureaucracy within the EU – the so-called REFIT agenda. Legal certainty will not be established solely on the basis of the announced EU guidelines since these are not legally binding.

- **Product and country lists instead of catch-all rules**

  BDI supports stronger protection of human rights in the area of export control. Stricter export controls over digital-surveillance technologies can improve this protection when the controls are effective and efficient. The legislator should opt for specific product and country lists instead of catch-all rules.

- **No criminalization of digital technologies: clarify definitions**

  The definitions for cyber-surveillance technology introduced in the proposed Regulation extend to components for crucial public digital infrastructure. Digital technology used for monitoring more intelligent and more complex infrastructure (such as in the supply of energy and water) is indispensable. Only the application of these technologies can guarantee the functioning and the protection of that infrastructure. The proposed Regulation does not take this important point sufficiently into account.

Verena Kantel | Abteilung für Außenwirtschaftspolitik | T: +49 30 2028-1518 | V.Kantel@bdi.eu

Content

Goals and Drivers of the Reform

Through the reform, the European Commission intends to bring export controls in line with the changing technological and security environment. The Directorate-General for Trade emphasizes that this should be done within the framework of a value-based trade policy. Dual-use export controls have so far applied to products that can be used for both civilian and military purposes and are mainly associated with ABC weapons or with the missiles capable of delivering such weapons. However, in the view of the European Commission, cyber- surveillance technologies create new threats which require stricter export controls for these products. Members of the European Parliament are also demanding that EU countries and companies assume more responsibility in the export of certain cyber- surveillance technologies, for example technologies that could be used by states to monitor regime opponents. These demands are a response to the democratization movements of the Arab Spring, when human rights activists and journalists were located by means of cyber- surveillance technologies and readouts of their social-network posts were obtained. According to press reports, these technologies originated from the EU, among other places.

The value-based trade policy is an integral part of the EU's "Trade for All" strategy and is intended to ensure high standards of sustainability, human rights, and democracy. At the same time, the European Commission stresses that through the reform, export controls should become more effective (when protecting against threats) and more efficient (in control procedures). In order to strengthen the value-based trade policy, the European Commission has additionally enshrined the "human security approach" in the EU export control regime. To this end, the export of cyber-surveillance technologies will be subject to more restrictions through new definitions of the dual-use good, new authorization requirements, and EU autonomous lists of products. The European Commission also aims to more closely harmonize EU export controls. Among other things, the licensing practices of the EU Member States are to be more rigorously coordinated with one another through an additional exchange of information.

Does the Reform accomplish the Balancing Act between Effectiveness and Efficiency?

The draft Regulation COM(2016)0616 submitted on 28 September 2016 includes a number of positive approaches to increasing the efficiency of controls through the more widespread use of simplifies procedures in the form of EU general export authorizations and collective or global export authorizations. Instead of having to apply for costly individual authorizations for numerous exports of the same goods, firms exporting certain products to non-sensitive countries are exempted under general authorizations from the permit requirement. Moreover, exporters considered especially trustworthy can obtain authorization in advance for a large number of other product exports through one application procedure. In return, those exporters must comply with so-called ancillary clauses – for example, registration and reporting requirements – under the EU general authorizations. A positive feature of the proposed Regulation is the inclusion of new EU general authorizations for encryption technologies (EU009), low-value shipments (EU007), and intra-company software and technology transfers (EU008). The latter is particularly important for global development teams, which increasingly find themselves working on projects across different time zones and different countries.

However, a negative feature is that the validity of individual export authorizations and global export authorizations is limited to one year (Article 10, paragraph 3). Furthermore, an internal compliance program (ICP) is required for global export authorizations (Article 10, paragraph 4). It remains unclear whether the evaluation of the company-specific ICPs will take into account the differences between the organizational structures of small and large companies in a sufficient manner. From the perspective of industry, several fundamental rules weigh heavy. These include the authorization requirements through new catch-all rules (Article 4, paragraphs 1d and 1e), imprecise new definitions of the dual-use good (Article 2, paragraphs 1b and 21), the extraterritorial effect of new definitions of broker and supplier of technical assistance (Article 2, paragraphs 7 and 9), and new EU autonomous lists (Article 16).

German industry does not question the human security approach of the European Commission. Industry organizations have supported the latest amendments to the anti-torture regulation, the new listings in the international export control regimes, and the EU embargos which lists goods that could be used for internal repression. The BDI, for its part, explicitly backs a stronger protection of human rights. But the legislator has so far failed to concretely identify the critical cases and provide tailor-made controls for protection against internal repression in third countries. Non-specific catch-all rules cannot achieve this. They are neither effective nor efficient. Concrete definitions and country and product lists are better suited to achieving this goal. The European Commission has failed to take sufficient account of two important criteria – namely, ensuring a global level playing field as well as an EU internal level playing field.

Legal uncertainty can have serious consequences. Non-precise definitions and non-specific catch-all rules threaten the export potential and competitiveness of German and European industry. They lead to uncertainty in export procedures. Employees, out of fear of liability consequences, submit so-called safeguard applications to the licensing authorities, leading to an unnecessary delay in delivery. If a non-specific human rights catch-all rule puts cyber surveillance technology under export license reservation, the core of industry 4.0 will be affected – an area that is essential for the economic development of the EU. For this reason, it is imperative that the legislator passes a regulation after careful consideration that includes precise rules. Today, soft- and hardware for monitoring and evaluating data streams or processes are used in almost all industrial applications and fulfil important functions:

1. **Intelligent energy, water and gas supplies.** Security and surveillance technologies serve to protect against attacks and help detect security flaws. In addition, network loads are analyzed to control the desired energy mix.

