BRIEFING

EU Legislation in Progress

European Parliament

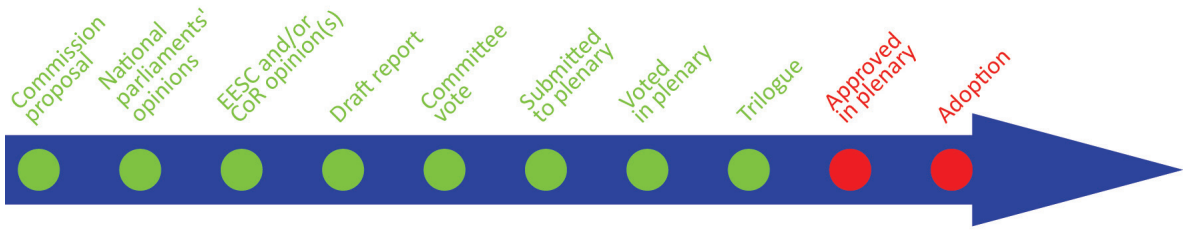
Review of dual-use export controls

OVERVIEW

Certain goods and technologies have legitimate civilian applications but can also be used for military purposes; so-called 'dual-use' goods are subject to the European Union's export control regime. The regime has just been revised, mainly to take account of significant technological developments, increase transparency and create a more level playing field among EU Member States. The proposed regulation will recast the regulation in force since 2009. Among other elements, the proposal explicitly defines cyber-surveillance technology as dual-use technology and introduces human rights violations as an explicit justification for export control. It also includes provisions to control emerging technologies. The proposed regulation introduces greater transparency into dual-use export control by increasing the level of detail Member States will have to provide on exports, licences, licence denials and prohibitions.

On 17 January 2018, based on the INTA committee's report on the legislative proposal, the European Parliament adopted its position for trilogue negotiations. For its part, the Council adopted its negotiating mandate on 5 June 2019, and on the basis of this mandate, the Council Presidency began negotiations with the European Parliament's delegation on 21 October 2019. Trilogue negotiations ended on 9 November 2020, with agreement on a final compromise text. Endorsed by the INTA committee on 30 November, the Parliament is expected to vote in plenary on the text in early 2021.

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).		
Committee responsible:	International Trade (INTA)	COM(2016) 616 28.9.2016
Rapporteur:	Markéta Gregorová (Greens/EFA, Czech Republic)	2016/0295(COD)
Shadow rapporteurs:	Sven Simon (EPP, Germany) Bernd Lange (S&D, Germany) Liesje Schreinemacher (Renew Europe, the Netherlands) Geert Bourgeois (ECR, Belgium) Martina Anderson (GUE/NGL, United Kingdom)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Final first-reading vote in plenary	



EPRS | European Parliamentary Research Service

Author: Beatrix Immenkamp
Members' Research Service

PE 589.832 – January 2021

EN

Introduction

The high-tech nature of dual-use goods and technologies, and the sizeable volume of trade in them, means that the dual-use sector is a very important part of the EU economy. When controlling exports in these goods and technologies, careful attention needs to be paid to striking the right balance between security considerations and imposing unnecessary restrictions on business activities. This close link between security and trade is at the core of dual-use export controls. It also creates particular challenges for implementation within the European Union. On 28 September 2016, the European Commission published a proposal for a regulation setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items ('the proposed regulation') (and its Annexes), to replace Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (Regulation 428/2009), which came into force in 2009.

Parliament, Council and Commission joint statement (2014)

In April 2014, the European Parliament, the Council and the Commission published a joint statement on the review of the dual-use export control regime, which recognised the importance of 'continuously enhancing the effectiveness and coherence of the EU's strategic export controls regime, while ensuring a high level of security and adequate transparency without impeding competitiveness and legitimate trade in dual-use items'. The three institutions considered that modernisation and further convergence of the system were needed in order to keep up with new threats and rapid technological changes, to reduce distortions and to create a genuine common market for dual-use items. The statement recognised that controls were needed on the export of certain information and communication technologies (ICT) that can be used in connection with human rights violations and to undermine the EU's security.

