Europe and the World:
A law review

UCLPRESS

Special issue: *Economic and Non-economic Values and Objectives in the EU's International Trade: Actors and Processes in Resolving Normative Tensions*

Article

The EU's dual-use export control and human rights risks: the case of cyber surveillance technology

Machiko Kanetake

Assistant Professor of Public International Law, Utrecht University, the Netherlands; m.kanetake@uu.nl

How to Cite: M. Kanetake, 'The EU's dual-use export control and human rights risks: the case of cyber surveillance technology' [2019] 3(*1*): 3. *Europe and the World: A law review* [16].
DOI: https://doi.org/10.14324/111.444.ewlj.2019.14.

Submission date: 26 July 2018; Acceptance date: 26 April 2019; Publication date: 26 June 2019

Peer review:
This article has been peer reviewed through the journal's standard double blind peer-review, where both the reviewers and authors are anonymised during review.

Abstract

Export of cyber technology can undermine human rights in countries of destination. In the aftermath of the Arab Spring, political controversies have arisen around EU-exported cyber surveillance technology, which allegedly helped autocratic states monitor and arrest dissidents. While cyber technology is indispensable to our lives, it can be used to suppress the right to privacy, the freedom of expression and the freedom of association, not only in the EU, but also in the countries it trades with. The EU has taken a proactive role in reforming the export of human rights-sensitive cyber technology. In September 2016 the European Commission proposed the integration of human rights due diligence in the process of export control. The Commission's proposal, however, invited strong contestations both from industry and Member States. Essentially, dual-use export control has developed in order to mitigate military risks. Attempts to integrate human rights risks in export control have thus invited discomfort among stakeholders. This paper unpacks normative tensions arising from the EU's attempts to integrate human rights risks in its export control regimes. By so doing, the paper highlights fundamental tensions embedded in the EU's value-based Common Commercial Policy, of which dual-use export control forms an integral part.

Keywords: export control; dual-use; cyber surveillance; human rights; EU trade

1. Introduction

The export of cyber technology can bring both benefits and harms to destination countries. Take, for instance, the export of a computer device that is used to intercept private online communications. The device may serve states' police agencies by detecting fraudulent transactions and preventing organised crime. At the same time, however, the same computer device can be used to suppress freedom of expression, the right to privacy and freedom of association in the country of destination. The Arab Spring from 2010 to 2012 revealed the strong interlinkages between, on the one hand, the export of cyber surveillance technology and, on the other hand, the infringement of human rights in countries of destination. During and after the Arab Spring, cyber surveillance technology exported by EU companies was reportedly employed by autocratic governments to monitor and arrest dissidents.[1]

'Dual-use export control', which is the topic of this paper, is one of the fields of law which can potentially be mobilised to mitigate human rights risks involved in the export of cyber technology. A 'dual-use' item is defined as an item which serves both civilian and military purposes. A vast amount of material, machinery, equipment and technology, which are in fact critical to sustaining our ordinary lives, can also be used by states and non-state actors for a variety of military purposes, including the production of weapons of mass destruction (i.e. chemical, biological and nuclear weapons). Non-proliferation is the core aim of dual-use export control and a set of rules have been developed internationally and implemented at the domestic level. In the EU, the export of dual-use items has been regulated by Council Regulation (EC) No 428/2009 of 5 May 2009.[2] The Regulation has direct effect across the EU and forms part of the EU's Common Commercial Policy under Article 207 of the Treaty on the Functioning of the European Union (TFEU). The Regulation is supplemented by each EU Member State's domestic export control law to implement licensing and enforcement processes.

This paper aims at analysing how the EU's dual-use export control accommodates human rights risks, especially those associated with the export of cyber surveillance technologies. In principle, given that the EU's dual-use export control forms an integral part of the EU's Common Commercial Policy, such trade control ought to be carried out 'in the context of the principles and objectives of the Union's external action', as provided in Article 207 TFEU. Included in such principles is the universality and indivisibility of human rights and fundamental freedoms.[3] In practice, however, to integrate human rights norms in export control gives rise to a fundamental dilemma. The basic problem lies in the fact that dual-use export control has essentially developed to mitigate 'military' risks. The military mandate of dual-use export control creates conceptual, political and normative hurdles for the EU's attempts to accommodate human rights norms, as will be elaborated upon in this paper.

The paper starts with providing concrete examples which highlight human rights risks associated with the export of cyber technology (Section 2). Political controversies levelled against the misuse of EU-originated cyber technology in non-EU countries have led to the European Commission's proposal submitted in September 2016 to 'recast' existing Council Regulation (EC) No 428/2009, which governs the EU's dual-use export control.[4] In its September 2016 proposal, the Commission put forward a more stringent control over the export of cyber surveillance technologies (Section 3). While such a proposal is consistent with the EU's normative commitment to promoting human rights through its international trade law and policies, to place the protection of human rights as a normative pillar of the EU's export control gives rise to interlinking challenges. To begin with, export control to mitigate human rights risks incurs a

[1] See e.g. 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) <http://www.bbc.com/news/world> accessed 1 December 2018.

[2] 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 [2009] OJ L 134/1. Council Regulation (EC) No 428/2009 was amended most recently by Commission Delegated Regulation (EU) 2017/2268 of 26 September 2017. For background to the 2009 Regulation, see Anna Giulia Micara, 'Current Features of the European Union Regime for Export Control of Dual-Use Goods' (2012) 50(4) *Journal of Common Market Studies* 578.

[3] Article 21 Treaty on European Union (TEU).

[4] Council Regulation (EC) No 428/2009 (n 2).

conceptual tension with the traditional mandates of the control regime based on the mitigation of 'military' risks (Section 4). Such a conceptual challenge is accompanied by *political* contestations levelled against the imposition of general human rights risk assessment on industries (Section 5). Furthermore, to tighten the export of cyber surveillance technology gives rise to a *normative* tension, not only between trade and human rights, but also *within* human rights norms themselves (Section 6). This paper's main focus is on a particular field of law. Nevertheless, the three-fold tensions highlighted in this paper can likewise exist in other domains of the EU's Common Commercial Policy such as the conclusion and implementation of international trade agreements, in which the EU, according to Article 207 TFEU, ought to integrate human rights and fundamental freedoms.