2. **Intelligent traffic concepts.** Security and surveillance technologies make intelligent traffic management systems possible and contribute to the increased digitalization of tracks, roads, and aviation and shipping routes. They also make an important contribution to protecting against injuries.

3. **Industrial plant construction and e-health** are increasingly using security and surveillance technologies in data analysis, error minimization control, and remote diagnosis.

Another cause for concern is the statement that unclear provisions of the proposed Regulation will be dealt with only in EU guidelines. From the perspective of industry, this is unacceptable. Guidelines are non-binding and do not guarantee legal certainty. In the course of revising the proposal, the legislator should constantly ask itself if, and to what extent, the goals can be achieved through amendments to the Dual-Use Regulation or if other mechanisms are better suited to serve this purpose. Thus a revision of the proposed Regulation is essential.

Criticism of the Impact Assessment Process

The *Impact Assessment* report submitted in October 2016 fails to perform its important filter and justification function. For this reason, Members of the European Parliament and Council representatives should make use of their right to ask questions and demand justifications at the forthcoming debates. The European Commission must be measured against the rules that it established within the framework of the "better regulation" agenda and the REFIT program for reducing EU bureaucracy. This program envisages reforms that would present EU citizens with a comprehensive *Impact Assessment* report citing the reasons for new regulations and specifying the related costs and administrative burden. For the current reform proposal, the findings of the *Impact Assessment* report SWD (2016) 315 final serve as an important basis. It should be acknowledged that factual knowledge about the number of authorizations in the 28 EU Member States has been documented. However, the report lacks comprehensive information about the strengths and weaknesses in implementation at the national level. Gaps in EU legislation are not concretely identified: while the rapid technological transformation and

the changing security situation[1] are described as constituting a challenge "yet to be tackled" and as justification for the reform, no further details are given.

The report fails to answer the following key questions:

1. Which threat do we want to avert? According to the European Commission, numerous press reports have given rise to the need for stricter export controls. Specifically, those reports relate to cases of internal repression during the Arab Spring.[2] But the European Commission report refrains from listing those cases and describing them in detail. It references only one such case explicitly.[3] Otherwise, it refers to reports and cases only in very general terms.[4] However, those references do not answer the following questions: What happened precisely? Which rights were violated? And which threats could the company have foreseen? The report wholly lacks a detailed description of the critical product groups. Thus it is hardly surprising that definitions and rules such as the catch-all ones in the proposed Regulation are imprecise.

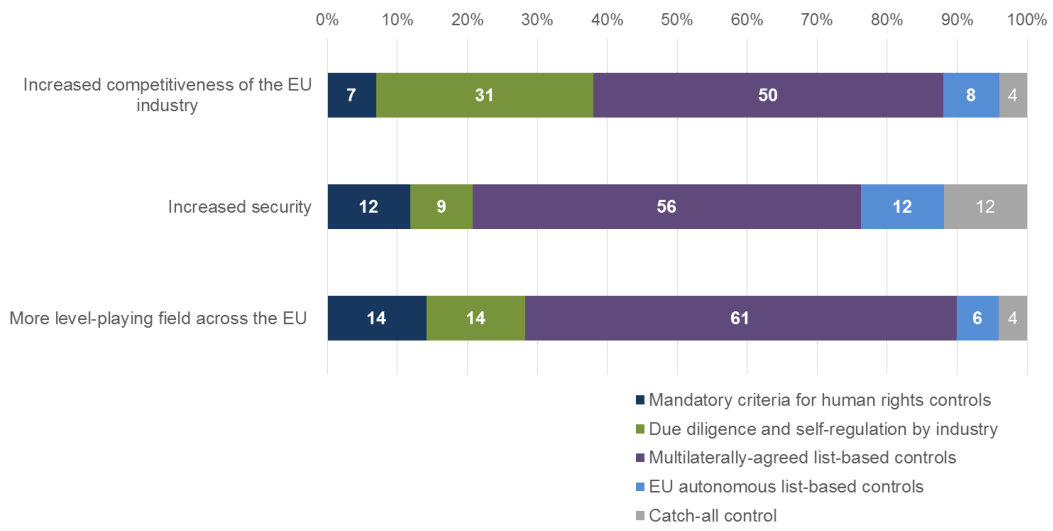
2. Which critical exports are not sufficiently regulated? The European Commission confirms that the EU offers a sound export control mechanism through the EU Dual-Use Regulation that is currently in place.[5] At the same time, it underscores the gaps in regulation for cyber- surveillance technologies and stresses that the implementation of export controls in the Member States is often inadequate. However, these inadequacies are not described in detail. No distinction is made between shortcomings in legislation and in the implementation. Yet the REFIT program provides guidance that demands precisely such a distinction: the functioning of existing legislation should be examined before new laws are passed. Moreover, there is no analysis of the most recent legislative amendments at the European level. Which critical cases have already been prevented by the latest updates to the product lists in Annex I of the Dual-Use Regulation? Which further new listings are currently being discussed in the international export control regimes? Which issues relevant to export controls are not being tackled by the four regimes? And what examples can be found of good national export control rules? The review of the current situation remains incomplete.

3. Why is the legislator deviating from the conventional list approach? The European Commission recommends catch-all rules[6] but thereby breaks with the tried and tested principle of defining lists, which until now has enabled sound export control. The European Commission hardly provides any justification for doing so. Above all, it remains unclear why catch-all controls should be more effective. Even the European Commission's own statistics show: in an EU public consultation conducted in 2015, participants assessed the list approach as being a more effective means of safeguarding security. Specifically, the European Commission asked how likely it was that the human security approach would contribute to increased security. Only 12 per cent of those surveyed believed that catch-all rules would have any effect whatsoever on improving security. By contrast, 56 per cent of those surveyed voiced the opinion that improved security could be achieved by means of the list approach in international regimes. Thus, the existing alternative options are not being sufficiently weighed, even though the very purpose of the REFIT program is to identify the most efficient and effective means among the available alternatives. Moreover, no alternative course of action is identified in the impact assessment. The standard approach involving product lists can be combined with a fast-track procedure, which would offer a more effective means of control than a catch-all rule.

