IV. Developments in the European Union's dual-use and arms trade controls

MARK BROMLEY, KOLJA BROCKMANN AND GIOVANNA MALETTA

The European Union (EU) is currently the only regional organization with a common legal framework for controls on the export, brokering, transit and trans-shipment of dual-use items and also, to a certain extent, military items. The key elements of this legal framework are the EU's arms embargoes, dual-use regulation, common position on arms exports, directive on intra-Community transfers, and anti-torture regulation.[1] Developments in EU arms embargoes are addressed in section II of this chapter. This section focuses on developments with regard to the dual-use regulation and the common position. During 2020 the EU reached a provisional agreement on the text of a new version of the dual-use regulation, thereby drawing to a close a long-running process of review and recast that began in 2011. Following a review of the common position that concluded in 2019, the EU also implemented measures to improve the level of transparency and accessibility of the EU annual report on arms exports.

The EU dual-use regulation

The EU dual-use regulation covers controls on the export, re-export, brokering and transit of dual-use goods, software and technology. The regulation is directly applicable law in EU member states but is implemented and enforced via their national control systems. As mandated in Article 25 of the dual-use regulation, the instrument has been under review since 2011. As part of this process, the European Commission published a 'recast' proposal in the form of a new draft version of the regulation in September 2016.[2] The European Parliament published its proposed amendments to the Commission proposal in January 2018 and the Council of the EU published

---

[1] Council Regulation 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, *Official Journal of the European Union*, L134, 29 May 2009; Council Common Position 2008/944/CFSP of 8 Dec. 2008 defining common rules governing control of exports of military technology and equipment, *Official Journal of the European Union*, L335, 8 Dec. 2008; Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community, *Official Journal of the European Union,* L146, 10 June 2009; and Regulation (EU) 2016/2134 of the European Parliament and of the Council of 23 Nov. 2016 amending Council Regulation (EC) 1236/2005 concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment, *Official Journal of the European Union*, L338, 13 Dec. 2016.

[2] European Commission, '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)', 12798/16, 28 Sep. 2016. See also Bauer, S. and Bromley, M., 'Developments in EU dual-use and arms trade controls', *SIPRI Yearbook 2017*, 612–15.

its own negotiating mandate in June 2019.[3] In the second half of 2019 the Commission's proposal began to go through a process of 'trilogue' involving the Commission, the Parliament and the Council. Four trilogues were held between October 2019 and September 2020. In November 2020 the Council of the EU—under the presidency of Germany—announced that the Council and the Parliament had reached a provisional political agreement on a revised version of the dual-use regulation in the form of a final compromise text.[4] The new version of the dual-use regulation is expected to be adopted by the Parliament in the first half of 2021 and enter into force in the second half of 2021.[5] The proposal put forward by the Commission sought to revise virtually all aspects of the dual-use regulation, setting the stage for a complex and wide-ranging recast process. However, the length of time needed to adopt a final compromise text was largely due to differences that emerged on certain key points. The most contentious of these was the creation of stronger controls on exports of cybersurveillance items by—among other things— expanding the range and prominence of human rights concerns in the dual-use regulation. Here, the Parliament largely endorsed or expanded on the Commission's proposals. However, member states were initially divided on how to respond and later—through the Council's mandate—pushed back on the Commission and Parliament's proposals.[6]

This section reviews the areas that proved most substantive in terms of the amount of debate generated or the significance of changes made to the dual-use regulation: harmonizing member states' controls; simplifying controls on less sensitive items; and strengthening controls on cybersurveillance items. The section then addresses a fourth area which became increasingly prominent as the review and recast progressed: responding to challenges posed by 'emerging technologies'; and discusses the other initiatives the EU

---

[3] European Parliament, 'Amendments adopted by the European Parliament on 17 January 2018 on the 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)0616–C8–0393/2016–2016/0295(COD))', 17 Jan. 2018; and Council of the European Union, 'Proposal for a for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)—Mandate for negotiations with the European Parliament (2016/0295(COD))', 5 June 2019.