2. Human rights risks of the export of cyber technology

The EU-level initiatives to strengthen the export control of cyber technologies started to take shape in response to mass demonstrations and revolt across the Middle East and North Africa from 2010 to 2012.[5] Controversies surround the sales from the EU of surveillance equipment to non-EU authorities which are often regarded as autocratic, and about which the EU or its Member States have raised repeated concerns about human rights situations. For instance, according to Privacy International, an international NGO, Italian and South African companies made 'important contributions' from 2007 to 2012 to the building of Syria's surveillance state.[6] Various other sources likewise suggest that a number of European and US information technology companies contributed to the development of Tunisian surveillance infrastructure and that some European consultants offered technical support to the Tunisian government to maintain its surveillance mechanisms.[7]

Al Jazeera's investigation, reported in April 2017, provides a glimpse of the human rights risks of the EU's export practices.[8] Al Jazeera's report, entitled 'Spy Merchant', revealed an Italian company's readiness to execute a 20-million euro deal to export, to Iran, an IP-intercept system that could readily be used for spying on citizens.[9] The Italian company was willing to proceed with the deal, despite the EU's export control regime against Iran, which had been imposed as the EU's response to serious human rights violations within the country.[10] On another front, in June 2017 the BBC and a Danish newspaper reported that the Danish authorities had allowed the export of a surveillance system to Saudi Arabia, the United Arab Emirates, Qatar, Oman, Algeria, Morocco and Tunisia around the period of the Arab Spring.[11] The system, called Evident, was sophisticated enough to allow authorities (and private persons) to 'intercept any internet traffic', including 'a whole country'.[12] The surveillance system was developed by a Danish company that had been purchased in 2011 by a British defence giant. According to the BBC, which contacted a former Tunisian intelligence official, the exported surveillance system was indeed used to trace dissidents during the time of the Arab Spring.[13] Licensing approval continued after the popular uprisings; on 12 February 2016 the Danish government authorised the British defence company's Danish subsidiary to export USD 70 million-worth of surveillance technology to Saudi Arabia, on the

[5] See e.g. European Commission, 'Report from the Commission to the Council and the European Parliament on the Implementation of Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items' COM (2013) 710 final (16 October 2013) 13.

[6] Privacy International, 'Open Season: Building Syria's Surveillance State' (n 1) 6.

[7] Wagner, *Exporting Censorship and Surveillance Technology* (n 1) 8.

[8] '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 1 December 2018.

[9] ibid.

[10] Council Decision 2011/235/CFSP of 12 April 2011 concerning restrictive measures directed against certain persons and entities in view of the situation in Iran [2011] OJ L 100/51; Council Regulation (EU) No 359/2011 of 12 April 2011 concerning restrictive measures directed against certain persons, entities, and bodies in view of the situation in Iran [2011] OJ L 100/1.

[11] 'How BAE Sold Cyber-Surveillance Tools to Arab States' (n 1); '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> accessed 1 December 2018; 'Udenrigsministeren kæder overvågningseksport sammen med kampen mod IS' (*Information*, 18 August 2017) <https://www.information.dk/indland/2017/08/udenrigsministeren> accessed 1 December 2018.

[12] 'How BAE Sold Cyber-Surveillance Tools to Arab States' (n 1).

[13] ibid.

basis that the technology would be used for the purposes of 'national security and investigation of serious crimes'.[14] One must acknowledge that it is hard to verify any specific link between the governmental use of the surveillance system and the arrest of dissidents. Nevertheless, according to Amnesty International, the imprisonment of some Saudi Arabian human rights activists could only have been accounted for by the governmental interception of email correspondence between the arrested individuals and Amnesty International.[15]

The story surrounding the Danish-exported surveillance system highlights how the export of cyber surveillance technology from EU Member States or other industrial countries could be a catalyst for violations of the right to privacy, freedom of speech and freedom of assembly in third countries. For the sake of this paper, 'cyber surveillance technologies' are meant to include the following technology and equipment: mobile telecommunications interception equipment (which is to track, identify, intercept and record mobile phones); intrusion software (which is used to remotely monitor computers); internet protocol (IP) network surveillance systems (to intercept data passing through an IP network); monitoring centres (designed to collect, store and analyse communications data); lawful interception systems and data retention systems (used by service providers to intercept and store data as required by law); and digital forensics (to retrieve and analyse communications data stored in networks, computers and mobile devices).[16] While Edward Snowden's revelation in 2013 heightened EU citizens' awareness of governmental mass surveillance at home, the technology can still be exported, and thereby the misuse can carry over to the EU's trading partners.

Following the Arab Spring in 2010–12 the European Parliament repeatedly requested a revision of the EU's Dual-Use Export Regulation in order to avoid cyber technology being used to violate human rights.[17] In September 2015 the European Parliament adopted a resolution entitled 'Human Rights and Technology', which specifically focused on the impact of intrusion and surveillance systems on human rights in third countries.[18] In ensuring 'coherence' between the EU's external actions and its policies relating to information and communication technologies (ICTs), the European Parliament reaffirmed that the EU's human rights standards 'prevail' in the assessment of the export of dual-use technologies used in ways that may restrict human rights.[19] On this basis, the Parliament urged the Commission to swiftly put forward a proposal to address potentially harmful exports of ICT products and services to third countries.[20] In December 2015, in its annual report on 'human rights and democracy', the European Parliament, having expressed concerns about the use of ICTs by authoritarian regimes, called on the Commission to 'pay particular attention to the human rights aspects of dual-use goods' in the framework of revising the EU's export control.[21] The Council also joined the parliamentary calls; the Council's Action Plan on Human Rights and Democracy 2015–19 included the review of the Dual-Use Regulation to mitigate the potential risks associated with the 'uncontrolled export of ICT [information and communications technology] products'.[22] Overall, the political climate galvanised reform sentiment at the EU level towards a better human rights risk management of ICT exports.

[14] 'Danmark tillod salg af teknologi, der kan overvåge en hel befolkning, til et af verdens mest undertrykkende regimer: Saudi-Arabien' (n 11).

[15] ibid.