---

[1] European Commission, *Impact Assessment – Report on the EU Export Control Policy Review*, SWD (2016) 315 final, pp. 5–6.
[2] Ibid., p. 10.
[3] Ibid., p. 11 ("Hacking Team").
[4] Ibid., p. 10.
[5] Ibid., p. 5.
[6] Ibid., p. 37ff.

Low Support for Catch-all Controls
"Would you agree that the actions to pursue the 'human security approach' will likely have the following impact?"



Source: European Commission, Impact Assessment – Report on the EU Export Control Policy Review, SWD (2016) 315 final,

4. Why has the EU refrained until now from ensuring consistent and effective compliance with export control legislation in the EU Member States through their companies and from exercising control over compliance or from making such controls mandatory? According to a company survey, 20 out of the 28 Member States are either unwilling or unable to control legal compliance of their companies. The *Impact Assessment* did not undertake a similar survey. It remains unclear which national controls are currently being carried out in the Member States. Foreign trade audits are conducted in Germany and Austria, for example. But what is the situation in other countries? The principle that before new regulations are passed, it must be made sure that existing rules are being uniformly implemented and observed must also apply in this context.

What is clear is that the legislator must be in a position to explain precisely which threats it wants to avert and why it does not consider other, less burdensome means. During the legislative process, Members of the European Parliament and Council representatives should clarify these issues with the European Commission since all three EU institutions bear political responsibility for the reform.

High Degree of Uncertainty for Companies through New Catch-All Rules

The new catch-all rules are a cause for concern as it could lead to considerable efficiency losses. Particularly noteworthy are the human rights-related catch-all rule in Article 4, paragraph 1d and the terrorism catch-all rule in Article 4, paragraph 1e. Since the proven list principle is hereby undermined the European Commission must provide better justification for these measures – or provide justification in the first place. Imprecise legal terms make for legal uncertainty. That uncertainty can result in a *de facto* general export license reservation that was not intended. Moreover, the effectiveness of the catch-all rules is unclear. After all, EU companies can only influence that exports are conducted responsibly if they are able to hold their own in competition with their rivals in foreign markets.

Under the Dual-Use Regulation which is currently in place (Council Regulation (EC) No. 428/2009)**,** goods will be required, as a rule, to obtain an export license based on their technical parameters. Such goods are listed in Annex I of the Dual-Use Regulation. A catch-all provision exists only for possible uses in the area of ABC weapons and missile technology as well as for an application in the military-technical complex that is specified in more or less concrete terms and limited to countries against which a weapons embargo has been imposed. Exceptionally, it is the end use rather than the technical parameter that is relevant under these catch-all rules. However, the end use is specified in accordance with factual circumstances and requires no classification in legal technical terms. On the grounds of the fact-based, sufficiently concrete specification, industry can live with this regulation. Otherwise, the proven list approach applies for both product and country listings.

In the case of non-specific catch-all rules, however, the uncertainty of legal interpretation would be considerable. But it is precisely such uncertainty that is to be found in the proposed catch-all rules in Article 4, paragraphs 1d and 1e.

Terrorism Catch-All Rule (Article 4, paragraph 1e)

According to the Commission draft, the so-called catch-all rules would be extended to the new control target of "terrorism". Companies must henceforth identify critical cases in which there is a danger of products being misused for the purpose of carrying out terrorist acts. To this end, they are required at times to undertake measures and risk assessments not unlike those of intelligence agencies and regional or federal criminal police departments. But owing to the lack of evidence and intelligence information, this goes beyond the capabilities of companies. Moreover, the legal assessment is by no means simple. The definition of "terrorist acts" is itself extremely complex. It is not without reason that the proposed Regulation only refers to the definition contained in Article 1, paragraph 3 of the European Council Common Position 2001/931/GASP, which lists 11 different types of act and describes their aims.

Government entities should not pass on their political responsibility onto companies. For some time now, the European Council has been drawing up sanctions lists composed of natural and legal persons if there is sufficient evidence to suggest that they are supporting terrorist organizations. Trade with these contractual partners is prohibited, providing financial funds is prohibited and punishable (Council Regulation (EC) No. 2580/2001 and No. 881/2002). In their routine export-control compliance activities, companies effectively check their contractual partners against these lists. Furthermore, the criminal codes of Member States prohibit and criminalize the assistance of a terrorist act and make obstruction of justice punishable. Other countries and supra-regional organizations also rely on the tried and tested principle of listing individuals for the purpose of preventing terrorism and other threats or enforcing sanctions: for example, the OFAC's SDN and FSE Lists[7] and the BIS's Entity, DPL, and Unverified Lists[8] in the United States. But both the Office of Foreign Asset Control (OFAC) and the Bureau of Industry and Security (BIS) are – for good reason – government institutions, and their listings are based on intelligence information. These official entities use the specialist knowledge, skills, and information sources of the investigative authorities and secret services. In addition, the lists provide for transparency. They enable citizens and companies to see with whom they are not allowed to do business. As part of the fight against terrorism, the United Nations similarly draws up lists of individuals in the relevant Security Council resolutions.[9] All this begs the question: why should a non-specific catch-all rule be more effective than the combination of terrorism/sanctions lists and national criminal law? In the *Impact Assessment*, this question is not addressed. Indeed, the *Impact Assessment* provides no justifications for or assessments of a terrorism catch-all rule. This is contrary to the REFIT goal of justifying draft regulations, providing more transparency and "better regulation".

