The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches

Machiko KANETAKE*

Keywords: cyber technology, due diligence, export control, European Union, surveillance

I. INTRODUCTION

International trade in the field of information and communication technologies (ICTs) can be a vehicle to bring not only business opportunities but also human rights risks into trading partners. While Edward Snowden's revelation facilitated public debate on governmental mass surveillance at home, much less discussed is the human rights implication of the *export* of cyber surveillance technology.[1] In a news report in April 2017 entitled 'Spy Merchant', Al Jazeera provided a glimpse of the human rights risks of ICT exports.[2] The report captured an Italian company's preparedness to execute the 20 million Euro deal to export to Iran an internet protocol (IP) interception system that could readily be used to monitor citizens.[3] Multiple other reports further reveal that, in response to popular revolt across the Middle East and North Africa from 2010 to 2012, a number of European and United States (US) ICT companies exported surveillance equipment to Syria, Tunisia, Saudi Arabia, the United Arab Emirates, Qatar, Oman, Algeria and Morocco, and helped advance their mass surveillance systems.[4]

* Assistant Professor, Utrecht University (email: m.kanetake@uu.nl).

[1] For the purpose of this piece, 'cyber surveillance technologies' include mobile telecommunications interception equipment, internet protocol (IP) network surveillance systems, monitoring centres, lawful interception systems and data retention systems, and digital forensics. See Mark Bromley, '*Export Controls, Human Security and Cyber-Surveillance Technology: Examining the Proposed Changes to the EU Dual-Use Regulation*' (Stockholm International Peace Research Institute, December 2017) 6–10.

[2] 'How the "Dual-Use" Ruse is Employed to Sell Spyware', *Al Jazeera* (10 April 2017), https://www.aljazeera.com/indepth/features/2017/04/dual-ruse-employed-sell-spyware-170409092222936.html (accessed 20 July 2018).

[3] Ibid.

[4] Ben Wagner, 'Exporting Censorship and Surveillance Technology' (Humanist Institute for Co-operation with Developing Countries (Hivos), January 2012); Privacy International, 'Open Season: Building Syria's Surveillance State' (December 2016); 'How BAE Sold Cyber-Surveillance Tools to Arab States', *BBC News* (15 June 2017), https://www.bbc.com/news/world-middle-east-40276568 (accessed 20 July 2018); 'Danmark tillod salg af teknologi, der kan overvåge en hel befolkning, til et af verdens mest undertrykkende regimer: Saudi-Arabien', *Information* (15 June 2017), https://www.information.dk/indland/2017/06/danmark-tillod-salg-teknologi-kan-overvaage-hel-befolkning-verdens-mest-undertrykkende-regimer-saudi-arabien (accessed 20 July 2018); 'Udenrigsministeren kæder overvågningseksport sammen med kampen mod IS', *Information* (18 August 2017), https://www.information.dk/indland/2017/08/udenrigsministeren-kaeder-overvaagningseksport-sammen-kampen-is-0 (accessed 20 July 2018).

Business and Human Rights Journal, 4 (2019), pp. 155–162
doi:10.1017/bhj.2018.18

Following the Arab Spring, the political climate within the European Union (EU) has pushed forward legislative reforms towards a better human rights risk management of ICT exports. In 2015, the European Parliament repeatedly voiced the need for regulating the export of human rights-sensitive cyber technology.[5] The field of law in which the European Parliament saw potential is the EU's 'dual-use export control' regime, which is the subject of this piece. The regime aims at regulating the cross-border transfer of items that serve 'both civil and military purposes'.[6]

This piece provides a brief account of the EU's recent legislative reform on the export control of cyber surveillance technology. Within the EU, the export of dual-use items has been governed by Council Regulation (EC) No. 428/2009 of 5 May 2009,[7] which forms an integral part of the EU's Common Commercial Policy. In response to the European Parliament's call,[8] the European Commission submitted, in September 2016, the proposal to recast the EU's existing dual-use regulation.[9] In essence, the Commission's proposal situated human rights as one of the conceptual pillars of dual-use export control. The fundamental hurdle, however, lies in the fact that export control has developed essentially to mitigate 'military' risks, especially those involving the proliferation of chemical, biological and nuclear weapons.[10]