Context

The EU export control system was set up in the 1990s under Regulation (EC) No 3381/94, setting up a Community regime for the control of exports of dual-use goods, and Council Decision 94/942/CFSP, concerning the control of exports of dual-use goods, and was considerably strengthened with the adoption of Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology. Regulation 428/2009 introduced significant improvements to the EU export control regime, in particular in response to the EU strategy against the proliferation of weapons of mass destruction of December 2003 and in light of reports from exporters and industry. Regulation 428/2009 provides for the free circulation of dual-use items – with some exceptions – within the single market and lays down basic principles and common rules for the control of the export, brokering, transit and transfer of dual-use items, in the framework of common commercial policy. It also provides for administrative cooperation and harmonised policies and tools for implementation and enforcement. The regulation is directly applicable to exporters but requires some additional implementing measures by EU Member States under a mixed system under which national competent authorities are responsible for licensing decisions, for instance.

Existing situation

International level

Regulation 428/2009 implements international commitments under United Nations Security Council Resolution (UNSCR) 1540 (2004), international agreements such as the Chemical Weapons Convention (CWC) and the Nuclear Non-Proliferation Treaty (NPT), and multilateral export control regimes such as the Wassenaar Arrangement, the Nuclear Suppliers Group (NSG), the Australia Group and the Missile Technology Control Regime (MTCR).

European level

The impact assessment that was published alongside the proposal on 28 September 2016 noted that the current EU export control system was not fully geared up to keep up with 'today's evolving and new security risks, rapid technological and scientific developments as well as transformations in trade and economic processes'. The current system is described as not taking clearly into consideration the emerging trade in cyber-surveillance technology and the risks it creates for international security and human rights. From an economic perspective, the system is seen as imposing a heavy administrative burden on industry and authorities alike, and as occasionally lacking legal clarity. It is seen as problematic that divergent interpretations and applications among Member States result in asymmetrical implementation and distort competition within the Single Market. The problem is believed to affect a variety of economic operators across numerous industries, including SMEs.

The changes the Commission's proposal would bring

Human rights and cyber-surveillance items

Traditionally, export control seeks to mitigate military risks, especially the proliferation of weapons of mass destruction. The Commission proposal marks a fundamental shift in this respect, as it introduces the protection of human rights as a 'normative justification'[1] for export control. Moreover, the proposal seeks to set new standards for the control of cyber-surveillance items that go beyond existing multilateral controls.[2] In doing so, the Commission responds to calls from the European Parliament and Council to address concerns about the proliferation of cyber-surveillance technologies and software that have in the past been misused in violation of human rights and could threaten the EU's digital infrastructure.

Cyber-surveillance items

First, the Commission proposes to expand the definition of dual-use items to include 'cyber-surveillance technologies'. By explicitly including the term 'cyber-surveillance technology' in the definition of dual-use items, the Commission proposal would bring any such item within the catch-all controls, even if it is not explicitly listed among the items subject to control (Annex I).

Second, the Commission is proposing to create a new EU autonomous list of cyber-surveillance technology subject to export control. Three types of cyber-surveillance technologies – namely mobile telecommunications interception or jamming equipment, intrusion software, and internet protocol (IP) network communications surveillance systems – are already covered by internationally agreed dual-use controls and already appear in Annex IA of the existing regulation. The Commission is proposing to create a new category of controlled items, entitled 'Other items of cyber-surveillance technology', that would comprise two additional items of cyber-surveillance technology, namely monitoring centres and data retention systems or devices. These two types of cyber-surveillance technology are not yet covered by internationally agreed dual-use controls. However, one EU Member State – Germany – has made those two types of surveillance technology subject to export control under national legislation.