---

[7] U.S. Department of the Treasury, *Information on Financial Sanctions,* <https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx> (accessed 18 January 2017).
[8] Bureau of Industry and Security, *Lists of Parties of Concern*, <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list> (accessed 18 January 2017).
[9] United Nations Security Council, *Sanctions*, <https://www.un.org/sc/suborg/en/sanctions/1267> (accessed 18 January 2017).

Human Rights Catch-All Rule (Article 4, paragraph 1d)

The Commission draft also provides for the so-called catch-all rules to extend to the control target of human rights. The question when an export increases the danger of human rights being violated is difficult for companies to answer in a specific case if there is no binding guidance from an official government office about sensitive target countries and critical practices. While the European Commission intends that under the new catch-all rules, guidance will (also) be available from (supra-) state organizations, these are not named. It is also unclear whether the guidance will be binding and how it would be published and made universally accessible. Moreover, the potential filter function is dropped at the latest in the factual situation described in Article 4, paragraph 2, in which it comes down solely to the subjective knowledge of the exporter. Thus it is unclear to companies on the basis of which information they should judge whether surveillance activities in third countries are critical. Indeed, while surveillance and investigative activities by third countries' governments can lead to the monitoring of undesirable regime opponents, they can also provide necessary protection against terrorism and other threats. An effective system of preventing terrorism and other threats is in the interest of global security policy. For companies, it is also unclear which democracy standards apply when making such judgments. Even within Europe itself, the legal assessment of measures related to protection against terrorism and other threats differs from one country to another. How long a company would require for each individual assessment could not be predicted, while conventional and effective risk controls based on IT and lists would be impossible. Companies would carry out individual checks via the authorities not only in cases of doubt or when authorization is clearly required; they would do so routinely as a safeguard. Government entities can better assess which states are to be classified as sensitive countries of final destination on the basis of human rights violations. They have intelligence information at their disposal and, through political processes in the Council, can evaluate and check that information as well as submit it to a consensus. They should not pass on responsibility for evaluations of a political-legal nature onto companies.

In addition, the criterion "country of final destination, as identified by relevant public international institutions or European or national competent authorities" is insufficiently defined. It is unclear what these abstractly described institutions are. Where can the texts in which they "identify" critical countries on the basis of human rights violations be found? Will they be published in the Official Journal of the European Union, as are EU laws and formal notifications?

Moreover, a critical aspect is that the goods-related area of application of the human rights catch-all rule has been expanded, contrary to what was announced earlier. In the *Impact Assessment*, it is only the impact of a catch-all rule related to the product group "cyber-surveillance technology" that is examined.[10] However, in the proposed Regulation, the human rights catch-all rule covers all dual-use products or, according to another interpretation, almost all goods. Thus by no means is the European Commission limiting its catch-all rule to the application area that it had subjected to scrutiny – namely, "cyber-surveillance technology". By the standards of the REFIT process, this is unacceptable.

Impact of New Catch-All Rule: Long Delivery Times Paralyze Project and Product Business

If lengthy individual export authorizations were to make life difficult in particular for the spare parts and services sector, European companies would run the risk of becoming less competitive in the overall project and product business. When making decisions about awarding contracts, a crucial factor for the customer is the assurance of rapid remote diagnosis, repairs, or deliveries of spare parts. The customer wants to minimize the downtime risk. Plants must not be allowed to stand idle. From the customer's point of view, an authorization process that holds up the provision of services by several months would be unacceptable – and inefficient. Overall, German and European companies would become less competitive against foreign manufacturers and lose market power.

[10] Ibid., p. 37.

Industry's Recommendations:

- **Protection of human rights:** The new catch-all control of Article 4, paragraph 1d should be omitted. Instead, companies should check the export of goods against clearly formulated product and country lists. Those lists should be included in Annex I of the Regulation by means of a delegated act. If a new listing in the international regime and thus in Annex I, section A of the Regulation cannot be made but if a control is nonetheless urgently needed, a new listing in Annex I, section B of the Regulation by means of fast-track procedure will be more effective and efficient than a catch-all rule. The fast-track procedure can be analogous to that provided in the recently approved anti-torture regulation. However, an autonomous listing should be a measure of last resort only.

- **Protection against terrorist threats:** The new catch-all control of Article 4, paragraph 1e should be omitted. Instead, companies should check their contractual partners against clearly formulated lists of individuals drawn up by the European Council. In order to provide lists that are more reliable, European intelligence agencies should pool their information in a more targeted manner.

- **Organizational duties of companies:** Article 4, paragraph 2 should be reformulated. In the catch-all rule, organizational and due diligence obligations must be clearly based on the positive knowledge of a critical export. The concept of "due diligence" is confusing and should be omitted. The goal must be that companies can guarantee to halt exports if necessary.

- **Consultations about individual interventions:** If Member States are forced to intervene unilaterally under time pressure, the mandatory consultation of all Member States provided for by Article 4, paragraph 4 must neither impair the ability of the national authorities to respond nor leave companies too long in the dark about whether the export is eligible for authorization. At the same time, the economic players must be offered a legal protection mechanism.

Clarifying Definitions: The New Dual-Use Good

Article 2, paragraphs 1a and 1b and paragraph 21 of the Regulation must precisely define what is to be understood by "dual-use good". Only a clear and meaningful definition can ensure effective export controls. The definition determines the goods-related area of application of the Regulation.