[4] European Council, 'New rules on trade of dual-use items agreed', Press release, 9 Nov. 2020.

[5] Angersbach, R., 'Stand der EG-Dual-Use-Novelle' [Status of the EU Dual-use Recast], *AW-Prax*, vol. 27, no. 1 (Jan. 2021), pp. 13–16.

[6] Moßbrucker, D., 'Surveillance exports: How EU Member States are compromising new human rights standards', Netzpolitik, 29 Oct. 2018; and Cerulus, L., 'Europe to crack down on surveillance software exports', Politico, 15 Oct. 2020. For a more detailed overview of the Commission's, Parliament's and Council's positions during the review and recast process see Bromley, M. and Maletta G., 'Developments in the European Union's dual-use and arms trade controls', *SIPRI Yearbook 2019*, 532–37; Bromley, M. and Gerharz, P., 'Revising the EU Dual-use Regulation: Challenges and opportunities for the trilogue process', SIPRI Commentary, 7 Oct. 2019; and Immenkamp, B., 'Review of dual-use export controls', European Parliamentary Research Service briefing, 15 Jan. 2021.

engaged in with relation to this area, over and above making changes to the dual-use regulation.

Harmonizing member states' controls

In April 2014 the Commission outlined four priorities for the review of the dual-use regulation. Two of these were focused on creating greater harmonization in the way member states implement dual-use export controls: promoting 'export control convergence and a global level-playing field', and supporting 'effective and consistent export control implementation and enforcement'.[7] During the review and recast, attempts to achieve a more harmonized application of the regulation focused on three key areas: achieving a more uniform interpretation of key concepts; improving intergovernmental information-sharing; and creating new mechanisms in the field of public transparency.

Both the multilateral export control regimes and the dual-use regulation provide limited clarity about how certain key terms associated with dual-use export controls should be interpreted. Areas where there is a lack of common understanding include how the exemptions for 'basic scientific research' and information that is 'in the public domain' should be implemented. This, in turn, contributes to differences in how controls are applied at the national level.[8] The final compromise text makes clear that guidelines are needed and that their development is a joint responsibility of the Council and the Commission.[9] In parallel with the review process, the EU and its member states have taken other steps aimed at promoting a more harmonized implementation of the dual-use regulation, including by publishing guidelines on how to set up and implement internal compliance programmes and developing an additional set of compliance guidelines for the research sector.[10] The final compromise text also seeks to standardize the way in which transfers of knowledge and 'technical assistance' are regulated. In particular, it creates controls on transfers that occur within the national borders of EU member states, such as may happen when a foreign

---

[7] European Commission, 'Ensuring security and competitiveness in a changing world', Communication from the Commission to the Council and the European Parliament on the review of export control policy, COM (2014) 244 final, 24 Apr. 2014.

[8] E.g. Germany and the Belgian region of Flanders recently published guidance material detailing how the exceptions for 'basic scientific research' should be applied, which points to differing views in this area. Flemish Chancellery and Foreign Office, 'Controle op de Handel in Dual-use Items' [Control of trade in dual-use items], 30 Sep. 2017; and German Federal Office for Economic Affairs and Export Control (BAFA), *Export Control and Academia Manual* (BAFA: Eschborn, Feb. 2019).

[9] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)', 12798/20, 13 Nov. 2020, p. 47.

[10] Commission Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009, *Official Journal of the European Union*, L205, 5 Aug. 2019; and European Commission, 'EU compliance guidance for research involving dual-use items', Nov. 2020.

citizen enters the EU to attend a university course or participate in industry training, something not covered by the dual-use regulation. However, providing guidance material for how these controls should be applied is the responsibility of member states.[11]

Under the dual-use regulation, member states exchange information on denials of export licences and meet regularly to discuss the implementation of the regulation. However, information exchanges in other areas—particularly on measures taken to enforce controls at the national level and to prosecute violations of export controls—are more limited. The final compromise text makes significant changes in this area, particularly with regard to enforcement issues. Specifically, the Dual-Use Coordination Group—which is chaired by the Commission and brings together officials from EU member states to discuss the application of the dual-use regulation—is tasked with establishing an 'Enforcement Coordination Mechanism'. The new body will bring together member states' licensing authorities and enforcement agencies to exchange information on a range of areas, including 'risk-based audits' and 'the detection and prosecution of unauthorised exports of dual use items'.[12]