[16] 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; Mark Bromley, Kees Jan Steenhoek, Simone Halink and Evelien Wijkstra, 'ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns' (2016) 2 *Strategic Trade Review* 37.

[17] See European Parliament, 'Resolution on the European Defence Union (2016/2052(INI), P8_TA(2016)0435 (22 November 2016)' para 21.

[18] 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).

[19] ibid, paras 2, 39.

[20] ibid, para 36.

[21] 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.

[22] Council of the European Union, 'Council Conclusions on the Action Plan on Human Rights and Democracy 2015–2019' 10897/15 (20 July 2015) 24.

3. Modernising the EU's export control

3.1. Human rights as a basis for restricting exports

In order to respond to the political concerns levelled against the export of cyber surveillance technology, the European Commission proposed the pursuit of the 'modernisation' of the EU's export control in line with rapidly changing technological, economic and political circumstances.[23] In October 2013, in accordance with the scheduled review of Council Regulation (EC) 428/2009,[24] the European Commission presented a report on the implementation of the Dual-Use Regulation to the Council and the Parliament.[25] This was followed by the Communication in April 2014 in which the Commission identified policy options for modernising the EU's export control.[26] What matters for the purpose of this paper is that the Commission, in its April 2014 Communication, proposed the consideration of a 'human security' approach to recognise the inextricable linkage between security and human rights.[27] The Commission explained, albeit merely in a footnote, that the human security approach 'intends to place people at the heart of EU export control policy'.[28] The Commission contrasted the human security approach with the 'traditional military and state-centred approach to security' and called for the extension of dual-use concepts beyond military-related end uses.[29]

Consideration of human security then allowed the European Commission to put a stronger emphasis on the protection of fundamental rights in the proposal submitted subsequently in September 2016.[30] The proposal was meant to recast and replace Council Regulation (EC) No 428/2009. While the Commission no longer used the term 'human security', the proposal kept adhering to at least one of the elements of human security – namely, the protection of human rights. Among them, a particular emphasis was put on respect for the right to privacy, freedom of expression and freedom of association.[31]

It must be noted that there is nothing novel in the EU employing human rights as a normative ground for restricting the export of sensitive items. First, within the context of dual-use export control, Article 8(1) of Council Regulation (EC) No 428/2009 already allows, if not mandates, a Member State to prohibit (or impose an authorisation requirement on) the export of dual-use items 'for reasons of public security or human rights considerations'.[32] Second, in addition to the Dual-Use Regulation, the EU has enacted the so-called Anti-Torture Regulation, an autonomous export control on goods which could be used for torture and other cruel treatment.[33] Third, in the field of arms trade control, Council Common Position 2008/944/CFSP of 8 December 2008 requires EU Member States to consider the destination country's respect for human rights and international humanitarian law when the states assess arms export licences.[34] Under the Common Position, EU Member States must deny an export licence if there is a 'clear risk'

[23] 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) 2.

[24] Council Regulation (EC) No 428/2009 (n 2) Article 25(2).

[25] European Commission, 'Report from the Commission to the Council and the European Parliament on the Implementation of Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items' COM (2013) 710 final (16 October 2013). For analysis of the Commission's proposal, see e.g. Bromley, *Export Controls, Human Security* (n 16).

[26] European Commission, 'The Review of Export Control Policy' (n 23).

[27] ibid 6.

[28] ibid.

[29] European Commission, 'Commission Staff Working Document, Impact Assessment, Report on the EU Export Control Policy Review', SWD (2016) 315 final (28 September 2016) 28.

[30] 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) Article 2(1).

[31] ibid 6.

[32] Council Regulation (EC) No 428/2009 (n 2) Article 8(1).

[33] Council Regulation (EC) No 1236/2005 of 27 June 2005 concerning trade in goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment [2005] OJ L 200/1.

[34] 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, respect for human rights as well as humanitarian law).

that the military technology or equipment might be used for internal repression.[35] Such repression is not limited to cases of torture, arbitrary executions, disappearances or arbitrary detentions. Internal repression can also take the form of 'other major violations of human rights and fundamental freedoms'.[36] Finally, the EU has a record of imposing economic sanctions as part of its Common Foreign and Security Policy on the basis of human rights violations. For example, the EU's sanctions regime against Myanmar was based on the continuing violations of human rights in the country, including torture and summary and arbitrary executions.[37]

Nor is it novel for the EU to impose export control on certain cyber surveillance technologies. Already several years before the Commission's 2016 proposal on the reform of dual-use export control, some of the cyber surveillance technologies had been added to the control list of the Wassenaar Arrangement, one of the most comprehensive international export control regimes, which serves as the basis for the EU's export control list. Mobile telecommunications interception equipment, known as IMSI catchers, was added to the list of the Wassenaar Arrangement in December 2012.[38] IP network communications surveillance systems and intrusion software were listed on the Wassenaar Arrangement's control list in December 2013.[39] These changes made in the Wassenaar Arrangements were duly incorporated in the EU's control list in 2014.[40]

3.2. Strengthening the human rights pillar

Despite the EU's record of invoking human rights as a ground for restricting exports and controlling the export of certain cyber surveillance technologies, the Commission's September 2016 proposal still marked a significant change in export control laws. In essence, the proposal was an attempt to situate a consideration of human rights not as a marginal consideration, but as one of the key normative grounds for controlling the export of sensitive items. A fundamental difference between the earlier changes made in the Wassenaar Arrangement, on the one hand, and the European Commission's 2016 September proposal, on the other, thus lies in a *normative justification* for imposing export control. The traditional justification for adding items to an export control list was to mitigate military risks, especially the proliferation of weapons of mass destruction. By contrast, under the European Commission's 2016 proposal, human rights risks served as a separate 'non-military' basis for imposing export licensing requirements.

Based on the human rights pillar, the September 2016 proposal mandated Member States' competent authorities to take into account 'respect for human rights in the country of final destination' as well

[35] ibid, Article 2(2)(a).

[36] ibid, Article 2(2)(b).