The definition performs two main functions:

- **Legal and planning certainty for companies competing on international markets:** Based on the definition of the dual-use good, companies and national licensing authorities must be able to reliably determine which products require an export authorization. If the authorization requirement cannot be determined from the product listing (Article 3 in combination with the list of items in Annex I, section B), companies and administrative bodies have to rely on the general definition provided in Article 2 (Article 4 in combination with Article 2, paragraphs 1 and 21). In this chain of references, some non-listed goods would, exceptionally, be subject to authorization too. But the definition must be neither too broad nor imprecise. Otherwise, it would take longer to export goods designed for civilian purposes such as for e-mobility or for the protection of utility facilities.

- **Control through the European Parliament and the Council**: The definition of the dual-use good in Article 2, paragraphs 1 and 21 determines which products the European Commission will be able to include in Annex I, section B of the Regulation in the future. Article 16 grants the Commission the right to make additions to the list autonomously. Because the Parliament and the Council cannot exercise comprehensive

control over these new autonomous listings by means of delegated act, the listing possibilities should be limited in advance through the definition.

Clarifying the new definition

The definition of the dual-use good in Article 2 has been expanded to include the term "cyber-surveillance technology" in Article 2, paragraphs 1b and 21. Under this new definition, export controls and product lists will be extended in the future to include security and surveillance technology products. However, the expanded definition corresponds only in part with the political goals of the reform, and damages the global level playing field for companies. It creates obstacles not only for critical exports that increase the threat of internal repression but also for technologies in infrastructures that are environmentally friendly and essential for communication. The EU and its citizens have a strategic interest in being competitive in technologies that are crucial for Industry 4.0 and for the mass consumer market as well as in being able to purchase those products from trustworthy companies. For this reason, both the product group and intended use must be specified. This is also important for the security of supply and consumer protection. For example, in order to guarantee the customer a high level of product safety on the consumer market, manufacturers must ensure that the IT connections through which customers make use of their IT services are secure. Thus a car manufacturer must protect cloud services from unauthorized access by a third party. Driver assistance systems and autonomous driving must be safeguarded against hacker attacks. The same applies for crucial infrastructure; in this area, secure IT connections ensure that the population enjoys security of supply. Surveillance systems reduce the chances of security gaps remaining undiscovered and hacker attacks causing considerable damage.

- **The definition of Article 2, paragraph 1b** establishes that cyber-surveillance technology is subject to export controls if it "can be used for the commission of serious violations of human rights or international humanitarian law or can pose a threat to international security or the essential security interests of the Union and its Member States".

  Because Members of the European Parliament originally wanted to safeguard against certain cases of internal repression in third countries, the definition should now specify the characteristics of such cases: they include the protection of privacy as well as the protection of freedom of expression and the freedom of assembly from/with regard to the use of surveillance technology. Moreover, the area of application should be limited to "systematic and serious" violations of human rights. It is impossible for companies themselves to foresee grave individual cases. For this reason, a definition that offers distinct criteria when a third country is no longer meeting its obligation to protect its citizens and to uphold the rule of law is important. Possible components of such a definition include the absence of court jurisdiction orders in investigative proceedings, the lack of the right to sue and to appeal, and the non-existence of fair trials. If action appears nonetheless necessary in particularly grave individual cases, it must be politically evaluated and flagged.

- **The definition of Article 2, paragraph 21** attempts to specify what comprises the product group "cyber-surveillance technology". However, it falls short of doing so. The illustrative listing of general products such as "mobile telecommunication interception equipment", "intrusion software", "monitoring centers", and "digital forensics" is generic, confusing, and open to interpretation. Moreover, the listing includes technologies that are necessary for the construction, safeguarding, and protection of IT and communication systems. Non-critical applications are also included. These technologies are used in the construction of essential communication facilities and public infrastructure as well as in the protection of companies, public (energy and water) supply facilities, and future traffic management systems from external attacks.

  A limitation of intended end use is achieved by means of a negative delimitation and factual exceptions in Article 2, paragraph 21. As a first step, the factual exceptions in Annex I, section B must be carried over to the definition in Article 2, paragraph 21. According to section B, controls do not apply to security and surveillance technologies that are specially designed for the following purposes*:* billing, data collection func-

tions within network elements (for example, exchange or HLR), quality of service of the network, user satisfaction (quality of experience), and operations at telecommunications companies (service providers). This formulation should be part of the definition in the Regulation and not just that provided in the Annex. Second, other non-critical and desirable intended end uses should be formulated as factual exceptions. These could include, for example, if the technology is specially designed for the protection of public digital infrastructure, the protection of companies from industrial espionage, and the protection of companies and their products from hacker attacks as well as for the use in companies' internal compliance systems for combatting fraud and corruption.

In addition, there must be an honest debate about the fact that not all gathering of data in third countries can be prevented by the EU Dual-Use Regulation. Data collection and the right to informational self-determination as well as the protection of privacy and the freedom of expression must be regulated in third countries – as is the case in the European Union – through data protection laws and the corresponding substantive and procedural criminal legislation. Here EU partner projects can contribute to promoting the development of the legal and judicial systems in third countries. It is important not to overload the EU Dual-Use Regulation.

Industry's Recommendations:

Towards a Better Definition of Security and Surveillance Technologies:

- **Recognize non-critical intended end uses:** Non-critical intended end uses must be exempted from the authorization requirement. The exceptions listed in Annex I, section B of the Regulation should be incorporated as factual exceptions into the definition of the relevant cyber-surveillance product in Article 2, paragraph 21. Moreover, exemptions must also be made for technology that is used for the protection of public infrastructure, the protection of companies from industrial espionage, and the protection of the consumer/customer.