Human rights considerations

The EU has a record of invoking human rights as a ground for restricting exports of technologies, including cyber-surveillance technologies. Nevertheless, according to experts, the Commission proposal still marks a significant change, situating considerations of human rights 'not as a marginal consideration, but as one of the key normative grounds for controlling the export of sensitive items'.[3]

The Commission is proposing to expand the catch-all provision and make it obligatory to obtain an authorisation for the export of dual-use items not included in the control list destined 'for use by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination' (Article 4(1)(d)). In October 2012, the European Parliament already proposed a similar catch-all provision, but this was not reflected in the final legislative act adopted at the time.

The obligation to discover whether items are intended for abuse in the manner described above is to be shared by both the competent authorities *and* the exporter. The latter's obligation to conduct 'due diligence' is stated explicitly in the proposal (Article 4(2)).

Moreover, in deciding whether or not to grant an individual or global export authorisation, competent authorities are henceforth to take into account 'respect for human rights in the country of final destination, as well as respect by that country of international humanitarian law (Article 14(1)(b))', 'the internal situation in the country of final destination' (Article 14(1)(c)), 'preservation of regional peace, security and stability' (Article 14(1)(d)), 'considerations of national foreign and security policy, including security of Member States' (Article 14(1)(e)) and 'considerations about intended end use and the risk of diversion' (Article 14(1)(f)).

It should be noted that Article 8 of the current regulation already allows Member States to prohibit or impose an authorisation requirement on the export of non-listed dual use items for reasons of public security or for human rights considerations. It should also be noted in this context that Article 12 of the existing Regulation 428/2009 already requires competent authorities to take into account 'considerations of national foreign and security policy, including those covered by Council Common Position 2008/944/CFSP defining common rules governing control of exports of military technology and equipment. Criterion Two of Council Common Position 2008/944/CFSP requires EU Member States to deny an export licence if the country of final destination fails to respect human rights and international humanitarian law, including if the technology or equipment to be exported might be used for internal repression.

Nevertheless, fears have been voiced that the Commission's proposal to expand the catch-all provision to include human-rights considerations could lead to a greater administrative burden for operators and authorities, at both national and EU level, since a new layer of control is added to the export of such items. This could imply several additional licensing procedures, owing in particular to the lack of experience in implementing these provisions. Critics of the provision also argue that it may also to give rise to distortions of competition at global level, as it cannot be ensured that other key technology suppliers (China, US) would introduce similar controls.[4]

Addition of controls on brokering and technical assistance and harmonisation at EU level

The proposal seeks to amend certain control provisions relating to technology transfer, in order to provide greater clarity with regard to the application of controls on software and technology. In doing so, the Commission is addressing confusion that has arisen in the past over how controls apply when technology is stored and shared via cloud computing, for example. The provision of 'technical assistance' involving a cross-border movement became an EU competence with the entry into force of the Lisbon Treaty. Therefore, the proposal adds a definition for 'technical assistance' and clarifies applicable controls. The proposal also provides clarification on 'brokering' and 'brokering services', by extending the definition of 'broker' to subsidiaries of EU companies located outside the EU, and to 'brokering services' supplied by third-country nationals from within the EU territory. The proposal also extends the application of brokering to non-listed items and military end-uses, and extends their violation to terrorism and human rights violations. Controls on brokering and technical assistance are to apply throughout the EU jurisdiction, thus establishing an EU-wide legal basis for the prosecution of export control violations. EU persons located in third countries will become subject to control, and the proposal introduces anti-circumvention clauses.

Optimisation of the EU licensing architecture

The proposal seeks further harmonisation of the licensing processes with the aim of reducing the administrative burden associated with obtaining export licences. Importantly, the draft regulation proposes to introduce new EU general export authorisations (EUGEA) for encryption, low value shipments and intra-company transmissions of software and technology and for 'other dual-use items' on an ad-hoc, as-needed basis. As a pre-requisite for a more harmonised approach, it attempts to harmonise the definitions of a number of the regulation's key concepts, such as, for instance, those of 'exporter', 'export' and 'broker'. The proposal also introduces a new authorisation for 'large projects', where one licence covers export operations related to one project, e.g. the construction of a nuclear power plant, for the entire duration of the project. The Commission also proposes to further harmonise the validity period of licences and to promote e-licensing systems by Member States. Enhancing the exchange of information on licensing decisions, notably denials, is another important element of the Commission proposal.