In contrast to the common position, the dual-use regulation does not include any requirements for public reporting on issued or denied export licences. Both the Commission and Parliament called for significant advances to be made on this front, while the Council made no reference to the issue in their negotiating mandate. The final compromise text creates an ambitious set of targets on public reporting. Specifically, the annual report which the Commission produces on the implementation of the dual-use regulation will be expanded to include information on export licence 'authorisations', 'denials' and 'prohibitions'. The commitments are most far-reaching for cybersurveillance items. Here, the EU commits itself to publishing annual data on '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'.[13] The final compromise text does not specify which data will be collected and published, or when the first report will be produced, but instead tasks the Commission and Council with developing 'guidelines' to address these points.[14] It also notes that member states are obliged to give 'due consideration . . . to legal requirements concerning the protection of personal information, commercial sensitive information or protected defense, foreign policy or national security information' when collecting and submitting data.[15]

---

[11] Council of the European Union, 12798/20 (note 9), p. 47, Article 24(1).
[12] Council of the European Union, 12798/20 (note 9), pp. 46–47, Article 22(2).
[13] Council of the European Union, 12798/20 (note 9), p. 48, Article 24(2).
[14] Council of the European Union, 12798/20 (note 9), p. 48, Article 24(2).
[15] Council of the European Union, 12798/20 (note 9), p. 48, Article 24(3).

Simplifying controls on less sensitive items

The third priority outlined in the April 2014 Commission Communication was to 'develop an effective and competitive EU export control regime'. Many of the Commission's proposals were focused on modernizing EU controls to reduce the regulatory burden they place on both exporters and member states' licensing authorities. Two of the key areas of focus that emerged during the review and recast process were creating additional EU General Export Authorizations (EUGEAs) and facilitating the use of cloud computing services by exporters of dual-use items.[16]

An EUGEA is a type of open licence agreed at the EU level that allows exporters to carry out multiple shipments under a single licence. The dual-use regulation has six EUGEAs and the final compromise text adds two more: one for items that employ cryptography and one for transfers of software and technology to subsidiary and sister companies. The Commission and Parliament had proposed more language on EUGEAs and the Parliament had gone further, particularly on cryptography where it called for a complete lifting of all restrictions.[17] EU member states supported the adoption of new EUGEAs but differed on their precise scope and content due to their particular national economic and security concerns.[18] There was also broad opposition among member states to the Parliament's idea of dropping controls on cryptography completely. Many governments value the controls for their ability to provide oversight of the trade in technologies that are of potential relevance to national security.[19] The coverage of the two new EUGEAs was less ambitious than the Commission and Parliament had proposed and two other EUGEAs—for low-value shipments and 'other dual-use items'—were dropped completely. However, the Commission also received wider powers to amend the coverage of EUGEAs.

For several years, companies and research institutes have pointed to differences in the ways in which EU member states regulate the use of cloud computing services to store and share technical data or software that is subject to dual-use export controls. These differences centre on whether controls take account of the location of the servers where the software or

---

[16] Cloud computing emerged in the early 2000s and can be broadly defined as 'the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.' Dryfhout, M. and Hewer, S., 'What is cloud computing?', Scout Technology Guides blog, 11 Apr. 2019. For a discussion of cloud computing and export controls see Tauwhare, R., 'Cloud computing, export controls and sanctions', *Journal of Internet Law*, vol. 19, no. 2 (Aug. 2015).

[17] European Parliament, 'Amendments' (note 3), amendments 13 and 15.

[18] Göstl, C., Foreign Trade Administration, Federal Ministry for Digital and Economic Affairs, Austrian Presidency of the Council of the European Union, 'Opening remarks', EU Export Control Forum 2018, Brussels, 13 Dec. 2018.