- **Take into account systematic violations of objects of protection:** The legislator must make the definition in Article 2, paragraph 1b more concrete: export controls should apply to exports that increase the danger of internal repression and pose a threat to the freedoms of expression and assembly as well as the protection of privacy, whereby it is crucial to determine whether functioning legal protection mechanisms do or do not exist in principle (court jurisdiction orders in investigative proceedings, the right to sue and to appeal, and fair trials).

Country Lists Provide for Transparency and Effective Control

Embargo measures and country lists provide for clarity and transparency in cases where export trades with sensitive countries are to be prevented. Thus the export controls reform should more closely examine, and take greater account of, the various embargo instruments and the country lists in general export control regulation. For the general dual-use controls, country lists should be drawn up that complement the three control criteria of export product, end-user and end-use as means of control.

Precisely because the reform is intended to ensure protection against cyber- surveillance technology in those countries in which internal repression by state actors is to be feared, strictly positive or negative lists or even grey country lists (so-called unverified lists) would be the appropriate instrument to achieve effective control through companies and authorities. However, the European Commission's *Impact Assessment* makes no mention about either the means of imposing an embargo or restrictions imposed through country lists.

Embargo Policy

Insofar as trade with a country of destination is to be prohibited or limited because that state has violated international law, UN and EU embargos are the correct means of control. The desired restrictions are adopted at the EU level within the framework of the European Council's Common Foreign and Security Policy (CFSP) in a Common Position and subsequently (in most cases) in an EU regulation. The Council's decision is legally binding for the Member States, while the EU regulation is directly and immediately binding for companies as well.

Similarly, the export of products that can be used for internal repression can be limited in a carefully targeted manner through embargo regulations, as shown by the EU regulations on Iran, Libya, Belarus and Myanmar.[11] The so-called Iran human rights regulation (Regulation (EU) No. 359/2011)[12] is a good example of how the export of various cyber- surveillance technology products can be effectively prohibited. That regulation explicitly listed particularly sensitive end-users. They included the so-called Information Minister, who at the time was responsible for censorship and control over the internet. Furthermore, such a regulation can be temporary or lifted depending on the circumstances within the country in question. Thus it allows the European Commission to respond in a flexible manner to changing political circumstances. Given the above examples, it is incomprehensible why the advantages and effectiveness of these measures were not more closely examined in the *Impact Assessment*.

Country Lists

Country lists included in the Annex of the Dual-Use Regulation could be another means of exercising effective control over various export trades. They could be adopted by EU institutions by means of delegated acts. Establishing three different types of country list would allow for a gradual assessment of the level of suspicion. Depending on the available evidence about the allegedly critical situation in a third country and/ or about a specific end user in that country as in the U.S. entity list, the European Commission could propose positive, negative or grey lists. Like the U.S. unverified lists, the grey lists would have the advantage of being able to signal that in a third country, critical surveillance practices were suspected but had by no means been established. The Parliament and Council could stipulate in the proposed Regulation which infringing surveillance practices should be part of the lists. The advantage of this approach is clear: country lists provide companies and authorities with an overview of sensitive countries. Unnecessary safeguard applications would be avoided. Listed states could respond to any suspicions.

Understandably, it is difficult for political institutions to publicly evaluate the behavior of third countries. Among other things, diplomatic relations must always be taken into account. However, strictly speaking, the reform proposal provides for precisely such a political-legal evaluation of third-country trade – only behind closed doors. A value-based trade policy should allow the EU to speak openly about the values it espouses. Moreover, the list approach offers more transparency in the decision-making process.

---

[11] German Federal Office for Economic Affairs and Export Control, *Embargos*, <http://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Embargos/embargos_node.html> (accessed 18 January 2017).
[12] Council Regulation (EU) No. 264/2012 of 23 March 2012 amending Regulation (EU) No. 359/2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran, <http://eur-lex.europa.eu/legal-content/TXT/?uri=CELEX:32012R0264>.

Industry's Recommendations:

- **Negative country lists** could (following the lead of the embargo policy) restrict exports to certain countries if information and evidence held by the 28 intelligence services suggest a high probability of certain critical state surveillance measures and resulting acts of infringement.

- **Grey country and end user´s lists** could (following the lead of the US-unverified lists/entity lists) signal that a majority of the 28 intelligence agencies have increased suspicions about critical surveillance practices and acts of infringement.

- **Positive country lists** could be formulated in the product listings of Annex I, section B as factual exceptions. In the event of an export license reservation, the listed countries are already classified through the product listing as fundamentally safe. This instrument, which has been tried and tested at the national level, is mentioned in the Annex of the reform proposal and must be resolutely pursued.

The criteria for listing countries must be enshrined in the proposed Regulation. In this way, the European Parliament and Council can determine on what basis decisions about critical-case groups are to be made. Criteria analogous to the end-use ones in the products definition are needed for critical surveillance practices.

Industry's Recommendations:

A critical – infringing – surveillance practice, as defined in the Regulation, **exists when**

1. **the following civil rights are neither enshrined nor recognized as civil rights in the Constitution of the third country, its laws, its Supreme Court rulings or its common law:**
    - Protection of privacy/inviolability of the home (protection from wire-tapping)
    - Fundamental right to the confidentiality and integrity of IT systems (the so-called computer fundamental right)
    - Freedom of expression
    - Freedom of assembly;
2. **in cases of typically covert surveillance measures, official surveillance is permitted without a court order for the purpose of risk prevention or criminal prosecution** even though it encroaches on the fundamental rights enumerated in Point 1 above; and
3. **citizens confronted with burdensome measures have insufficient means of legal redress** whereby the official measures can be examined through administrative channels or by the (administrative) courts and, where appropriate, declared invalid (including retroactively).