Intra-EU transfers

In order to take account of technological and commercial developments, the proposal revises the list of items that are subject to control within the EU. Controls are limited to the most sensitive items, in order to minimise the administrative burden and disruption of EU trade.

Enhanced cooperation on implementation and enforcement

In an effort to improve the exchange of information between national authorities and the Commission, the proposal envisages the introduction of electronic licensing systems that are interconnected through the dual-use electronic system (DUES). The proposal also calls for the setting up of 'technical expert groups', bringing together key industry and government experts to determine the technical parameters for controls. The Commission also proposed to develop guidance to support interagency cooperation between licensing and customs authorities. Most importantly, the Commission proposes to create an Enforcement Coordination Mechanism with a view to establishing direct cooperation and exchange of information between competent licensing and enforcement authorities.

Catch-all controls

Catch-all controls allow for the control of exports of non-listed dual-use items or technologies in certain situations, where there is evidence that they may be misused. The proposal clarifies and harmonises the definition and scope of catch-all controls to ensure their uniform application across the EU (Article 4).

Anti-circumvention clause

The Commission proposes to make it illegal to participate 'knowingly and intentionally' in activities the object or effect is to circumvent the licensing and/or catch-all provisions set out in Articles 4 to 7 of the regulation.

Legislative process

European Parliament

The legislative proposal was submitted to the European Parliament on 6 October 2016. The Committee for International Trade (INTA), which is responsible for the file, appointed Klaus Buchner (Greens/EFA, Germany) as rapporteur on 12 October 2016. The rapporteur published his draft report on 4 April 2017. Following adoption of the report by the INTA committee on 23 November 2017, the Parliament voted in plenary on 17 January 2018 to adopt amendments to the proposal, with an

overwhelming majority in favour of the positions set out in the INTA report. 571 MEPs voted in favour, 29 against, and 29 abstained. Parliament also voted to open interinstitutional negotiations with the Council.

Cyber-surveillance technology

Parliament supports the Commission's proposal to classify certain cyber-surveillance technology as 'dual-use items'. However, Parliament's definition of the kind of cyber-surveillance technology to be covered by the regulation is slightly more comprehensive than that proposed by the Commission (*additions in italics*). The European Parliament's definition comprises 'cyber-surveillance *items including hardware, software and* technology, *which are specially designed to enable the covert intrusion into information and telecommunication systems and/or the monitoring, exfiltrating, collecting and analysing of data and/or incapacitating or damaging the targeted system without the specific, informed and unambiguous authorisation of the owner of the data, and which can be used in connection with the violation of human rights, including the right to privacy, the right to free speech and the freedom of assembly and association, or* which can be used for the commission of serious violations of human rights *law* or international humanitarian law, or can pose a threat to international security or the essential security of the Union and its *Members* (Article 2(1)(1)(b)).

Human rights

Parliament also supports the Commission's proposal to include a 'catch-all' provision that would require an authorisation for the export of dual-use items not included in the control list destined for use in connection with human rights violations (Article 4(1)d)). However, as a compromise, Parliament suggested limiting the human rights catch-all provision to cyber-surveillance items.

The Commission's proposal expanded the list of criteria that competent authorities have to take into account in deciding whether or not to grant an individual or global export authorisation. Parliament proposes to strengthen further the requirement to check the human rights situation in the country of final destination by adding a list of further elements to be taken into account in the licensing decision as assessment criteria (Article 14(1)(ba). These comprise looking at 'the *behaviour of the country of destination with regard to the international community, as regards in particular its attitude to terrorism, the nature of its alliances and respect for international law' (Article 14(1)(da), and looking at 'the compatibility of the exports of the items with regard to the technical and economic capacity of the recipient country*' (Article 14(1)(db).