[37] e.g. Common Position 96/635/CFSP of 28 October 1996 [1996] OJ L 287/1; Council Regulation 1081/2000 of 22 May 2000 [2000] OJ L 122/29; Council Decision 2010/232/CFSP of 26 April 2010 [2010] OJ L 105/22; Council Decision 2013/184/CFSP of 22 April 2013 [2013] OJ L 111/75; Council Decision (CFSP) 2017/734 of 25 April 2017 [2017] OJ L 108/35. Human rights-based trade sanctions can be reconciled with the General Agreement on Tariffs and Trade (GATT), particularly under Article XX(a) (public morals) and (b) (human life or health) objectives insofar as the measures are necessary to achieve these objectives and comply with the requirements in the chapeau of Article XX. See e.g. Robert Howse and Jared M Genser, 'Are EU Trade Sanctions on Burma Compatible with WTO Law' (2007) 29 *Michigan Journal of International Law* 165, 182–96; Sarah H Cleveland, 'Human Rights Sanctions and International Trade: A Theory of Compatibility' (2002) 5(1) *Journal of International Economic Law* 133–89; Rachel Harris and Gillian Moon, 'GATT Article XX and Human Rights: What Do We Know from the First 20 Years?' (2015) 16 *Melbourne Journal of International Law* 432–83.

[38] The Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (12) 1 (12 December 2012), Category 5.A.1.f (mobile telecommunications interception).

[39] The Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (13) 1 (4 December 2013), Categories 4.A.5 (intrusion software), and 5.A.1.j (IP network communications surveillance systems); Innokenty Pyetranker, 'An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement' (2015) 13 *Northwestern Journal of Technology and Intellectual Property* 153, 162–64.

[40] Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014 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 [2014] OJ L 371/1. At that time, the ICT industry levelled concerns that the export control over intrusion software would hamper the industry's legitimate activities. This industrial opposition led the US to delay the national implementation of intrusion software controls and prompted the Wassenaar Arrangement to create certain exceptions: Bromley, 'Export Controls, Human Security' (n 16) 10–11. See the Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, WA-LIST (17) 1 (7 December 2017), Category 4.E.1.

as respect by that country for international humanitarian law in deciding whether or not to grant an export authorisation.[41] With respect to cyber technology, the Commission's proposal introduced the EU's 'autonomous list'[42] of items subject to export control. Under Regulation 428/2009, dual-use items were catalogued according to ten groups, from 'Category 0' to 'Category 9'. The Commission's 2016 proposal then created a new group, 'Category 10', specifically for 'cyber surveillance technology', and listed items which had not yet been regulated by the Wassenaar Arrangement.[43] Under the proposal, cyber surveillance technology is defined as an item 'specifically designed to enable the covert intrusion' into information and telecommunication systems, with a view to 'monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system'[44] although what constitutes 'covert intrusion' was not defined by the proposal. In addition to the creation of the EU's autonomous list, the Commission's proposal revised a so-called 'catch-all' control based on human rights risks. A catch-all control is a residual mechanism to allow authorities to exert export control over items even if they are not specifically listed. The proposal's catch-all clause, which strengthened human rights assessment, attracted a great deal of controversy, as will be further elaborated upon in Section 5 below.

As of 1 May 2019, the European Commission's proposal, which follows the ordinary legislative procedure, is under the first reading before the Council. On 17 January 2018, the European Parliament in its plenary session adopted its first reading of the Commission's proposal and a series of amendments to it. The European Parliament has given strong support to the proposal; 571 members of the Parliament voted in favour, 29 against, and 29 abstained.[45] It remains to be seen how the legislative process will move forward and to what extent human rights considerations will be preserved in the end. Regardless of the outcome of the EU's legislative process, however, the fact that the Commission's proposal invited contestations is intriguing in its own right. As a matter of principle, EU law anticipates the permeation of human rights into the EU's external action.[46] Also, internationally, businesses are increasingly expected to bear the role of human rights guardians, especially since the adoption of the UN's Guiding Principles on Business and Human Rights in 2011.[47] Yet there remains a fundamental gap between normative expectation and the actual modus operandi of corporations, and the reform of dual-export control epitomises such a reality. Controversies surrounding the Commission's proposal highlight some of the actual hurdles that subsist in the EU's ambition to integrate respect for human rights in its international trade law and policies.

4. Conceptual tensions: departures from military risks and international harmonisation

The EU's attempts to accommodate human rights in its export control have given rise to three-fold challenges. The first line of resistance is at the conceptual level, which is one of the sources of political disagreements explained in Section 5 below. As dual-use export control has developed in order to mitigate military risks, invoking human rights as a normative pillar involves a fundamental shift from the traditional raison d'être of export control. Under Regulation 428/2009, 'dual-use items' are simply defined as items that can be used for 'both civil and military purposes'.[48] The military mandate of export control is manifested, for instance, in the founding document of the Wassenaar Arrangement, which is the most comprehensive international standard-setting regime on export control.[49] The Wassenaar Arrangement is built on COCOM (Coordinating Committee for Multilateral Export Control), which was the Western

[41] European Commission 'Proposal' (28 September 2016) (n 30) Article 14(1)(b).

[42] ibid, 9.

[43] 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) 243–44, Annex I, Category 10.

[44] European Commission 'Proposal' (28 September 2016) (n 30) Article 2(21).

[45] 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).

[46] Article 207 TFEU; Article 21 TEU.

[47] United Nations, 'Guiding Principles on Business and Human Rights: Implementing the UN "Protect, Respect and Remedy" Framework', HR/PUB/11/04 (2011).

[48] Council Regulation (EC) No 428/2009 (n 2) Article 2(1).