[19] Bromley, M., Brockmann, K. and Maletta, G., 'Controls on intangible transfers of technology and additive manufacturing', *SIPRI Yearbook 2018*, pp. 437–47.

technology is stored and the steps companies are required to take in order to ensure that technical data or software uploaded to a cloud is kept secure.[20] The final compromise text recommends that member states use 'facilitations in the form of general or global licenses or harmonised interpretation of provisions' for cloud services but leaves the overarching definition of an export intact. This means that member states will remain free to regulate the use of cloud computing according to their own national standards.[21] The Commission had sought to go further by amending the definition of export in a way that would have made clearer that the act of uploading controlled software or technical data to a cloud did not require a licence.[22]

Strengthening controls on cybersurveillance items

The fourth priority provided in the April 2014 Communication was to 'adjust to the evolving security environment and enhance the EU contribution to international security'. Following pressure from the Parliament, the Commission, Council and Parliament committed in 2014 to exploring how to use the dual-use regulation to create stronger controls on the export of cybersurveillance items.[23] Debates about how to achieve this outcome focused on three areas: controlling additional cybersurveillance items through a new 'catch-all control'; controlling additional items through a new 'autonomous' EU control list; and ensuring that fewer exports take place by expanding the range of human rights concerns states would need to consider in their risk assessments.

The list of items subject to licensing requirements under the dual-use regulation is outlined in the EU dual-use list, which is drawn from the control lists produced by the Wassenaar Arrangement and other multilateral export control regimes (see section III). The dual-use regulation also includes so-called catch-all controls, which cover items that do not appear on the dual-use list but that may contribute to a programme to develop weapons of mass destruction, have a 'military end use' in an embargoed state, or be used as parts and components in an illegally exported military item. The final compromise text creates a new catch-all control for unlisted cybersurveillance items that may be used for 'internal repression and/or the commission of serious violations of international human rights and international humanitarian law [IHL]'.[24] Exporters are also obliged to inform

---

[20] See Bromley, M. and Maletta, G., *The Challenge of Software and Technology Transfers to Non-proliferation Efforts: Implementing and Complying with Export Controls* (SIPRI: Stockholm, Apr. 2018), pp. 23–24.

[21] Council of the European Union, 12798/20 (note 9), para. 7.

[22] European Commission, 12798/16 (note 2), p. 7.

[23] See Immenkamp (note 6); and 'Joint Statement by the European Parliament, the Council and the Commission on the review of the dual-use export control system', *Official Journal of the European Union*, L173, 12 June 2014.

[24] Council of the European Union, 12798/20 (note 9), p. 23, Article 4a(1).

their national authorities if they are 'aware according to [their] due diligence findings' of any such risks.[25] The creation of a new catch-all control for cybersurveillance items and language on due diligence were supported by the Commission and Parliament but opposed by the Council on the grounds that they risked creating unclear and unnecessary regulatory obligations for governments and exporters.[26] While their inclusion represents a concession by the Council, the final compromise text defines cybersurveillance items more narrowly than the Commission or Parliament proposed—thereby limiting the scope of the catch-all control—and does not create an explicit legal obligation for companies to have due diligence measures.

Between 2012 and 2019 controls on five types of cybersurveillance items were added to the Wassenaar Arrangement dual-use list and—subsequently—the EU dual-use list.[27] However, both the Commission and Parliament saw a need to create an 'autonomous' EU control list for additional cybersurveillance items that did not appear on the Wassenaar Arrangement list. EU member states were initially divided over whether to support the creation of an autonomous EU list but neither the Council's negotiating mandate nor the final compromise text makes any reference to the issue.[28] Instead, the final compromise text states that if an EU member state uses the new catch-all control to regulate an unlisted cybersurveillance item—and if all other EU member states provide their approval—the EU will publish details 'in the C series of the *Official Journal of the European Union*'.[29] EU member states are also required to 'consider' supporting the addition of these items to the 'appropriate' control regime.[30]

The dual-use regulation requires member states 'to take into account' the considerations outlined in the common position when granting an export licence for dual-use items including—by extension—the common position's eight risk assessment criteria. This means that states are obliged to deny an export licence for dual-use items if they 'might be used for internal

[25] Council of the European Union, 12798/20 (note 9), p. 23, Article 4a(2).

