BRILL
NIJHOFF

SECURITY AND HUMAN RIGHTS (2021) 1-10

SECURITY AND
HUMAN RIGHTS
brill.com/shrs

Controlling the Export of Digital and Emerging Technologies

Security and Human Rights Perspectives

Machiko Kanetake
Assistant Professor, Utrecht University, Utrecht, The Netherlands
m.kanetake@uu.nl

Abstract

Dual-use export control regulates the trade of items which serve both civilian and military purposes. Justification for imposing export controls has been furnished by the need for safeguarding regional and international security, especially the non-proliferation of weapons of mass destruction. The rationale for applying export controls has been subject to challenges, however. This *Security and Human Rights* special issue addresses the underlying justification for imposing export controls by focusing on their technological fronts. Scott A. Jones' piece sheds light on the regulatory challenges that have arisen for the US' control over so-called "emerging" technologies. Cindy Whang moves on to compare the US' approach with that of the EU's dual-use export control. Ben Wagner proposes a set of policy options for the design of export controls on digital technologies, so that they can serve as an effective vehicle for promoting the protection of human rights.

Keywords

trade – export control – dual-use – digital surveillance – emerging technologies – human rights – national security

1 Introduction: Theme of the Symposium*

Export control is one of the sub-fields of international law situated at the intersection of international security law and international trade law.[1] At the international level, export control has been justified by the need for controlling military risks that undermine international and regional security. This account holds true for so-called "dual-use" export control over those items which can serve both civil and military purposes.[2] Special attention has been given to the non-proliferation of weapons of mass destruction, as a result of which non-proliferation treaties provide a legal basis for imposing export controls,[3] such as Article III.2 of the Treaty on the Non-Proliferation of Nuclear Weapons.[4] International treaties have been complemented by a series of non-binding export control regimes, such as the Australia Group, the Nuclear Suppliers Group, and the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.[5] These multilateral regimes play a key role in identifying specific military and dual-use items subject to export control. While licensing decisions are ultimately in the hands of each state and its national legal frameworks, the existence of multilateral regimes creates certain foreseeability and regulatory harmonization in decentralized export control practices.

While the control of military risks has served as a common justification for export controls, their military rationale has been subject to the multitude of challenges. One of the sectors in which such challenges became apparent in

* The research for this paper is supported by a grant (2020–2021) from Gerda Henkel Stiftung, and carried out within the Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE). The theme of the present symposium was discussed at the workshop on 15 September 2020, co-organized with Dr. Berenice Boutin of the Asser Institute and the Utrecht Centre for Global Challenges.

1 P. Achilleas, "Introduction Export Control" in D. Tamada & P. Achilleas (eds.), *Theory and Practice of Export Control: Balancing International Security and International Economic Relations* (Springer, 2017), p. 4.

2 See, in particular, the definition of dual-use under the EU's regulation: Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, OJ 2009 L134/1, Article 2(1).

3 M. Kanetake, "Balancing Innovation, Development, and Security: Dual-Use Concepts in Export Control Laws" in N. Craik, C.S. Jefferies, S.L. Seck & T. Stephens (eds.), *Global Environmental Change and Innovation in International Law* (Cambridge: Cambridge University Press, 2018), pp. 184–185.

4 Treaty on the Non-proliferation of Nuclear Weapons, 1 July 1968 (entered into force 5 March 1970), 729 UNTS 161, Article III.2.

5 For an overview, see I. Anthony & J.P. Zanders, "Multilateral Security-Related Export Controls," *SIPRI Yearbook 1998: Armaments, Disarmament and International Security* (1998).

recent years pertains to the export control of so-called "emerging" technologies. The determination of what constitutes an "emerging" element in a continuous process of technological advance appears to be necessarily more political than technical. Certain categories of technologies have nevertheless been discussed under the broad banner of "emerging technologies," whose content is inherently subject to change. Export control is no exception in this regard.