Quick Stop of Exports Possible Even Without New Catch-All Regulations

The conclusions of the European Commission's *Impact Assessment* suggest that without the new catch-all regulations, EU states are unable to take the necessary action if they want to halt goods exports to sensitive end-users at short notice. This view is based on the assumption that the fast changing technological and political environment needs quick response mechanisms. These concerns are understandable. However, the full range of proven control mechanisms is not sufficiently appreciated: thanks to the successful interplay of EU legislation and national administrative procedure, the ability of the administration to respond is already guaranteed today – even at a time of rapid political and technological change.

- **Export control regulations:** At the statutory level, the most effective means of systematically controlling exports are embargo provisions and the above-mentioned country and product lists of the general EU dual-use export controls. These lists serve as a benchmark for controls at company level as well as through the national licensing and customs authorities.

- **Administrative procedure:** Moreover, effective export controls are guaranteed by the administrative procedure of the national licensing authorities, which are responsible for enforcing export control regulations. Besides decision-making powers in the application process, EU Member States have the authority to intervene beyond that process. They can stop the export of goods outside an application process; if the goods have already reached the border, this can be achieved with the help of the customs authorities. Exports can be stopped if authorization for goods that are subject to authorization has not been granted. By the same token, goods that are not subject to authorization can be stopped. In such a case, the licensing authorities must have grounds to believe that the export of those goods and their delivery to the end-user poses a threat to public security or threatens to violate human rights. The legal basis is provided by national laws – for example, paragraph 6 of the Foreign Trade Law in Germany's *Außenwirtschaftsgesetz* (AWG). But at the same time, Article 8 of the EU Dual-Use Regulation offers the licensing authorities the possibility of preventing delivery.

  Overall, individual intervention is very effective: state (licensing) authorities can follow up on information about human rights violations, compare it with the findings of the intelligence agencies and take those findings into account in deciding whether to halt the export of the goods. By contrast, companies do not have access to the findings of the intelligence agencies.

One shortcoming is that in the *Impact Assessment*, the EU Commission does not examine whether the Member States do, in fact, make use of the authority to intervene. Perhaps all that is lacking is an effective EU-wide implementation of existing regulations. Foreign trade is essentially free and should not unnecessarily be restricted by catch-all regulations, as stressed by EU Trade Commissioner Cecilia Malmström in the reform proposal for the EU anti-torture regulation. In that context the catch-all instruments also had to be weighed against the list approach. At the time, the Trade Commissioner spoke out explicitly against new catch-all regulations.[13]

Industry's Recommendations:

- Ensure Implementation and enforcement of rules: **Before the legislator passes new rules, it should check if Member States make use of their authority to intervene and if an EU-wide implementation and enforcement of existing export control rules is possible.**

[13] European Parliament, *Debates,* See http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20151026&secondRef=ITEM-014&language=EN&ring=A8-2015-0267 (accessed 14 March 2017).

Further Key Elements

Standardize Definitions: The Exporter

With regard to the definition of the exporter, it must be ensured that the same definition of the exporter of goods requiring an export license is used in European customs legislation. This is important because the customs authorities are the oversight bodies that inspect deliveries of goods at the external borders of the European Union to make sure that, among other things, the accompanying paperwork is complete and that authorizations comply with export control legislation. For this reason, the definition of the exporter in Article 2, paragraph 3 in the new Dual-Use Regulation must be harmonized with the definition of the exporter in the Union's Customs Code and its delegated acts.

Industry's Recommendation:

- **Standardize the definition of the exporter:** the definition of the exporter should be harmonized with the definition provided in customs law.

Ensure Competitiveness: Caution Required over EU Unilateral and Autonomous Lists

Article 16, paragraphs 1, 2b, 4, 5 and 8 of the proposed Regulation provides for a new empowerment of the European Commission. Under this provision, the Commission can, by means of delegated act, draw up new product lists in the area of security and surveillance technology. The product lists will then be included in Annex I, section B.

Autonomous listing is a cause for concern because the European Commission can propose product lists unilaterally without having to consult the EU Member States. Currently, the Commission does not have the specialist expertise for new listings in Annex I, section B. Thus, there is a danger that standards will decline. Product lists must be drawn up in a technically flawless and meaningful manner. Before product lists are finalized in international export control regimes, expert panels composed of government representatives of the states belonging to the regimes regularly advise on the classification of technical products, technical descriptions, and risk evaluations. These quality standards should not be allowed to slip at the EU level. The involvement of the Member States in the EU autonomous lists through the Dual-Use Coordination Group provided for in Article 21, paragraph 3 is insufficiently systematic and does not require the specialist knowledge of the Member States to be taken into account. The veto power of the Council, which can be invoked later in the delegated act procedure, is too weak and does not give the Council the right to alter the lists. Company expertise should systematically be taken into account, as well, to resolve technology- and market-related issues.

Moreover, the EU's going it alone without holding consultations at the international level endangers the global level playing field and the competitiveness of European industry. At the same time, it means that the European Commission has less influence over responsible exports to third countries. Thus a product list drawn up unilaterally by the EU should not be preferred over a product list in the international export control regimes and should be used as a measure of last resort. Export control regulations are sustainable only when the same rules apply to all.

Industry's Recommendations:

- **Ensure global competitiveness and responsible exports:** The EU should avoid going it alone. Effective controls can be carried out only in cooperation with partners of the EU in the international export control regimes. The EU should prioritize promoting lists of critical products at the international

level in the existing four export control regimes. If it proves difficult to draw up lists of security and surveillance technologies, the mandate of the regime in question should be enlarged.