[26] See Council of the European Union, General Secretariat, 'EU export control: Recast of the Regulation 428/2009', Working paper WK 1019/2018 INIT, 29 Jan. 2018; and Council of the European Union, 'Paper for discussion: For adoption of an improved EU Export Control Regulation 428/2009 and for cyber-surveillance controls promoting human rights and international humanitarian law', Working paper WK5755/2018 INIT, 15 May 2018.

[27] Controls on 'Mobile telecommunications interception equipment' were added in 2012; controls on 'Internet protocol (IP) network surveillance systems' and 'Intrusion software' were added in 2013; and controls on 'Monitoring centres' and 'Digital forensics' were added in 2019. For more information see Bromley, M., *Export Controls, Human Security and Cyber-surveillance Technology: Examining the Proposed Changes to the EU Dual-use Regulation* (SIPRI: Stockholm, Dec. 2017); and Brockmann, K., 'The multilateral export control regimes', *SIPRI Yearbook 2020*, p. 556.

[28] See Council of the European Union, General Secretariat, WK 1019/2018 INIT (note 26); and Council of the European Union, WK5755/2018 INIT (note 26).

[29] Council of the European Union, 12798/20 (note 9), p. 24, Article 4a(6).

[30] Council of the European Union, 12798/20 (note 9), p. 24, Article 4a(10).

repression' or 'in the commission of serious violations of [IHL]'.[31] The European Parliament's amendments sought to expand the range of human rights concerns covered by the dual-use regulation beyond those covered by 'internal repression'. Specifically, member states and exporters would be obliged to assess the risk of violations of 'the right to privacy, the right to free speech and the freedom of assembly and association' when deciding whether to export cybersurveillance items. The Commission and the Parliament also called for guidance material to inform member states' export licence decision making. The Council's mandate and the final compromise text keep the link with the common position but take out all references to wider human rights concerns and guidance material. However, new language on 'internal repression', 'serious violations of human rights' and IHL have been added to the preamble, noting that these are issues that EU member states should consider when exporting dual-use items—particularly cybersurveillance items.[32] Moreover, the requirements on exports of cybersurveillance items in the section on reporting should provide greater intergovernmental, parliamentary and public oversight of member states' export licensing decision making in this area.

Responding to challenges posed by 'emerging technologies'

One of the central challenges that the review process sought to address was managing and responding to the challenges posed by rapidly developing and spreading dual-use technologies—so-called emerging technologies.[33] The issues mainly in focus in the early stages of the review process related to the increasing foreign availability of strategic technologies reducing the effectiveness of export controls.[34] However, the subsequent focus has expanded to include the increased usage of certain emerging technologies such as cloud computing, additive manufacturing (3D printing) and nanotechnology. The review process also sought to address the difficulties posed by the highly technical discussions on emerging technologies—often lacking technical standards—in the multilateral export control regimes and how some of these technologies could transform the ways in which transfers

---

[31] 'Internal repression', in turn, is defined as including 'inter alia, torture and other cruel, inhuman and degrading treatment or punishment, summary or arbitrary executions, disappearances, arbitrary detentions and other major violations of human rights and fundamental freedoms as set out in relevant international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights'. Council of the European Union, Common Position 2008/944/CFSP of 8 Dec. 2008 (note 1).

[32] Council of the European Union, 12798/20 (note 9), p. 4, para. 1a.

[33] European Commission, 'The dual-use export control system of the European Union: Ensuring security and competitiveness in a changing world', Green Paper, COM (2011) 393 final, 30 June 2011; and European Commission, 'Ensuring security and competitiveness in a changing world', Communication from the Commission to the Council and the European Parliament on the review of export control policy, COM (2014) 244 final, 24 Apr. 2014.

