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 is now being revised, mainly to take account of significant technological developments and to create a more level playing field among EU Member States.

The proposed regulation would recast the regulation in force since 2009. Among other elements, the proposal seeks to introduce an 'autonomous' EU list for cyber-surveillance technology featuring items that are not (yet) subject to multilateral export control. Moreover, the proposal seeks to introduce human rights violations as an explicit justification for export control.

Stakeholders are divided over the incorporation of human rights considerations, with the technology industry particularly concerned that it might lose out to non-European competitors. 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.

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).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapporteur:</td>
<td>Klaus Buchner (Greens/EFA, Germany)</td>
<td>2016/0295(COD)</td>
</tr>
<tr>
<td>Shadow rapporteurs:</td>
<td>Sven Simon (EPP, Germany)</td>
<td>Ordinary legislative procedure (COD)</td>
</tr>
<tr>
<td></td>
<td>Bernd Lange (S&amp;D, Germany)</td>
<td>(Parliament and Council on equal footing – formerly 'co-decision')</td>
</tr>
<tr>
<td></td>
<td>Liesje Schreinemacher (Renew Europe, the Netherlands)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Geert Bourgeois (ECR, Belgium)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Martina Anderson (GUE/NGL, United Kingdom)</td>
<td></td>
</tr>
</tbody>
</table>

Next steps expected: Continuing trilogue discussions
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. The 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 proposal’) (and its Annexes) will 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.

The proposal seeks to modernise export control, taking into consideration four main developments and trends. These include (i) rapid scientific and technological developments (e.g. cloud computing and 3-D printing), massive global data networks that are vulnerable to attacks, and the growing availability of cybertools and information and communication technologies (ICTs) that can be used in violation of human rights; (ii) evolving foreign policy considerations and security risks, including growing challenges relating to the proliferation of weapons of mass destruction (WMD) (e.g. Iran and North Korea) and uncontrolled access to biological and chemical weapons materials in conflict zones (Syria and Libya); (iii) the multiplication of complex cross-border trade flows and intangible technology transfers in globalised supply chains, which has led to increased foreign availability of certain dual-use items and technologies and risks undermining EU export controls while at the same time exacerbating the distortion of competition for EU companies that results from a lack of global control standards; and (iv) the lack of uniform application of export controls at EU Member State level, as well as insufficient information exchange and coordination among Member States.


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.

**Comparative elements**

Germany is the only EU Member State to have introduced controls on the export of surveillance technologies that go beyond the controls at EU level. These controls, put in place in July 2015, mirror the controls on the export of surveillance technologies proposed by the draft regulation. According to amendments to the German Foreign Trade Ordinance (Außenwirtschaftsverordnung) introduced on 8 July 2015, law enforcement monitoring facilities and retention systems or devices have become subject to new mandatory export licence requirements. The measures were introduced to control the export of surveillance technologies to third countries more effectively and to prevent their misuse for internal repression.

By contrast, the United States (US), a participating state in the Wassenaar Arrangement, has not transposed certain elements of the Wassenaar control list pertaining to surveillance technology. In principle, US export control lists correspond directly to the lists maintained by the various multinational export control regimes. However, following strong opposition from industry and the research community in the US, ‘intrusion software’ and ‘Internet protocol (IP) network communications surveillance systems’ – that were added to the Wassenaar control list in 2013 – have not yet been added to the Commerce Control List (CCL), the list that normally includes all the items on the Wassenaar Arrangements Dual-Use List.

**Parliament’s starting position**

A series of statements and resolutions, set out below, give an indication of the position the Parliament has taken in the past on the issue of dual-use export control.
European Parliament resolution of 17 December 2015 on arms export: implementation of Common Position 2008/944/CFSP

In this resolution, Parliament noted that technological developments make it increasingly difficult to ‘distinguish between pure military and pure civilian use’ and called on the Commission to pay particular attention to new technologies of strategic importance, such as ‘Remotely Piloted Aircraft Systems, applied robotics and surveillance technology’. Parliament recalled that the proliferation of certain surveillance and intrusion technologies around the world might not only be detrimental to human rights but might also pose a ‘significant threat to European strategic interests and its digital infrastructure’. In this context, Parliament welcomed the Commission’s initiative to modernise EU dual-use export controls and its intention to submit a new legislative proposal on control of exports of dual-use items and technologies. Parliament noted that the proposal should ‘aim to improve the coherence and transparency of the export control regime and fully take into account the changing nature of security challenges and the speed of technological development, especially with regard to surveillance and intrusion software equipment’.