[49] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 'Initial Elements' (11–12 July 1996) <www.wassenaar.org/docs/IE96.html> accessed 1 December 2018.

bloc's export control regime during the Cold War.[50] According to the founding document, the Wassenaar Arrangement aims to ensure that transfers of conventional arms and dual-use goods and technologies do not contribute to the development of 'military capabilities' which undermine regional and international security and stability.[51]

The concept of military risks, which provide the rationale for imposing export control, is by no means static. Not only the development of new technologies, but also political priorities among industrial countries have altered the terrain of military risks. The non-proliferation of weapons of mass destruction has been the core priority for export control, built on a series of international treaties. One of the earliest non-proliferation treaties is the 1925 Geneva Protocol, which prohibits in war the use of poisonous gases and bacteriological methods of warfare.[52] Other major treaties include the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT),[53] the 1972 Biological and Toxin Weapons Convention (BTWC),[54] and the 1993 Chemical Weapons Convention (CWC).[55] These conventions are accompanied by UN Security Council Resolution 1540 on the non-proliferation of weapons of mass destruction.[56] While the non-proliferation of weapons of mass destruction has been one of the backbones of export control, it has been recognised politically that conventional weapons also undermine regional and international security. The Wassenaar Arrangement, established in 1996, encompasses dual-use goods and munitions which serve not only for weapons of mass destruction, but also for conventional weapons.[57] The adoption of the Arms Trade Treaty in 2013 gave the most clear-cut recognition to the importance of regulating the cross-border transfer of conventional weapons. Under Article 7 of the Treaty, a state party cannot grant export licences if there is an overriding risk that conventional arms would undermine peace and security or that they could be used for a serious violation of international humanitarian or human rights law.[58]

While the kind of military risks which justify export controls have been subject to changes, the European Commission's September 2016 proposal added another layer of conceptual uncertainties. The Commission's proposal still maintained the basic definition of dual-use items built on the dichotomy of 'civil and military purposes'.[59] At the same time, the proposal extended the definition so as to include 'cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law'.[60] This definition was apparently an uncomfortable compromise since cyber surveillance technologies do not always fit in with the duality of civil and military purposes.[61] The proposed definition created an inconsistency with the overall definition of dual-use items.

[50] Kenneth A Dursht, 'From Containment to Cooperation: Collective Action and the Wassenaar Arrangement' (1997) 19(3) *Cardozo Law Review* 1079–23, 1098.

[51] 'Initial Elements' (n 49) para I.1.

[52] Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, 17 June 1925, 94 LNTS 65 (entered into force 8 February 1928). On the scope of the Protocol, see RR Baxter and Thomas Buergenthal, 'Legal Aspects of the Geneva Protocol of 1925' (1970) 64(5) *The American Journal of International Law* 853.

[53] Treaty on the Non-proliferation of Nuclear Weapons, 1 July 1968, 729 UNTS 161 (entered into force 5 March 1970).

[54] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 10 April 1972, 1015 UNTS 163 (entered into force 26 March 1975).

[55] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, 13 January 1993, 1974 UNTS 45 (entered into force 29 April 1997).

[56] UN Doc S/RES/1540, 28 April 2004.

[57] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 'Initial Elements' (11–12 July 1996) para I.1 <www.wassenaar.org/docs/IE96.html> accessed 1 December 2018.

[58] Arms Trade Treaty, 3 June 2013, 52 ILM 988 (2013) (entered into force 4 December 2014) Article 7(1)(a), 7(1)(b)(i) and (ii), 7(3).

[59] European Commission 'Proposal' (28 September 2016) (n 30) Article 2(1).

[60] According to the proposal of September 2016: '"dual-use" items shall mean items, including software and technology, which can be used for both civil and military purposes, and shall include: . . . (b) cyber surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law, or can pose a threat to international security or the essential security interests of the Union and its Member States': ibid, Article 2(1)(b).

[61] On the analysis of duality within export control, see Machiko Kanetake, 'Balancing Innovation, Development, and Security: Dual-Use Concepts in Export Control Laws' in Neil Craik, Cameron SG Jefferies, Sara L Seck and Tim Stephens (eds), *Global Environmental Change and Innovation in International Law* (Cambridge University Press, 2018) 180.

Understandably, therefore, even one of the key advocates of export control reforms and a member of the European Parliament (MEP), Marietje Schaake, tabled a series of amendments in order to treat cyber surveillance technology as a controlled item independent from dual-use items.[62] Her amendments were meant to achieve conceptual coherence by recognising, in a much more straightforward manner, that the EU's export control is no longer constrained by the traditional dichotomy of civil and military purposes.

The proposed conceptual reform further entails the EU's departure from the idea of 'harmonisation' which is embedded in the practices of export control. Regulatory harmonisation across industrial countries is indeed crucial in securing the effectiveness of export control; without harmonisation, those countries which adopt a stricter trade control may end up losing their economic competitiveness. The idea of harmonisation thus traditionally served the basis for the EU's Dual-Use Export Control Regulation. Under Regulation No 428/2009, the list of dual-use items was said to be the implementation of 'internationally agreed dual-use controls', including the Wassenaar Arrangement, the Missile Technology Control Regime, the Nuclear Suppliers Group, the Australia Group and the CWC.[63]

By aligning itself with these multilateral export control regimes, the EU's Dual-Use Regulation inherits the military rationale of export control. The military mandate of dual-use export control is illustrated by so-called 'catch-all' controls, according to which the authorities can impose a licensing requirement even if an item in question is not listed by Annex I of the Regulation. Under Council Regulation 428/2009, Member States' authorities can require a licence if the items in question are or may be intended for use in connection with the development of weapons of mass destruction or missiles capable of delivering such weapons.[64] In short, while the definition of military purposes itself is no doubt wide, this does not change the basic fact that dual-use export control has developed essentially to regulate military risks, especially those associated with the development of weapons of mass destruction.

Resistance against the Commission's proposal is therefore understandable in light of the aforementioned assumptions that dual-use export control is for military risks and that the EU's Regulation should be in harmony with international regimes. For instance, DIGITALEUROPE, a voice of the European digital technology industry, claimed that the 'existing dual-use definition should continue being based on the internationally established definition'.[65] DIGITALEUROPE, in its comments released in November 2018, reiterated the need for maintaining the basic dual-use definition. The industry association expressed its opinion that the Commission's proposal would 'expand the category of items considered "dual use" in a conceptually concerning manner'.[66] According to DIGITALEUROPE, dual-use items should remain to be identified by 'their technical characteristics rather than their potential misuse'.[67]

Contestations come from EU Member States' authorities as well. Shortly after the conclusion of the first reading by the European Parliament, the 11 EU Member States, in their leaked working paper dated 29 January 2018, expressed their clear dissent from the Commission's proposal.[68] The working paper, drafted primarily by Germany and France, stressed the importance of the EU working through international export control regimes as a global level-playing field. The 11 Member States' working paper

[62] 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 104, 110, 115, 163, 185 (Marietje Schaake).