On this technological front, some of the major industrial actors have relied upon, or attempted to rely on, a set of justifications which are less intertwined with military risks. In the US, during the administration of President Trump, the country introduced export controls over "emerging and foundational technologies,"[6] including advanced surveillance technologies (such as faceprint and voiceprint technologies) and machine learning technology.[7] In applying the export control over such technologies, the US stretched the concept of "national security" and created a stronger and explicit linkage between national security controls and the US' economic and scientific competitiveness.[8] The US' controls over emerging and foundational technologies posed various conceptual challenges to the basis for imposing export controls.[9]

On the other side of the Atlantic, the EU has been debating, since 2013, how to strengthen its export control of information and communications technology. Within the EU, the guiding narrative has been found in the protection of human rights, in order to prevent the repressive use of digital surveillance technologies in destination countries.[10] The watershed moment arrived in September 2016 when the European Commission submitted a proposal to recast Council Regulation No 428/2009.[11] One of the proposal's

6 Export Controls Act of 2018, 50 U.S.C. 4817, Section 1758.

7 US Department of Commerce, Bureau of Industry and Security, "Review of Controls for Certain Emerging Technologies" (Advance Notice of Proposed Rulemaking, ANPRM), 83 FR 58201 (19 November 2018).

8 On the analysis of US Export Controls Act, see C. Whang, "Undermining the Consensus-Building and List-Based Standards in Export Controls: What the US Export Controls Act Means to the Global Export Control Regime," Vol. 22, No. 4, *Journal of International Economic Law* (2019), pp. 579–599.

9 See S. Jones, "Disrupting Export Controls:"Emerging and Foundational Technologies" and Next Generation Controls," Vol. 6, No. 9, *Strategic Trade Review* (2020), pp. 31–52.

10 For the repressive use of certain technologies, see, e.g., B. Wagner, *Exporting Censorship and Surveillance Technology* (Humanist Institute for Co-operation with Developing Countries (Hivos), 2012).

11 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), COM(2016) 616 final (28 September 2016).

ambitions was to provide an "effective response to threats for human rights resulting from their uncontrolled export."[12] Such an attempt to achieve the "modernisation"[13] of the EU's dual-use export control has met strong resistance, however. Many EU member states and several industry associations voiced their disagreement with the Commission's proposal.[14] After several years of negotiations, on 9 November 2020, the Council of the EU and European Parliament finally reached a provisional political agreement regarding the EU's dual-use regulation which will replace Council Regulation No 428/2009.[15] The informal draft text as of 13 November 2020 explicitly acknowledged human rights implications associated with the export of cyber surveillance items.[16] Furthermore, the draft introduced a mechanism for EU member states to coordinate their responses to swiftly react to "serious misuse of existing technologies" and to "new risks associated with *emerging* technologies."[17]

Against this background, this journal symposium aims at analyzing the narrative and justification used by the US and EU as the key players in regulating the international trade of digital as well as so-called "emerging" technologies. The symposium addresses the mixed narrative of security and human rights underlying trade restrictions introduced, or to be introduced, by the US and EU. The symposium considers some of the fundamental differences among the key industrial players in reforming the technological fronts of export controls. Particular attention is paid to the role of the EU—both at the regional and international levels—in integrating human rights perspectives into the justification for imposing dual-use export controls.

12 Ibid., p. 6.

13 European Commission, Communication from the Commission to the Council and the European Parliament: the review of export control policy: ensuring security and competitiveness in a changing world, COM (2014) 244 final (24 April 2014), p. 2.

14 See M. Kanetake, "Converging Dual-Use Export Control with Human Rights Norms: The EU's Responses to Digital Surveillance Exports" in E. Fahey (ed.), *Framing Convergence with the Global Legal Order: The EU and the World* (Oxford: Hart Publishing, Bloomsbury Publishing Plc, 2020), pp. 65–81.

15 Council of the EU, New rules on trade of dual-use items agreed, Press release (9 November 2020), available at: https://www.consilium.europa.eu/en/press/press-releases/2020/11/09/new-rules-on-trade-of-dual-use-items-agreed/ (last accessed 15 November 2020).