European Parliament resolution of 8 September 2015 on human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries

In this resolution, Parliament called on the Commission to ‘ensure coherence between the EU’s external actions and its internal policies related to ICTs’. Parliament deplored ‘the fact that some EU-made information and communication technologies and services are sold, and can be used, in third countries by private individuals, businesses and authorities with the specific intent of violating human rights by means of censorship, mass surveillance, jamming, interception and monitoring, and by tracing and tracking citizens and their activities on (mobile) telephone networks and the internet’ and expressed concern ‘that some EU-based companies may provide technologies and services that can enable such human rights violations’. Parliament further deplored ‘the active cooperation of certain European companies, as well as of international companies trading in dual-use technologies, with regimes whose actions violate human rights’. In that context, Parliament called on the Commission to propose effective policies to address ‘potentially harmful exports of ICT products and services to third countries’.

European Parliament resolution of 21 May 2015 on the impact of developments in European defence markets on security and defence capabilities in Europe

With regard to dual-use items, Parliament stressed the importance of ensuring that the control measures applicable to these items did not stand in the way of the free flow of goods and technology within the internal market and of preventing diverging interpretations of EU rules. Parliament called on the Commission to improve the ‘coherence, efficiency, transparency and a recognition of human rights impact’ of existing dual-use export control legislation as a matter of urgency. According to Parliament, the proposal had to reflect ‘the changing nature of security challenges and the speed of technological developments’.

European Parliament resolution of 5 February 2014 on the ratification of the Arms Trade Treaty (ATT)

In this resolution, Parliament called on Member States ‘to pay greater attention to goods which might be used for both civilian and military purposes, such as surveillance technology’. Moreover, Parliament suggested ‘exploring the possibility of extending the scope of the ATT to include arms exports-related services and dual-use goods and technology’.
Council starting position

In November 2014, the Council noted in its Conclusions on the review of export control policy that Member States face a substantial question on how to maintain or enhance the level of control while striking a balance between security and legitimate trade. The Council recognised that the EU export control system had to have a strong capacity to respond to potential threats arising from proliferation risks.

The changes the proposal would bring

Human rights and cyber-surveillance technology

Traditionally, export control seeks to mitigate military risks, especially the proliferation of weapons of mass destruction. The Commission's proposal marks a fundamental shift in this respect, as it seeks to introduce human rights as a 'normative justification' for imposing export control. Moreover, the proposal seeks to set new standards for the control of cyber-surveillance technology that go beyond existing multilateral controls. In doing so, the Commission is responding to calls from the European Parliament and Council to address concerns about the proliferation of cyber-surveillance technologies that could be misused in violation of human rights and could threaten the EU’s digital infrastructure.

Cyber-surveillance technology

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 controlling the export of technologies, including cyber-surveillance technologies. Nevertheless, according to exports, the Commission's 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’.

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

Terrorism
The Commission is also proposing to extend the catch-all provision to include items 'for use in connection with acts of terrorism' (Article 4(1)(e)).

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 licenses 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).

Terrorism

Parliament did not follow the Commission’s proposal to extend this catch-all provision to include items ‘for use in connection with acts of terrorism’ (Article 4(1)(e)).

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.
Cooperation with third countries
Parliament also asked for better cooperation with third countries.

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 rejects 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 seeks to remove the substantive provisions relating to cyber-surveillance technology and human rights. Notably, it rejects the idea of an EU-autonomous list for controlling cyber-surveillance technology, and does 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
The Council is 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.

By removing this provision, the Council is advocating that the EU simply revert to transposing the control lists of international regimes into EU legislation, and forgoing the opportunity to set-up an EU-wide control for certain additional cyber-surveillance items.

The Council mandate drops ‘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, Council removes ‘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. Council has also removed the list of technologies that the Commission proposes 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 removes 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 rejects 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. 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)).
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, 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.

Terrorism
Council also disagrees with the Commission's proposal to extend the catch-all provision to include items 'for use in connection with acts of terrorism' (no Article 4(1)(e)), as did Parliament.

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
EP SUPPORTING ANALYSIS


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

ENDNOTES


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.


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.