[63] Council Regulation (EC) No 428/2009 (n 2) Annex I. See Kanetake, 'Balancing Innovation, Development, and Security: Dual-Use Concepts in Export Control Laws' (n 61).

[64] See Council Regulation (EC) No 428/2009 (n 2) Article 4(1).

[65] DIGITALEUROPE, 'Updated DIGITALEUROPE Comments on Proposal for Recast of Export Control Regulation' (30 January 2018) <http://www.digitaleurope.org/resources/updated-digitaleurope-comments-on-proposal-for-recast-of-export-control-regulation/> 1, accessed 1 December 2018.

[66] DIGITALEUROPE, 'Comments on Recent Developments in Council Export Control Working Group' (22 November 2018) <https://www.digitaleurope.org/resources/digitaleurope-comments-on-recent-developments-in-council-export-control-working-group/> accessed 1 December 2018.

[67] ibid.

[68] 'Working Paper: EU Export Control – Recast of Regulation 428/2009', WK 1019/2018 INIT (29 January 2018) available via EURACTIV.com <https://www.euractiv.com/wp-content/uploads/sites/2/2018/02/11_member_states_dual-use.pdf> accessed 1 December 2018. The document was prepared on behalf of the Croatian, Czech, French, German, Italian, Polish, Portuguese, Romanian, Slovak, Slovenian and Spanish delegations.

made it clear that the existing dual-use definition based on the civil–military dichotomy 'should remain as it is today', given that it is the internationally established definition of dual-use items.[69] In essence, the 11 Member States strongly favoured regulatory harmonisation with international regimes, on the basis that the 'EU does not work in isolation' in regulating international exports.[70] Likewise, in another working paper dated 15 May 2018, nine EU Member States also expressed their concern about the EU's 'unilateral measures'.[71] The nine Member States were opposed to the introduction of the EU's autonomous list and favoured working through international export control regimes.[72] Otherwise, the nine Member States claimed, the EU would not be considered an attractive destination for global frontrunners in ICT.[73]

5. Political tensions in human rights risk assessment

5.1. Due diligence in the Commission's September 2016 proposal

The conceptual challenges intrinsic to human rights-based export control were combined with political or more pragmatic concerns levelled against the Commission's 2016 proposal to modernise export control. A great deal of controversy stemmed from the inclusion of 'due diligence' in the context of dual-use export control and whether and how businesses could be expected to play a role in assessing human rights risks. One of the striking features of the Commission's proposal was the invocation of general due diligence obligations applicable to exporters. Particularly relevant is Article 4 of the proposal, concerning the 'catch-all' control over non-listed items. Article 4(1)(d) of the 2016 proposal first expects authorities – and not exporters themselves – to be vigilant in human rights risks. Under Article 4(1)(d) of the proposal, authorisation 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'.[74] Article 4(1)(d) of the proposal triggered a relatively moderate debate, as exporters were supposed to be the mere recipients of information from relevant authorities.

Highly contested was instead Article 4(2) of the Commission's proposal, according to which exporters themselves are under an 'obligation to exercise due diligence'. In exercising 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 of serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression.[75] Although the EU's political initiatives to address human rights risks were encouraged by controversies surrounding the export of cyber surveillance technologies,[76] Article 4(2) of the Commission's proposal applies the due diligence obligation and notification requirements, not only to ICT sectors, but to exporters in general.

5.2. Due diligence under EU and international legal frameworks

The invocation of human rights due diligence itself is nothing new under EU law.[77] A noteworthy example in this regard is the EU's Directive 2014/95/EU on disclosure of non-financial information, according to which large public interest entities that exceed 500 employees are obliged to publish reports

[69] ibid 2.

[70] ibid 1.

[71] '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> 1–2, accessed 1 December 2018. The Working Paper was prepared on behalf of the Czech Republic, Cyprus, Estonia, Finland, Ireland, Italy, Poland, Sweden and the United Kingdom.

[72] ibid 2–4.

[73] ibid 4.

[74] European Commission 'Proposal' (28 September 2016) (n 30) Article 4(1)(d).

[75] ibid, Article 4(2). See also Section 4 above.

[76] See Section 2 above.

[77] See Angelica Dziedzic, Céline Lelièvre, Jonathan Povilonis, Alberto Alemanno and Paige Morrow, '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.

on the companies' policies on human rights due diligence processes.[78] While Directive 2014/95/EU on disclosure by no means holds companies liable for their failure to meet human rights standards, mandatory disclosure requirements are aimed at incrementally altering business practices and reducing associated human rights risks.[79] Apart from the general non-disclosure requirement applicable to large companies, Regulation (EU) 2017/821 sets out sector-specific due diligence, which is in part motivated by the mitigation of human rights abuses.[80] The so-called Conflict Minerals Regulation, which will be in force on 1 January 2021, imposes supply chain due diligence on EU importers of conflict-sensitive minerals (tin, tantalum and tungsten, their ores, and gold).[81] The Regulation's focus is to ensure responsible sourcing of minerals originating in conflict-affected and high-risk areas, which include those areas with 'widespread and systematic violations of international law, including human rights abuses'.[82] The Conflict Minerals Regulation requires importers to identify and assess risks in the supply chain, implement a strategy to respond to the risks, and conduct an independent third-party audit, following the Organisation for Economic Co-operation and Development (OECD) Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas.[83] International human rights and humanitarian law are part of the standards against which supply chain risks are assessed.[84]

Yet the European Commission's 2016 proposal on dual-use export control differed from these precedents on human rights due diligence in corporate practices. Due diligence requirements envisaged under the proposal go beyond the mere disclosure requirement and are expected to be applicable to small and medium-sized corporations as well. Also, due diligence requirements are presumed applicable to a wide range of industrial sectors as long as their products can be relevant to serious violations of human rights in destination countries.