[34] European Commission, COM (2011) 393 final (note 33).

of controlled items occur.[35] As the recast process continued, the Commission and an increasing number of EU member states began to pay greater attention to the challenges of creating and agreeing on timely controls on transfers of certain emerging technologies that were not currently or only partially captured by the regimes' control lists. In doing so, the EU further expanded the issues it sought to address in relation to emerging technologies and also responded to steps taken by the United States to create new national controls on exports of emerging technologies. In particular, an advance notice of proposed rule-making issued by the US Department of Commerce in 2018—including a list of emerging technology categories—and increasing discussions on competition with China over the leadership in strategic technologies, spurred the international and European debate on this issue.[36] In this context, the Commission came to view the introduction of an EU autonomous control list—which was initially only considered in the context of cybersurveillance items (see previous subsection)—as a means of also allowing the EU to respond more quickly to risks posed by emerging technologies.

The Council strongly rejected the introduction of an autonomous control list but saw the value of creating an EU export control mechanism to address emerging technologies, particularly in cases where the regimes have yet to reach agreement on new measures, including because of the constraints of the consensus rule.[37] The final compromise text acknowledges the need for coordination mechanisms for the EU to use when 'new risks associated with emerging technologies' are identified.[38] However, it noted that any such controls 'should be followed by initiatives to introduce equivalent controls at the multilateral level', which highlights the primary role of the export control regimes in addressing emerging technologies.[39] The final compromise text introduces transmissible controls whereby one member state can use a national control list entry created by another member state under Article 8 to impose an authorization requirement on a particular transfer.[40] The Commission will compile and publish such national control list entries in a watch list to make them available to all member states. A licensing requirement, however, is not triggered automatically but only if the member state assesses that the items 'are or may be intended . . . for uses of concern with respect to public security, including the prevention of acts of terrorism, or to human rights considerations' and has informed the

---

[35] European Commission, COM (2014) 244 final (note 33).

[36] US Department of Commerce, Bureau of Industry and Security, 'Advance notice of proposed rulemaking: Review of controls for certain emerging technologies', *Federal Register*, vol. 83, no. 223 (19 Nov. 2018).

[37] See recital 6 in Council of the European Union, 5 June 2019 (note 3).

[38] Council of the European Union, 12798/20 (note 9), p. 6, para. 6.

[39] Council of the European Union, 12798/20 (note 9), p. 6, para. 6.

[40] Council of the European Union, 12798/20 (note 9), p. 28.

exporter.[41] While Article 8a is structured similarly to a catch-all control, it notably omits any requirement for exporters to inform national authorities if they have knowledge of a specific end use of concern.

Separately, the EU organized a series of technical workshops on emerging technologies for interested member states, led by the Commission and Germany, which took place between November 2019 and December 2020. The series included workshops on additive manufacturing, quantum computing, semiconductors, biotechnologies, brain–computer interfaces and advanced materials, and a virtual workshop on artificial intelligence. The workshop series resulted in a non-public technical report shared among all member states. Notably, the workshops were limited to member states' delegations and did not include public consultations with experts and stakeholders from science, industry or civil society. While an expansion of the workshops to include public consultation elements was considered, after the outbreak of the Covid-19 pandemic the workshop series was initially put on hold and then concluded with virtual workshops which remained exclusive to the member states.

These measures reflect the EU's continued focus on working through the multilateral export control regimes, rather than replacing regime functions. The EU pursued the creation of forums where member states could obtain the latest information and coordinate views on emerging technologies, which they could then bring to the regimes. At the same time the EU acknowledged the possible need for timely unilateral actions by a member state and enabled other member states to easily uphold and replicate such national controls.

The EU common position on arms exports

In September 2019, almost two years after the initiation of the process, the EU member states completed the second review of the common position.[42] The review resulted in a limited number of amendments to the text of the common position and substantive changes to its accompanying user's guide.[43] Some adjustments sought to increase the level of transparency in EU member states' arms exports. In particular, the text of the common position was amended to include a firm deadline for member states' reporting, with a

---

[41] Council of the European Union, 12798/20 (note 9), pp. 28–29, Article 8a.

[42] Council of the European Union, 'Control of arms export: Council adopts conclusions, new decision updating the EU's common rules and a revised user's guide', Press release, 16 Sep. 2019.