This piece begins in part II with an overview of the key human rights elements included in the European Commission's proposal, and then analyses three major points of resistance to the proposed reform in part III. As of 20 July 2018, the Commission's proposal, which follows the ordinary legislative procedure,[11] is under the first reading before the Council of the EU. In the European Parliament, the proposal received strong support on 17 January 2018 in the first reading, with 571 members in favour, 29 against, and 29 abstained.[12] Yet subsequent negotiations have slowed down as a number of member states, as well as industries, have manifested their opposition to the proposed reform. Regardless of the EU's legislative outcomes, the fact that the Commission's initiatives invited a great deal of resistance is intriguing in itself. Contestations levelled against the proposal reveal some of the pragmatic obstacles that the EU encounters in achieving its rights-based international trade.

---

[5] European Parliament, 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries (2014/2232(ini))', P8_TA(2015)0288 (8 September 2015) paras 2, 36, 39; European Parliament, 'Resolution on the Annual Report on Human Rights and Democracy in the World 2014 and the European Union's Policy on the Matter (2015/2229(INI)', P8_TA(2015)0470 (17 December 2015) para 124; European Parliament, 'Resolution on the European Defence Union (2016/2052(INI))', P8_TA(2016)0435 (22 November 2016) para 21.

[6] Council Regulation (EC) No. 428/2009 of 5 May 2009 [2009] OJ L134/1, art 2(1).

[7] Ibid.

[8] European Parliament (8 September 2015), note 5, para 36.

[9] 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) art 2(1).

[10] On the relationships between export control and non-proliferation regimes, see, e.g., Oliver Meier, 'Dual-Use Technology Transfers and the Legitimacy of Non-Proliferation Regimes' in O Meier (ed), *Technology Transfers and Non-Proliferation: Between Control and Cooperation* (Abingdon: Routledge, 2014) 3.

[11] Consolidated Version of the Treaty on the Functioning of the European Union [2008] OJ C115/47, art 294.

[12] For the text adopted, see European Parliament, 'Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items', First reading, P8_TA-PROV(2018)0006 (17 January 2018).

II. EU's Reform on Rights-Based Export Control

The European Commission's September 2016 proposal is an attempt to invoke human rights considerations as one of the key justifications for restricting exports. A particular emphasis was put on protecting the right to privacy, freedom of expression and freedom of association.[13] The rights-based export control is normatively consistent with Article 207 of the Treaty on the Functioning of the European Union (TFEU) and Article 21 of the Treaty on European Union (TEU),[14] under which export control ought to be carried out in the context of the principles and objectives of the EU's external action, including the protection of human rights and fundamental freedoms.

The Commission's proposal notably obliges EU member states' authorities to take into account 'respect for human rights in the country of final destination' in deciding on the grant of export authorization.[15] This is contrasted with Article 8(1) of the EU's existing dual-use regulation, according to which member states are allowed, and thus not obliged, to prohibit (or require authorization on) exports for 'public security or human rights considerations'.[16] The Commission's proposal further introduced the EU's 'autonomous list'[17] of items subject to export control, which focused specifically on 'cyber surveillance technology'.[18] The EU's own control list is clearly contrasted with the existing regulation, under which the list of dual-use items reflects 'internationally agreed dual-use controls', including those agreed on by the Wassenaar Arrangement, one of the most comprehensive export control regimes.[19]

In addition, one of the most controversial changes pertains to a so-called 'catch-all' control, which is a residual export control mechanism over 'non-listed' items. Article 4 of the proposal expects *both* authorities and exporters to be vigilant in human rights risks even if export items in question are not specifically listed by the regulation. Under Article 4(1)(d) of the proposal, export authorization is required if an exporter is 'informed' by the authority that the items 'are or may be intended' 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'.[20] While Article 4(1)(d) still expects exporters to be passive recipients of governmental information, much more contested is Article 4(2) of the Commission's proposal. Under Article 4(2), exporters themselves bear an 'obligation to exercise due diligence'.[21] In carrying out such an obligation, exporters must notify the competent authority if the exporters become 'aware' that non-listed dual-use items are intended for the commission

[13] European Commission (28 September 2016), note 9, 6.