Guidance

Parliament has called on the Commission to publish a handbook before the entry into force of the new rules, to assist EU businesses with the interpretation of the new rules, especially more guidance for companies on how to go through the process of due-diligence. Parliament is also calling for better acknowledgment of fundamental rights as licensing criteria, notably for cyber-surveillance.

A level playing field

MEPs are also calling for the creation of a level playing field among Member States, by, for example, introducing similar penalties for non-compliance, along with greater transparency of national authorities' export control decisions.

Encryption

MEPs voted to delete encryption technologies from the list of cyber-surveillance products, as they consider these vital for the self-defence of human rights defenders.

Council

The Council adopted its negotiating mandate on 5 July 2019. The Council rejected many of the amendments to the regulation proposed by the Commission and endorsed by Parliament, reflecting a desire for a rather limited update to the existing Dual Use Regulation.

Human rights and cyber surveillance technology

Essentially, the Council mandate sought to remove the substantive provisions relating to cyber-surveillance technology and human rights. Notably, it rejected the idea of an EU-autonomous list for controlling cyber-surveillance technology, and did not want to add any explicit references to human rights (while leaving the implicit human rights catch-all through the reference to the Council Common Position 2008/944/CFSP of 8 December intact).

Cyber-surveillance technology

Council was opposed to the idea of introducing unilateral dual use controls for cyber-surveillance technology at EU level. Currently, Member States can take national measures to introduce such controls, and one EU Member State – Germany – is already controlling the cyber-surveillance items that the Commission has proposed for an EU autonomous control list.

The Council advocated that the EU simply revert to transposing the control lists of international regimes into EU legislation, and forgoing the opportunity to set up EU-wide control for certain additional cyber-surveillance items.

The Council mandate dropped 'cyber-surveillance technology' from the definition of 'dual use items'. By explicitly including the term 'cyber-surveillance technology' in the definition of dual-use items, the Commission proposal would have brought any such item – even if it was not explicitly on the list of dual-use items subject to control – within the catch-all controls (see below). As such, the Council removed 'cyber-surveillance technology' from the list of technologies that the regulation explicitly defines as 'dual-use items' in Article 2(1)(b) of the Commission's proposal. The Council also removed the list of technologies that the Commission proposed to define specifically as 'cyber-surveillance technology' for the purpose of the regulation, namely mobile telecommunications interception equipment; intrusion software; monitoring centres; lawful interception systems and data-retention systems; and digital forensics (Article 2(21)).

Moreover, the Council mandate removed the suggested Category 10 to Annex I ('other items of cyber-surveillance technology') covering surveillance systems, equipment, and components for information and communication technology. The Council thus rejected the proposal to create an EU autonomous list that would have added 'monitoring centres' and 'retention systems' to the list of dual-use items subject to control.

Human rights

The Council mandate also disagrees with adding new categories to expand the catch-all provision contained in Article 4, which applies to non-listed dual use items. The Council removed a 'catch-all' provision that would require an authorisation for the export of dual-use items destined for use in connection with human rights or international law violations (no Article 4(1)d)).

The Council does not agree with the Commission's proposal to expand the list of criteria that competent authorities have to take into account in deciding whether or not to grant an individual or global export authorisation (which are listed in Article 14 of the Commission proposal). Instead, the Council refers to the common rules already governing control of exports of military technology and equipment laid down in Council Common Position 2008/944/CFSP, and proposing an Article 14(2) that requires Member States to take into consideration the implementation by the exporter of an internal compliance programme when assessing an application for a global export authorisation.

Addition of controls on brokering and technical assistance and harmonisation at EU level

The Council mandate would limit the harmonisation of brokering and technical assistance controls to listed-items (Article 7).