[43] For an overview of the outcome of the second review process of the EU Common Position see Bromley, M. and Maletta, G., 'Developments in the European Union's dual-use and arms trade controls', *SIPRI Yearbook 2020*, pp. 561–64.

view to limiting the delay in the publication of the EU annual report on Arms exports.[44]

In addition, to increase the accessibility of the annual report—traditionally presented in a several hundred pages-long PDF file—the Council of the EU decided to transform it into a 'searchable online database'.[45] In October 2020, the European External Action Service (EEAS) implemented this decision by launching the Council Working Party on Conventional Arms Exports (COARM) online database.[46] The database does not replace the publication of the annual report or increase the level of detail in the data provided.[47] However, the database allows the data to be easily sorted and aggregated by the categories of the EU military list, the country of export and destination, and year; it also provides a clearer visual representation of the data by means of interactive graphs, charts and maps.[48] As of January 2021 data is available for 2013–19. However, the comprehensiveness and comparability of the information included in both the annual report and database remain limited due to the fact that EU member states use different methodologies to collect and submit data, while several are not able to submit any data on actual exports.[49] In this regard, the Council also tasked COARM with improving the quality of the annual report, including by supporting and encouraging states' efforts to submit information on their actual exports.[50]

The Council also tasked COARM with considering measures to harmonize 'end-user certificates for the export of small arms and light weapons and their ammunition' at the EU level.[51] The issue was discussed in COARM in 2020 and EU member states are reportedly close to agreeing a Council Decision providing common minimum elements for these certificates, but no decision had been taken by the end of the year.

---

[44] Council of the European Union, 'Consolidated text: Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment', 17 Sep. 2019.

[45] Council of the European Union, 'Council conclusions on the review of Council Common Position 2008/944/CFSP of 8 Dec. 2008 on the control of arms exports', 12195/19, 16 Sep. 2019, p. 4, para. 7.

[46] European External Action Service (EEAS), 'Arms exports control: Launch of online database increasing transparency on EU arms exports', Press release, 26 Oct. 2020; and EEAS, 'Arms export control', 26 Oct. 2020. COARM handles work concerning export controls for conventional arms.

[47] The EU annual report covers (*a*) the number of export licences issued and their value; (*b*) the value of arms exports (where available); and (*c*) the number of denials and the criteria of the EU Common Position invoked in their support.

[48] COARM Online Database, 'Introduction and guidelines', COARM Public v2.0, 16 Dec. 2020.

[49] European Parliament, 'Arms export: Implementation of Common Position 2008/944/CFSP', P9_TA(2020)0224, 17 Sep. 2020, p. 6; Cops, D., 'Past and future of the review of the EU Common Position on arms exports', Flemish Peace Institute, [n.d.]; and Stewart, I. J. et al., *Recommendations for a Transparent and Detailed Reporting System on Arms Exports within the EU and to Third Countries* (Policy Department, Directorate-General for External Policies, European Parliament: Brussels, May 2020), pp. 13–14.

[50] Council of the European Union, 12195/19 (note 45), p. 4, para. 9.

[51] Council of the European Union, 12195/19 (note 45), p. 5, para. 13.

Conclusions

Reaching an agreed final text of a new version of the dual-use regulation was by no means a foregone conclusion and was only possible to the extent that the Commission, Parliament and Council were willing to make concessions in key areas. The outcome ensures that, in most key respects, the dual-use regulation remains tied to the coverage of the multilateral export control regimes and that all decision making on export licences stays at the national level, both of which were key priorities for EU member states. However, significant changes have been made to the dual-use regulation and many adjustments that the Commission or Parliament proposed—and which member states did not initially support—have been implemented, not least in the field of public transparency. In particular, member states have agreed to an ambitious set of reporting practices that could make detailed information about their exports of dual-use items publicly accessible. This is a significant step given the limited transparency in this area that currently exists among most member states. Developments in the common position show that, in the field of arms export controls, making improvements to public transparency is also the area where the EU and its member states seem able to make the most significant advances.