- **Involve EU Member States**: Member States should systematically be involved in decisions about EU autonomous listings. If new listings are time-critical, the fast-track procedure can be employed, as is currently the case under the anti-torture regulation.

- **EU must be able not only to draw up autonomous lists but also to make delistings:** Insofar as the EU is able to draw up autonomous lists, it must also be able to make delistings. This is because one of the consequences of the rapid technological transformation is that the critical high-technology goods of today are the mass products of tomorrow. Elaborate export controls are neither effective nor efficient in the case of goods that can be obtained worldwide or are easily manufactured.

Beware of the Extraterritoriality of Rules

The broker and the supplier of technical assistance

The Commission draft envisages trade and brokering restrictions being imposed on companies with registered offices outside the EU if those firms are controlled by an EU company or EU citizen (Article 2, paragraph 7). A similar rule is to be introduced for suppliers of technical assistance (Article 2, paragraph 9). This extraterritoriality is questionable from a political and international-law perspective and almost impossible to administer. State action is conditional on the state having a relation to its own national territory. Traditionally, this requires, as point of reference, an act of a person on the sovereign territory of the state or an act that has an effect on the sovereign territory of the state. A person's nationality can serve as point of reference too. However, the weaker the reference point, the more difficult it is to justify the extraterritorial effect in terms of international law; this is because extraterritoriality assumes that foreign law can apply on the sovereign territory of the third country. Thus the European Parliament and the Council, as legislator on the territory of the EU, must decide whether other (foreign) legislators can be accepted alongside it. If EU institutions grant themselves this right in relation to third countries, they should grant the same right to foreign legislators.

Apart from this issue and the difficulty of resolving it in political-legal terms, it is unclear just what the point of reference of the definitions in Article 2, paragraphs 7 and 9 is. For example, when can "control over a company" be assumed? What majority ownership and blocking minority stake is required for it to apply? What is the impact of the regulation on the investment opportunities abroad for SMEs? And which foreign ICP rules will we in the EU have to accept at our companies in the future? Voluntary ICPs would not raise these difficult issues. The positive incentives for ICPs in the new EU general authorizations for technology transfers to affiliated companies (Annex II, section H, 3 as future EU008) are an effective but less than incisive means.

Industry's Recommendations:

- **No extraterritorial rules:** The EU must not apply double standards: it should not create binding extraterritorial regulations against which it would otherwise defend itself vis-à-vis other countries, such as the United States.

- **Create positive incentives for internal compliance systems:** Through the EU general authorizations for technology transfers to affiliated companies, the EU can reward companies that promote high export control standards worldwide at their subsidiaries.

License Validity: Guarantee Planning Security, Avoid Overloading the Authorities

The European Commissions´ draft provides for cutting the period of validity of export licenses from two to one year. Article 10, paragraph 3 makes such provision for both individual and global export licenses. Industry will lose planning certainty in this way. At the same time, there is a danger of longer processing periods during the application procedure since the volume of applications to be processed by the licensing authorities may double.

The proposed changes are damaging to competition. Suppliers are attractive only when they can keep (supply) commitments to their customers. Should there be any doubt about a company's reliability, customers will favor its competitors. If the validity of export licenses is cut from two to one year, European companies will no longer be able to meet long-term delivery commitments. Moreover, their planning ability in the project business will suffer considerably.

A shorter period of validity is unnecessary: if the political conditions in a third country change and the danger of human rights being violated there suddenly arises, exports can be stopped in any case. Licensing authorities are already able to cancel an export license by means of an annulment or revocation. In Germany, for example, this is in accordance with the provisions of general administrative law (paragraphs 48 and 49 of the Administrative Procedure Act). It is precisely the instrument of revocation that makes it possible to alter an administrative decision to reflect the changed factual and legal situation. In this context, the political-legal environment of a country can play a role, too, insofar as it has to be taken into account in the issuing of the export license.

Industry's Recommendations:

- **Keep the two-year validity period for licenses: The validity of both individual and global export licenses should continue to last over two years.**

EU Guidelines Do Not Establish Legal Certainty

Legal certainty is a cornerstone of the state based on law and the rule of law an essential principle of EU legislation. Compared with the version currently in force, the draft Regulation represents a decline in legal certainty. The new catch-all rules do not satisfy the principle of certainty; crucial definitions are unclear. The Commission is seeking to improve the situation through the development of guidelines[14] and has announced that it wants to develop them "in close consultations with the Member States and stakeholders". While such an approach is to be welcomed, it cannot alleviate the lack of legal certainty because EU guidelines are non-binding and do not have the force of law. Moreover, guidelines can serve to promote differences in implementation among the Member States because some Member States make stricter use of guidelines as a means of orientation than do others. That way, the level playing field within the EU will not be strengthened.

The provisions of the Regulation must permit its secure and efficient implementation even without EU guidelines. At best, guidelines should be understood as constituting a compendium of good administrative practice and should be constantly checked and updated independently of the legislative process.

[14] European Commission, Draft Regulation 2016/0295 (COD), p. 5.

Sources

European Commission (2016), *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.

European Commission (2016), *Commission Staff Working Document: Impact Assessment – Report on the EU Export Control Policy Review*, SWD (2016) 315 final.

Imprint

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
Tel.: +49 30 2028-0

Authors

Dr. Stormy-Annika Mildner
Tel.: +49 30 20 28-1562
S.Mildner@bdi.eu

Verena Kantel
Tel.: +49 30 2028-1518
V.Kantel@bdi.eu

Fabian Wendenburg
Tel.: +49 30 2028-1421
F.Wendenburg@bdi.eu

D 0839