Optimisation of the EU licensing architecture

The Council mandate proposes to drop two out of four EUGEAs, namely those for 'low value shipments' and 'other dual use items'. Moreover, the Council mandate proposes to introduce stricter licensing conditions with respect to the EUGEA for encryption. It also reduces the number of permitted countries under the 'intra-company' EUGEA. The Council mandate keeps the concept of a 'large project authorisation' (LPA), but dilutes the definition.

Enhanced cooperation on implementation and enforcement

The Council mandate calls only for voluntary exchange of information on enforcement and implementation (Article 20(2)). Moreover, the Council mandate proposes not to require national authorities to share information with the Commission on the average times for processing applications for authorisations. (Article 10(5)). As regards the Commission's proposal to develop guidance on interagency cooperation, the Council mandate asks for this to remain voluntary (Article 18.5).

Anti-circumvention clause

The Council mandate deletes the anti-circumvention clause that the Commission proposed in a new Article 23.[5]

Trilogue agreement

In October 2019, following the European elections, the INTA committee voted to open negotiations with the Council on the basis of the previous Parliament's position. Following trilogue negotiations, the Council and Parliament negotiators agreed on a compromise text, on 9 November 2020. The Ambassadors of the Member States meeting in Coreper endorsed it on 18 November, and the INTA committee did so on 30 November. Parliament is expected to vote in plenary on adopting the agreed text at first reading early in 2021.

Cyber-surveillance items

The Commission's and Parliament's views on the importance of further limiting the export of cyber-surveillance items prevailed during trilogue negotiations. Parliament and Council agreed to expand the definition of dual-use items to include 'cyber-surveillance items' (Article 2.21). By explicitly including the term 'cyber-surveillance items' in the definition of dual-use items, the proposed regulation brings any such item within the catch-all controls, even if it is not explicitly listed among the items subject to control (which appear in Annex I to the regulation). There is no agreed definition of 'cyber-surveillance items', but experts have in the past defined these 'as lying at the intersection of the information and communications technology (ICT) sector and the surveillance sector. Hence, cyber-surveillance goods, services and technologies are ICTs that are specifically designed, in whole or in part, for surveillance purposes'.

The proposed regulation notes that cyber-surveillance items that are particularly problematic include those that are 'specially designed to enable intrusion or deep packet inspection into information and telecommunications systems in order to conduct covert surveillance of natural persons by monitoring, extracting, collecting or analysing data, including biometrics data, from these systems' (Recital 5). The proposed regulation does not change the list of cyber-surveillance items listed in Annex IA, and does not add any additional items to this list (beyond the regular

update that brings the EU control list into line with the decisions taken within the framework of the international non-proliferation regimes and export control arrangements). The Commission had originally proposed to create a new category of controlled items, entitled 'Other items of cyber-surveillance technology', that would have comprised two additional items of cyber-surveillance technology, namely monitoring centres and data retention systems or devices. The compromise text agreed between the European Parliament and the Council did not retain this proposition.

Human rights considerations

The Commission's and Parliament's views on strengthening human rights considerations also prevailed over the Council's reluctance to do so. As previously stated, the EU has a record of invoking human rights as a ground for controlling the export of technologies, including cyber-surveillance technologies. However, the proposed regulation expands the catch-all provision and makes it obligatory to obtain an authorisation for the export of dual-use items not included in the control list 'if the items in question are or may be intended ... for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law (Article 4(a)(1)). In doing so, the proposed regulation explicitly introduces specific human-rights related end-use controls for non-listed cyber-surveillance items.

The obligation to discover whether items are intended for abuse in the manner described above is to be shared by both the competent authorities *and* the exporter. The latter's obligation to conduct 'due diligence' is stated explicitly in the proposal (Article 4(a)(2)). Accordingly, an exporter's internal compliance programme, intended to verify end-use and end-user, has to include human rights considerations and a risk assessment to that effect.