16 Council of the EU, 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), Confirmation of the final compromise text with a view to agreement (ST 12798/20 INIT) (13 November 2020).

17 Ibid., recital 6 (original emphasis omitted; new emphasis added). See ibid, Articles 8 and 8a.

2 Roadmap

The journal symposium invited three scholars who have expertise in trade restrictions on digital and emerging technologies. The symposium began with Scott A. Jones' contribution regarding the US' approaches to the export control of emerging and foundational technologies. As Jones articulated, national security concerns have been levelled against the development and use of some of the innovative technologies, such as artificial intelligence, additive manufacturing (e.g., 3D printing), and quantum computing. The perceived risks over the military applications of so-called emerging technologies prompted the US, among others, to reform its export control regulations. Central to the reform is Section 1758 of the Export Control Reform Act (ECRA), passed in 2018, which established a process to identify and control the export of emerging and foundational technologies.[18] Pursuant to the ECRA, the US' Bureau of Industry and Security (BIS) published a representative list of 14 technology categories as a framework for ascertaining specific emerging technologies that are essential to the US' national security and subject to export controls.[19] To ascertain such technologies would also trigger foreign investment controls. The basic difficulty, however, lies in the fact that the identification of "emerging" technology as envisaged under the ECRA is not directly linked to military or other weapons systems and necessarily obscures the concept of national security as a basis for export controls. Jones suggested that both the potential and limits of export controls ought to be properly understood in order for the governance of emerging technologies to be in line with their technological and economic realities.

Jones' paper was followed by Cindy Whang's article, in which she compared the US' approach with that of the EU's dual-use export control. As Whang articulated, the export control of emerging technologies involves a balancing act between responses to security concerns, on the one hand, and accommodation of technological realities, on the other hand. Whang discussed how the US and EU have been respectively seeking such a balance with regard to export liability for cloud computing service providers. Divergence in policies became more fundamental, however, when the ECRA of 2018 strengthened economic considerations as a basis for controlling the export of emerging and foundational

18 Export Control Reform Act of 2018, 50 U.S.C. 4801. See, in particular, 50 U.S.C. 4817, Section 1758 (as part of Export Controls Act of 2018, 50 U.S.C. 4801, Sections 1751 et seq.).

19 US Department of Commerce, Bureau of Industry and Security, "Review of Controls for Certain Emerging Technologies" (Advance Notice of Proposed Rulemaking, ANPRM), 83 FR 58201, 19 November 2018.

technologies. Such controls have been combined with other export control measures against specific technology companies, such as Huawei Technology Co. Whang characterized the US' policy changes as an example of "geoeconomics," the concept explored earlier by Roberts, Choer Moraes, and Ferguson.[20] The US' policy direction is rather in contrast to the narrative of human security and human rights that paved the way for the EU's reform of its export controls over digital surveillance technologies.

Building on the comparative analysis of the US and EU's approaches, the symposium invited Ben Wagner's contribution in order to consider what would be the way forward. In his paper, Wagner contextualized dual-use export control within the wider policy and governance challenges. As he pointed out, it is troubling that the human rights implications of some of the dual-use technologies have not been subject to wider public debate. One of the persistent problems lies in a lack of transparency regarding export licensing decisions, which simultaneously creates a basic obstacle for ensuring the accountability of relevant decision makers and exporters. Within the EU, the assessment of human rights implications has been strengthened with regard to the export of cyber surveillance items.[21] Yet what is needed, as suggested by Wagner, is a wider international initiative to integrate human rights perspectives into export control. Wagner recommends the strengthening of external oversight concerning export control licensing decisions involving both national and international human rights institutions.