[14] TFEU, note 11, art 207; Consolidated Version of the Treaty on European Union [2008] OJ C115/13, art 21.

[15] European Commission (28 September 2016), note 9, art 14(1)(b).

[16] Council Regulation (EC) No. 428/2009, note 6, art 8(1).

[17] European Commission (28 September 2016), note 9, art 9.

[18] European Commission, 'Annexes to 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) 616 final, Annexes 1 to 6 (28 September 2016) 243–244, Annex I, B (List of Other Dual-Use Items), Category 10.

[19] Council Regulation (EC) No. 428/2009, note 6, Annex I.

[20] European Commission (28 September 2016), note 9, art 4(1)(d).

[21] Ibid, art 4(2).

of serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression.[22]

Human rights due diligence itself is not entirely a novel requirement under EU law.[23] For instance, Directive 2014/95/EU on non-financial information disclosure requires large public interest entities that exceed 500 employees to publish reports on the companies' policies on human rights due diligence.[24] Also, the so-called Conflict Minerals Regulation (Regulation (EU) 2017/821) imposes, from January 2021, supply chain due diligence on EU importers of conflict-sensitive minerals,[25] in part for the purpose of preventing human rights abuses.[26] Nevertheless, the Commission's proposal on due diligence differs from these precedents. It goes beyond the mere disclosure requirement inasmuch as the proposal requires exporters to exercise due diligence. Moreover, the requirement is applicable to exporters in general, regardless of their size and business sectors, as long as their export items can be connected to the serious violations of human rights in destination countries.

III. Resistance to Rights-Based Export Control

A. Civil and Military Dichotomy

The European Commission's proposal, however, invited resistance from some Members of the European Parliament (MEPs), several EU member states and industry representatives. One of the sources of contestation lies in the premise that export control is essentially meant to address 'military' risks. Dual-use items are fundamentally defined by the 'civil and military' dichotomy,[27] and the evidence that an item may contribute to the development of 'military capabilities'[28] justifies it being listed for control by international export control regimes. However, the Commission's September 2016 proposal extended the definition of dual-use items to include 'cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law'.[29] Namely, the linkage to 'military' risks was no longer considered requisite.

Such a conceptual change was not readily welcomed by industry representatives. Having characterized the extended definition as 'one of the biggest changes',[30] DIGITALEUROPE,

---

22 Ibid.

23 See Angelica Dziedzic et al, 'Towards EU Legislation on Human Rights Due Diligence: Case Study of the Garment and Textile Sector' (2017) HEC Paris Research Paper No. LAW-2017-1207.

24 Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 [2014] OJ L 330/1, art 1; Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 [2013] OJ L 182/19, arts 19a, 29a (as amended by Directive 2014/95/EU).

25 Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 [2017] OJ L 130/1.

26 Ibid, art 2(f).

27 Council Regulation (EC) No. 428/2009, note 6, art 2(1).

28 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 'Initial Elements' (11–12 July 1996) para I.1.

29 European Commission (28 September 2016), note 9, art 2(1)(b).

30 DIGITALEUROPE, 'European Commission Proposed Recast of the European Export Control Regime: Making the Rules Fit for the Digital World' (24 February 2017), http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&entryID=2358&language=en-US&PortalId=0&TabId=353 (accessed 20 July 2018).

which represents the digital technology industry in Europe, claimed that the 'existing dual-use definition should continue being based on the internationally established definition'.[31] A number of EU member states also opposed the uneasy combination of cyber surveillance technology with the concept of dual-use items. In their working paper, dated 29 January 2018, the eleven EU member states enunciated that the existing dual-use definition 'should remain as it is' as the 'internationally established definition'.[32]

B. Harmonization with International Regimes

The definitional query is intertwined with a fundamental question as to whether and to what extent the EU's dual-use export control should follow an autonomous path. The idea of 'harmonization' with international regimes deeply governs the practices of export control, including those of the EU.[33] Without regulatory harmonization, countries that have a stringent trade control may put themselves in a less competitive position. Despite the economic rationale of regulatory convergence, the European Commission's proposal has chosen to diverge from international export control regimes.