Introducing a coordination mechanism at EU level for controls of non-listed cyber-surveillance items

Parliament and Council agreed to introduce a formal procedure that Member States can invoke to maintain an EU level playing field in the trade of specific non-listed cyber-surveillance items that give rise to concerns (Article 4(a)(4)-(11). A Member State that identifies and places under control the export of a non-listed cyber-surveillance item can now, under the new mechanism, initiate formal proceedings that aim to make the export of this item subject to licensing requirements across the EU. All other Member States are asked, within a defined time frame, to assess the information and provide their position. If all Member States agree that an authorisation requirement should be imposed for essentially identical transactions, the Commission is to publish in the Official Journal of the European Union information regarding the cyber-surveillance items and, where appropriate, destinations subject to authorisation requirements as notified by the Member States for this purpose. This procedure allows the Member States to create an autonomous list of cyber-surveillance items that are not covered by the international non-proliferation regimes or export control arrangements, with a view to their inclusion in such regimes and arrangements in due course.

Emerging technologies

An issue of increasing importance for dual-use export controls are emerging technologies such as biotechnology, advanced surveillance technologies, position, timing and navigation technology (PNT), additive manufacturing, artificial intelligence and robotics. Competition in technology has become a crucial element of the relationship between powerful international actors. One of the most visible manifestations of this is the rising relevance of technological supremacy in the competition between the USA and China. China's ambition to be a world leader in certain technologies, as laid out in its Made in China 2025 (MIC2025) industrial policy and its civil-military fusion policy, has led to concerns, including about the potential erosion of Western norms governing the use of emerging technologies.

Regulation 428/2009 already granted Member States the right to introduce national legislation to control the export of any non-listed dual-use item for reasons of public security or for human rights considerations. The proposed regulation maintains this possibility, but adds a new legal basis for all other Member States to implement equal controls on the basis of the first Member State's national legislation (Article 8(a) read in combination with Article 8). Referred to as 'a system of transmissible application of national measures', the new mechanism is designed to maintain a level playing field among Member States in an area of technology that is evolving very rapidly. National control lists that control items that do not feature on the EU's control list will be published in the Official Journal of the EU.

Increasing transparency

Parliament and Council agreed to introduce greater transparency as regards the export of dual-use goods, by increasing Member States' reporting obligations (Article 24). Since 2013, the European Commission has compiled an annual report on the implementation of Regulation 428/2009, which it submits to the European Parliament and the Council. The report is public. According to the 2019 report, in 2018, the Regulation primarily applied to the export of about 1 846 dual-use 'items' listed in Annex I (the 'EU Control List) and classified in 10 categories (Figure 1).

The proposed regulation introduces additional reporting requirements, including on authorisations (in particular number and value by types of items and by destinations at EU and Member State levels), denials and prohibitions, as well as on the administration (in particular staffing, compliance and outreach activities, dedicated licensing or classification tools), and on the enforcement of controls (in particular number of infringements and penalties) (Article 24(2)).

Moreover, with regard to cyber-surveillance items, Member States will be required to provide dedicated information per 'item', including on authorisations, in particular the number of applications received by items, the issuing Member State and the destinations concerned by these applications, and on the decisions taken on these applications. By requiring information at the 'items level', the proposed regulation is following the example of the 2019 Anti-Torture Regulation (Regulation (EU) 2019/125 of the European Parliament and of the Council of 16 January 2019 concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment).

Terrorism

Despite initial reservations, Parliament and Council agreed to follow the Commission's proposal to extend the catch-all provision to prohibit or impose an authorisation requirement on the export of dual-use items for reasons of public security, 'including the prevention of acts of terrorism' (Article 8(1)).