It is also difficult, from an international legal perspective, to see the due diligence requirement under the Commission's proposal as the reflection of what is already fully established under international human rights law. Under international law, 'due diligence' is not a free-standing concept but an area-specific obligation arising out of a specific primary norm of international law. This means that 'human rights' due diligence emanates from human rights law rather than any overarching principles of international law. Within international human rights treaty regimes, the concept of due diligence has certainly been gaining currency. In General Comment No. 31 on the International Covenant on Civil and Political Rights (ICCPR), the UN Human Rights Committee, which monitors the implementation of the ICCPR, remarked in 2004 that states may violate Covenant rights by 'permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm' that private persons or entities cause.[85] Also, according to the Human Rights Committee's 2017 draft General Comment No. 36 on the right to life, states parties are under a 'due diligence obligation' to undertake 'reasonable positive measures' in response to foreseeable threats to life originating from private persons and entities.[86]

[78] Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups [2014] OJ L 330/1 (entered into force 6 December 2014) Article 1; Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings [2013] OJ L 182/19 Articles 19a, 29a (as amended by Directive 2014/95/EU).

[79] See Stephen Kim Park, 'Human Rights Reporting as Self-Interest: The Integrative and Expressive Dimensions of Corporate Disclosure' in RC Bird, DR Cahoy and JD Prenkert (eds), *Law, Business and Human Rights: Bridging the Gap* (Edward Elgar Publishing, 2014) 48.

[80] Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas [2017] OJ L 130/1.

[81] ibid.

[82] ibid, Article 2(f).

[83] Regulation (EU) 2017/821 (n 80); OECD, *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas* (3rd edn, OECD Publishing, 2016) <http://dx.doi.org/10.1787/9789264252479-en> accessed 1 December 2018.

[84] *OECD Due Diligence Guidance* (n 83) 42.

[85] Human Rights Committee, 'General Comment No. 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant' UN Doc CCPR/C/21/Rev.1/Add.13 (29 March 2004) para 8.

[86] Human Rights Committee, 'Draft General Comment No. 36 on Article 6 of the ICCPR, on the Right to Life', First Reading, Revised Draft Prepared by the Rapporteur (July 2017), para 25.

These general statements on due diligence are not readily applicable to a state's decisions to authorise exports, however, simply because individuals who are to be protected are not under the state's jurisdiction. Among human rights treaties, jurisdictional hurdles are arguably the lowest with regard to states' obligations under the International Covenant on Economic, Social and Cultural Rights (ICESCR). Unlike the ICCPR,[87] the obligations of the ICESCR are provided without any explicit reliance upon territory or jurisdiction.[88] According to the UN Committee on Economic and Social and Cultural Rights, states parties are required to take necessary steps to prevent human rights violations committed abroad by corporations domiciled in the states' territory and/or jurisdiction.[89] States would violate the Covenant if they failed to take reasonable measures to prevent a private entity from causing the violation of Convention rights.[90] Nevertheless, even under the ICESCR, such obligations do not appear to oblige states to take preventive measures where private corporations (exporters) do not operate abroad without any immediate involvement in the violations of Convention rights.

More stringent is the case of the ICCPR, under which states' obligations only apply to individuals within its territory and subject to jurisdiction.[91] According to the Human Rights Committee, the jurisdictional clause of the ICCPR should be interpreted broadly and the Covenant is applicable to anyone within the effective control of a state party, even if not situated within the state's territory.[92] Yet the invocation of human rights in the context of export control requires consideration of the rights of those individuals who are outside the exporting state's jurisdiction and whose unique identity may still be unknown at the time of authorising exports. In light of the ICCPR's basic jurisdictional hurdle, the Human Rights Committee's 2017 Concluding Observation on Italy is particularly noteworthy. The Committee therein expressed its concern about allegations that Italian companies provided 'online surveillance equipment' to 'Governments with a record of serious human rights violations' without oversight mechanisms regarding the 'export of such equipment'.[93] On this basis, the Human Rights Committee requested that Italy take measures to ensure that all corporations under its jurisdiction, 'in particular technology corporations', respect human rights standards 'when engaging in operations abroad'.[94] This remark appears to envisage the applicability of human rights due diligence under the ICCPR even if individual victims are abroad and potentially beyond the state's effective control. Yet, despite the indication from the Concluding Observation, it is still premature to conclude that the ICCPR is already *strictu sensu* applicable to a state's decision to authorise exports in general.

Furthermore, at any rate, the principle of due diligence under the ICCPR pertains to a *state's* obligation to take reasonable steps. By contrast, the European Commission's 2016 proposal envisages that *exporters themselves* exercise due diligence. The expectation in relation to business communities is in line with the UN's Guiding Principles on Business and Human Rights.[95] Despite the influential status of the Guiding Principles, the general expectation that businesses should exercise human rights due diligence is formally non-binding. This is despite the narrative put forward by several prominent human rights NGOs in response to the European Commission's 2016 proposal. In May 2017 Accessnow, Amnesty International, Privacy International and several other NGOs, having welcomed the Commission's proposal, characterised the explicit inclusion of human rights considerations as an 'important recognition of the pre-existing responsibilities of both states and businesses'.[96] At least under the ICCPR, however, this

[87] See International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171 (1966) Article 2(1).

[88] Committee on Economic, Social and Cultural Rights, 'General Comment No. 24 (2017) on State Obligations under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activities' UN Doc E/C.12/GC/24 (10 August 2017) para 27.

[89] ibid, para 26.

[90] ibid, para 32.

[91] ICCPR (n 87) Article 2(1).

[92] Human Rights Committee, 'General Comment No. 31' (n 85) para 10.

[93] Human Rights Committee, 'Concluding Observations on the Sixth Periodic Report of Italy' UN Doc CCPR/C/ITA/CO/6 (1 May 2017) para 36.

[94] ibid.

[95] United Nations, 'Guiding Principles' (n 47).

[96] 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> 2, accessed 1 December 2018.

statement does not hold water; human rights considerations in the Commission's proposal go much further than pre-existing international human rights obligations.