The message that the EU would take an autonomous approach invited contestations from member states and business associations. The eleven EU member states' working paper in January 2018 demonstrated their clear preference for regulatory harmonization with international regimes.[34] In another working paper, dated 15 May 2018, nine EU member states also expressed concern that the EU's 'unilateral measures' 'could seriously undermine the competitiveness of EU-based industry'.[35] On this basis, the nine member states defied the introduction of the EU's autonomous list and favoured working through international export control regimes.[36] Otherwise, the nine member states claimed, the EU would not be considered an attractive destination for global frontrunners on ICT.[37]

C. Exporters' Capacity to Assess Human Rights Risks

Concerns are also raised that business enterprises are not fully capable of assessing human rights risks in the context of export control unless such risks are specifically defined in advance. Even before the Commission submitted the proposal, the Federation

[31] DIGITALEUROPE, 'Updated DIGITALEUROPE Comments on Proposal for Recast of Export Control Regulation' (30 January 2018), http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&entryID=2608&language=en-US&PortalId=0&TabId=353 (accessed 20 July 2018) 1.

[32] 'Working Paper: EU Export Control – Recast of Regulation 428/2009', WK 1019/2018 INIT (29 January 2018), https://www.euractiv.com/wp-content/uploads/sites/2/2018/02/11_member_states_dual-use.pdf (accessed 20 July 2018). The document was prepared on behalf of the Croatian, Czech, French, German, Italian, Polish, Portuguese, Romanian, Slovak, Slovenian and Spanish delegations.

[33] Machiko Kanetake, 'Balancing Innovation, Development, and Security: Dual-Use Concepts in Export Control Laws' in N Craik *et al* (eds), *Global Environmental Change and Innovation in International Law* (Cambridge: Cambridge University Press, 2018) 180, 184–6.

[34] 'Working Paper' (29 January 2018), note 32.

[35] 'Working Paper: 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 Globally' WK 5755/2018 INIT (15 May 2018), https://www.euractiv.com/wp-content/uploads/sites/2/2018/06/nine-countries-paper-on-dual-use.pdf (accessed 20 July 2018). The Working Paper was prepared on behalf of the Czech Republic, Cyprus, Estonia, Finland, Ireland, Italy, Poland, Sweden and the United Kingdom.

[36] Ibid, 2–4.

[37] Ibid, 4.

of German Industries (Bundesverband der Deutschen Industrie, BDI) had claimed that companies were 'not in a position to take political decisions'.[38] According to the BDI, German industry rejects 'non-specific human rights standards', especially their use in catch-all provisions.[39] On this basis, the BDI demanded that EU institutions specify human rights violations and list specific countries with the records of systematic human rights violations.[40] Likewise, DIGITALEUROPE requested that EU institutions identify a list of excluded end-users in advance and avoid relying on the broad protection of human rights through a catch-all provision.[41] As illustrated by these statements, industry representatives argued that human rights were so political that industry was not well equipped to render risk assessment as part of due diligence. As put by DIGITALEUROPE, '[g]overnments are much better prepared' to identify possible cases of human rights violations.[42]

A series of amendments tabled at the European Parliament during the proposal's first reading show differences in opinion among MEPs on the role of business communities. Some MEPs favoured retaining the exporters' proactive role in assessing human rights risks. For instance, German MEP Klaus Buchner, a key advocate of robust export control over cyber surveillance technology, proposed an amendment that explicitly links 'due diligence' with the UN Guiding Principles on Business and Human Rights (UNGPs).[43] The amendment expected exporters to identify, prevent, mitigate and account for human rights impacts of not only their own operations but also of 'business relationships'.[44] By contrast, some other MEPs resisted the idea of imposing on an exporter the 'obligation to exercise due diligence' under Article 4(2) of the proposal. Seven MEPs tabled amendments to omit the term 'due diligence' due to the lack of conceptual clarity.[45] Austrian MEP Paul Rübig further proposed the deletion of Article 4(1)(d) of the Commission's proposal on the grounds that the provision put a disproportionate burden on businesses and export control authorities.[46]

In the end, when the European Parliament adopted the proposal at first reading in January 2018,[47] the Parliamentary amendments deleted the term 'obligation' with regard to exporters' due diligence requirement.[48] Despite this omission, however, the

---

[38] BDI, 'EC Dual-Use: Review of the EC Dual-Use Regulation' (January 2016), https://bdi.eu/media/topics/global_issues/downloads/201601_FINAL_BDI-Assessment_Reform_EC_Dual-Use.pdf (accessed 20 July 2018).