Addition of controls on brokering and technical assistance and harmonisation at EU level

Parliament and Council agreed to follow the Commission's proposal to amend certain control provisions relating to technology transfer, to provide greater clarity with regard to the application of controls on software and technology. Confusion arose in the past over how controls apply when technology is stored and shared via cloud computing, for example. Therefore, the proposed regulation adds a definition for 'technical assistance' and clarifies applicable controls (Article 2(8) and Article 7). The proposal also provides clarification on 'brokering' and 'brokering services', by extending the definition of 'broker' to subsidiaries of EU companies located outside the EU, and to 'brokering services' supplied by third-country nationals from within the EU territory. The proposal also extends the application of brokering to non-listed items and military end-uses, and extends their violation to terrorism and human rights violations. Controls on brokering and technical assistance are to apply throughout the EU jurisdiction, thus establishing an EU-wide legal basis for

the prosecution of export control violations. EU persons located in third countries will become subject to control, and the proposal introduces anti-circumvention clauses.

Optimisation of the EU licensing architecture

Parliament and Council agreed to introduce new EU general export authorisations (EUGEA) for 'intra-group exports of software and technology' (Annex II G) and for 'encryption'. As a pre-requisite for a more streamlined approach, the proposed regulation attempts to harmonise the definitions of a number of the regulation's key concepts, such as, for instance, those of 'exporter', 'export' and 'broker'. The proposal also introduces a new individual export authorisation for 'large projects', where one licence covers export operations related to one project, e.g. the construction of a nuclear power plant, for the entire duration of the project. Enhancing the exchange of information on licensing decisions, notably denials and prohibitions, is another important element of the proposed regulation.

Enhanced cooperation on implementation and enforcement

Parliament and Council agreed to the Commission's proposal to introduce electronic licensing systems that are interconnected through the dual-use electronic system (Article 20(5)), to improve the exchange of information between national authorities and, where appropriate, the Commission. They also agreed that the regulation would include provisions for setting up 'technical expert groups', bringing together key industry and government experts to determine the technical parameters for controls. They also retained the Commission proposal to develop guidance to support inter-agency cooperation between licensing and customs authorities. Most importantly, the Commission proposes to create an Enforcement Coordination Mechanism with a view to establishing direct cooperation and exchange of information between competent licensing and enforcement authorities, and the Commission.

Guidelines

Following calls by Parliament for greater assistance for EU businesses with the interpretation of the new rules, Parliament and Council agreed that the proposed regulation would invite competent authorities to issue guidelines for internal compliance programmes (ICPs), to contribute to the level playing field between exporters and to enhance the effective application of controls. These guidelines should take into account the differences in sizes, resources, fields of activity and other features and conditions of exporters and subsidiaries such as intra-group compliance structures and standards, thus helping each exporter to find its own solutions for compliance and competitiveness. Exporters using global export authorisations should implement an ICP unless that is considered unnecessary by the competent authority due to other circumstances it has taken into account when processing the application for a global export authorisation submitted by the exporter.

EP SUPPORTING ANALYSIS

Regulation 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items: Implementation Appraisal, EPRS briefing, Milan Remáč, September 2016.

Initial Appraisal of the Impact Assessment Report on the EU Export Control Policy Review (SWD(2016)315), EPRS briefing, Alina Alexandra Georgescu, January 2017.

Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items. Recast, European Parliament, Legislative Observatory (OEIL).

ENDNOTES

[1] Machiko Kanetake, 'The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches', *Business and Human Rights Journal*, Vol. 4(1), 2019, pp. 155-162.

[2] For a detailed description of the cyber-surveillance sector, see Final Report of the Data and information collection for EU dual-use export control policy review, prepared by SIPRI and ECORYS for the Commission in November 2015.

[3] Machiko Kanetake, 'The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches', *Business and Human Rights Journal*, Vol 4(1), 2019, pp. 155-162.

[4] However, it is worth noting in this context that on 9 October 2019, the US decided to restrict exports of certain cyber-surveillance technologies to a number of specific Chinese companies (as end-users), on human rights grounds. These companies will be barred from buying products from US companies without prior approval from the US administration.

[5] For further details on the Council mandate, see EU Trade Mandate, International Trade Alert, 11 June 2019.
See also: Mark Bromley and Paul Gerharz, Revising the EU Dual-use Regulation: Challenges and opportunities for the trilogue process, 7 October 2019.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Sixth edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.