3 Conclusion: Challenges Beyond the EU's Recast Process

Overall, the present journal symposium highlighted an ongoing quest for justifications and modalities for the governments to impose export controls on emerging, as well as existing, technologies. The quest is by no means novel. Yet the rapid development of digital technologies and their increasing global connectedness has posed a novel challenge to the design and operationalization of export controls. The EU's recast process—especially from September 2016 to November 2020—illuminates some of the major challenges to the regulatory control of technological exports. Such challenges will certainly continue

20 A. Roberts, H. Choer Moraes & V. Ferguson, "Toward a Geoeconomic Order in International Trade and Investment," Vol. 22, No. 4, *Journal of International Economic Law* (2019), pp. 655–676.

21 According to the informal version of the text as of 13 November 2020, *supra* note 16.

to affect the shape of export controls and the level of certainty that the EU's new regulation provides to exporters and governments.

First, one of the fundamental, conceptual issues pertains to the *types of risks* that governments aim to mitigate by imposing export controls. While the construction of such risks is necessarily fluid and subject to political environment, there is no denying that dual-use export control has developed as a mechanism to mitigate *military* risks.[22] This is also embedded in the very definition of dual-use items.[23] However, the EU's recast process to "modernize" its export control regulation as well as the US' ECRA of 2018 have shown policy preferences for departing from a military-based rationale for imposing export controls, as discussed in depth in Jones and Whang's papers at this symposium.

Within the EU, one of the most controversial issues during the recast process was how to address human rights risks of the export of "cyber-surveillance items."[24] The Commission's 2016 proposal was led by concerns over the risks that such technologies pose to "the right to privacy and the protection of personal data, freedom of expression, freedom of association" and, indirectly, "freedom from arbitrary arrest and detention, or the right to life."[25] The attempt to address such human rights concerns without fundamentally changing the concept of dual-use items is destined to create uncertainty, however, over the types of risks that the EU's dual-use regulation aims to address.[26] According to the draft text as of 13 November 2020, the EU's regulation maintains the basic definition of dual-use items based on the duality of civil and military purposes (Article 2(1)).[27] Such a military pillar is preserved also for "cyber-surveillance items" which are understood to be part of "dual-use items" (Article 2(21)). While the concept of military purposes has already been flexible and context-dependent, to address the human rights concerns that motivated the recast process would require governments to further stretch the very notion of military purposes.

Second, the debates over the types of risks are intertwined with the long-standing question over the level of *transparency* in export controls. The narrative of military security has traditionally restricted the availability of information

22 See M. Kanetake, "The EU's Dual-Use Export Control and Human Rights Risks: The Case of Cyber Surveillance Technology," *Europe and the World: A law review* (2019) pages 7–9.

23 Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, OJ 2009 L134/1, Article 2(1).On the concept of dual-use items, see Kanetake, *supra* note 3.

24 M. Kanetake, "The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches," Vol. 4, No. 1, *Business and Human Rights Journal* (2019), pp. 155–162.

25 European Commission (28 September 2016), *supra* note 11, at 6.

26 See Kanetake, *supra* note 23 pages 8–9.

27 The informal version of the text as of 13 November 2020, *supra* note 16.

concerning export control licensing decisions. Yet the EU's deliberation on human rights risks during the recast process was accompanied by a call to improve the level of transparency. According to the text of November 2020, the requirement of transparency has apparently been strengthened. In particular, the annual report on the implementation of the regulation must include "dedicated information" on export authorizations with regard to cyber surveillance items (Article 24(2)). While the word "dedicated" may reflect disagreement over the level of detail required for annual reports, they should cover the information on the number of licensing applications received "by items" (as opposed to the "types" of items), the number of the destinations concerned, and the decisions taken on these applications (Article 24(2)). In order to improve the quality of the reports, EU-wide guidelines will also be made available on the "methodology for data gathering and processing" (Article 24(2)). While it remains to be seen how much information is publicly provided in practice, a growing expectation for transparency and external scrutiny cannot be distinct from the changes in the types of risks that export controls are expected to address.