[39] Ibid, 6.

[40] Ibid, 6–7.

[41] DIGITALEUROPE (24 February 2017), note 30, 3.

[42] DIGITALEUROPE (30 January 2018), note 31, 2.

[43] EP INTA Committee, Rapporteur Klaus Buchner, 'Draft Report 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) (4 April 2017) 18, Amendment 20.

[44] Ibid.

[45] EP INTA Committee, Rapporteur Klaus Buchner, 'Amendments: Draft Report 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) (16 May 2017), Amendments 181 (Paul Rübig), 182 (Franck Proust), 184 (Sander Loones), 186 (Christofer Fjellner, Artis Pabriks, Bendt Bendtsen, Godelieve Quisthoudt-Rowohl).

[46] Ibid, 68, Amendment 166 (Paul Rübig).

[47] European Parliament (17 January 2018), note 12.

[48] Ibid, Amendment 34 (regarding art 4(2) of the proposal).

Parliamentary amendments favoured, overall, strengthening rights-based catch-all controls under Article 4 of the proposal. According to the Parliamentary amendment to Article 4(2), an exporter must notify the competent authority if the exporter becomes aware, while exercising due diligence, that non-listed dual-use items 'may be intended' for the commission of human rights violations.[49] This is contrasted with the wording of the Commission's proposal, in which the notification duty arises when the exporter is aware that items 'are intended' for serious human rights violations.[50]

Overall, EU institutions and their stakeholders have different expectations about the appropriate degree of involvement of exporters in assessing the risks attached to cyber surveillance technology and potentially other human rights sensitive items. While the Commission's proposal was warmly welcomed by several prominent human rights organizations,[51] the proposal anticipates exporters wearing a 'different hat' and engaging in the difficult task of considering the rights of those individuals who are outside the exporting state's jurisdiction and whose unique identity is still unknown at the time of export.

IV. Conclusion

There is no denying that the export of cyber surveillance technology can serve legitimate purposes. The technology is critical, not only for law enforcement authorities to detect and prevent crimes, but also for private business enterprises that may need to acquire advanced intrusion software in order to build robust data security systems. At the same time, the cross-border transfer of surveillance technology can be a vehicle to facilitate the violations of civil and political rights in importing countries.

The European Commission's proposal marked a watershed in addressing the human rights risks of modern technological exports. Despite its significance, debates that followed reveal the intricate reality that a number of corporations, including those of ICT sector, hesitate to be an assessor of human rights risks in the context of exporting products abroad. Several EU member states, including Germany, France and the UK, also expressed their hesitation to impose human rights due diligence tasks on exporters.

The crux is that these resentments were expressed, despite the ostensible maturity of the 'business and human rights' narrative in the EU. A number of international guidelines, including the UNGPs, already expect business enterprises (along with states) to be the guardians of fundamental rights and to carry out human rights due diligence. Several EU member states have adopted National Action Plans to implement the UNGPs.[52] Yet the adoption of the UNGPs or the development of National Action Plans does not automatically speak to industries' readiness to apply human rights norms to their daily business undertakings. While the Commission's proposal needs conceptual

[49] Ibid, Amendment 34 (art 4, para 2).

[50] See ibid, Amendment 34 (art 4, para 2).

[51] Shared Statement on the Update of the EU Dual-Use Regulation (May 2017), https://www.accessnow.org/cms/assets/uploads/2017/05/NGO_Sharedstatement_dualuse_May2017.pdf (accessed 20 July 2018).

[52] Beata Faracik, 'Implementation of the UN Guiding Principles on Business and Human Rights' (European Parliament, Directorate-General for External Policies of the Union, 2017) 20–26.

clarification, a more proactive stance on the part of ICT industry would, at any rate, be necessary, should the EU integrate human rights in its external policies and EU member states integrate the UNGPs in their trade practices. The deliberation surrounding the reform of the EU's dual-use export control, while revealing obstacles towards rights-based export practices, must therefore be considered a necessary step forward in incrementally bringing human rights languages into the EU's international trade law and policies.