Third, the departure from military-based rationale triggers a related question over the extent to which a state may choose to impose its *autonomous* export controls. Within the EU, the Commission's 2016 proposal notably added the EU's autonomous lists of controlled items on "cyber-surveillance technology."[28] While the November 2020 draft no longer contains such an autonomous category of controlled items,[29] the draft creates a coordination mechanism for controls over "non-listed" cyber surveillance items. For instance, if an exporter is "aware"—according to its "due diligence findings"—that non-listed cyber surveillance items "are intended, in their entirely or in part" "for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law," the exporter is obliged to notify the competent authority (Article 4a(2)). On this basis, the member state authority must decide whether to impose an authorization requirement (Article 4a(2)).

The unique aspect of the text agreed by the Parliament and the Council was that a member state's control is followed by the EU-wide consultation as well as engagement with multilateral regimes. Once the authorization is

28 European Commission (28 September 2016), *supra* note 11, Annex I, Category 10.

29 It must be noted that some technologies which can fall under the broad understanding of cyber-surveillance technologies have been added to the Wassenaar Arrangement's control lists and thereafter to the EU's dual-use regulation. See, e.g., Commission Delegated Regulation (EU) 2020/1749 of 7 October 2020 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (2020) OJ L 421/1 (e.g., Annex I, 5D001.e).

imposed at the national level, the member state is obligated to inform the European Commission and other member states which thereafter "review" the information received (Article 4a(4), (5)). The information may eventually be published by the EU if "all Member States notify the other Member States and the Commission" that "an authorisation requirement should be imposed for essentially identical transactions" (Article 4a(6)). It remains to be seen how such an EU-wide consultation works in practice. At any rate, it must be remembered that the EU's "autonomous" controls under Article 4a are distinct from list-based controls under Annex I of the regulation. With regard to the list-based controls, Article 4a appears to promote what the Council has previously described as "upward convergence."[30] Namely, EU member states are expected to engage in multilateral export control regimes in view of altering the international control lists (Article 4a(10)).[31]

Finally, for the control over digital and emerging technologies to be workable, it would be crucial to develop understanding of *human rights due diligence* in the context of export controls. As noted above, Article 4a(2) of the November 2020 text assumes that exporters themselves conduct "due diligence" for "cyber-surveillance items." While Article 4a(2) borrows "some" of the legal terms used in the second criterion of the EU's Common Positions on arms control,[32] the terms and contexts are by no means the same. After all, Article 4a(2) pertains to the thresholds on which an authorization would be required in the first place, as opposed to the yardsticks on which the export ought to be eventually denied. While the Commission and the Council would make available the EU-wide guidelines for exporters (Article 24(1)), such guidelines would necessarily be read in conjunction with the concept of human rights due diligence developed in many other fields, especially to implement the UN's Guiding Principles on Business and Human Rights (UNGPs).[33]

---

30 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): Mandate for Negotiations with the European Parliament" (5 June 2019) at 11 (recital 29).

31 Furthermore, on top of the catch-all controls over cyber surveillance items under Article 4a, the draft text of November 2020 created a mechanism to coordinate member states' national export controls, including those imposed based upon human rights considerations: The text as of 13 November 2020, *supra* note 16, Articles 8 and 8a.

32 Council Common Position 2008/944/CFSP of 8 December 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment (2008) OJ L 335/99, Article 2(2) (Criterion Two).

33 United Nations, "Guiding Principles on Business and Human Rights: Implementing the UN "Protect, Respect and Remedy" Framework,' HR/PUB/11/04 (2011). See also Kanetake, *supra* note 14, pp. 72–76.

In conclusion, the export control of digital and emerging technologies cannot be separated from the wider normative development at the regional and international levels. In particular, the decisions to export such technologies cannot be exempt from the expectation to integrate the UNGPs' human rights due diligence in all aspects of business practices. While the EU's recast process should be understood as an attempt to promote the implementation of the UNGPs in export controls, what matters in the long run is how multilateral export control regimes can engage in non-military risks in a more explicit manner. It is no doubt difficult to alter the foundation of regimes such as the Wassenaar Arrangement. Yet, as proven from the EU's recast process to reform export controls, what will be tested is not only the EU's loyalty to multilateral fora but the quality and responsiveness of such international regimes themselves.