5.3. Contested role of industries in human rights assessment

The 2016 proposal, which anticipated exporters' due diligence obligation, invited controversy, not only because such an obligation goes beyond what is already established under international law, but also because private company exporters did not see themselves as capable of assessing human rights risks. A great deal of controversy has arisen from the inclusion of human rights as one of the grounds for catch-all controls. Even before the Commission's proposal was submitted, the Federation of German Industries (Bundesverband der Deutschen Industrie: BDI) had claimed that companies were 'not in a position to take political decisions'.[97] The BDI made it clear that German industry rejects 'non-specific human rights standards', especially their use in catch-all provisions.[98] The BDI found a mere reference to 'human rights violations' too broad to be left in the hands of companies.[99] Instead, the BDI demanded that EU institutions specify human rights violations and list specific countries with records of systematic human rights violations.[100] In a similar vein, DIGITALEUROPE, which represents the digital technology industry in Europe, raised serious concerns over legal uncertainties that the Regulation may create in terms of its regulatory scope. 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.[101] DIGITALEUROPE warned that it would be 'essential' for industry to know 'who is targeted and who is not'.[102] As seen from these statements, the overall sentiment of business communities is that industry is not in a position to render the assessment of potential human rights consequences. As put by DIGITALEUROPE, '[g]overnments are much better prepared' to identify possible cases of human rights violations in terms of the accessibility to information and the capacity to assess political contexts.[103]

Various amendments tabled at the European Parliament reflect differences of views in terms of the role of exporters in assessing human rights risks. On the one hand, some MEPs favoured preserving the exporters' proactive role on the basis of some of the influential international documents on corporate human rights due diligence. In the draft report of the Committee on International Trade (INTA) in April 2017, German MEP and rapporteur Klaus Buchner, a key advocate of robust export control over cyber surveillance,[104] proposed an amendment which explicitly links 'due diligence' with the UN Guiding Principles on Business and Human Rights.[105] This process means that exporters identify, prevent, mitigate and account for human rights impacts not only of their own operations, but also of 'business relationships'.[106] The rapporteur also suggested placing an explicit emphasis on the right to privacy in the digital age.[107] Likewise, at the Committee on Foreign Affairs, Dutch MEP and rapporteur Marietje Schaake also defined 'due diligence' as being based on the UN Guiding Principles.[108]

[97] 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> 7, accessed 1 December 2018.

[98] ibid 6.

[99] ibid.

[100] ibid 6–7.

[101] 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/resources/european-commission-proposed-recast-of-the-european-export-control-regime/> 3, accessed 1 December 2018.

[102] ibid 9.

[103] DIGITALEUROPE (30 January 2018) (n 65) 2.

[104] 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) 41.

[105] ibid 18, Amendment 20.

[106] ibid.

[107] EP INTA Committee, Rapporteur Klaus Buchner, INTA Committee Amendments (16 May 2017) (n 62) 7–8, Amendment 3.

[108] Committee on Foreign Affairs, Rapporter Marietje Schaake, 'Opinion of the Committee on Foreign Affairs for the Committee on International Trade 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))' (31 May 2017) 12–13 (Amendment 16, on Article 2(1)).

On the other hand, several MEPs opposed the idea of imposing on exporters the requirement of human rights due diligence. With regard to an exporter's 'obligation to exercise due diligence' (Article 4(2) of the 2016 proposal), seven MEPs tabled amendments to delete the term 'due diligence' due to the lack of conceptual clarity.[109] Also, Austrian MEP Paul Rübig proposed the deletion of Article 4(1)(d) of the Commission's proposal (on serious violations of human rights or international humanitarian law) on the basis that the provision put a disproportionate burden on businesses and export control authorities and undermined the EU's business competitiveness.[110]

In the end, the Parliamentary amendments in the first reading of January 2018 deleted the term 'obligation' to conduct due diligence. Yet, overall, the Parliamentary amendments further strengthened catch-all controls under Article 4 and favoured the broader coverage of due diligence beyond human rights. According to the amendments, exporters are expected to exercise due diligence as set out not only in the UN's Guiding Principles for Business and Human Rights, but also in the OECD Guidelines for Multinational Enterprises and the OECD Due Diligence Guidance for Responsible Business Conduct.[111] The Parliamentary amendment extended the catch-all control to where 'there is reason to suspect' that items 'may be used' for the purpose of violations of international human rights law or international humanitarian law (Article 4(1)(d)).[112] This is contrasted with the Commission's 2016 proposal, according to which there should be 'evidence of the use' of items for 'serious' violations of human rights or international humanitarian law in situations of armed conflicts or internal repression.[113] Furthermore, 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.[114] The wording of the amendment shows a contrast with the Commission's 2016 proposal, according to which the notification duty arises when the exporter is aware that items 'are intended' for serious human rights violations.[115]

Despite the parliamentary endorsement, several EU Member States still resisted the insertion of the additional human rights-based catch-all control. In their working paper prepared in January 2018, the 11 EU Member States, led by Germany and France, expressed their disagreements with the Commission's proposal. While the states which drafted the working paper were fully aware of the EU's identity to be 'at the forefront of protecting and promoting human rights', the EU had already developed an autonomous path through the Anti-Torture Regulation[116] and Article 8 of the EU's 2009 Dual-Use Regulation regarding human rights considerations.[117] According to the 11 Member States' working paper, the EU's efforts to control cyber surveillance items should be sought by list-based controls; in other words, '[t]here is no need for additional catch-all controls'.[118] In short, the 11 Member States expressed the sentiment shared by many export control officials that rights-based cyber surveillance controls do not fit well with dual-use export control.[119]

[109] EP INTA Committee, Rapporteur Klaus Buchner, INTA Committee Amendments (16 May 2017) (n 62) Amendments 181 (Paul Rübig), 182 (Franck Proust), 184 (Sander Loones), 186 (Christofer Fjellner, Artis Pabriks, Bendt Bendtsen, Godelieve Quisthoudt-Rowohl).

[110] ibid 68, Amendment 166 (Paul Rübig).

[111] European Parliament, 'Control of Exports' (17 January 2018) (n 45), Amendment 11 (Recital 13 a (new)).

[112] ibid, Amendment 32 (Proposal for a regulation, Article 4(1)(d).

[113] See ibid, Amendment 32 (Proposal for a regulation, Article 4(1)(d).

[114] ibid, Amendment 34 (Article 4(2).

[115] See ibid, Amendment 34 (Article 4(2).

[116] Council Regulation (EC) No 1236/2005 (n 33).

[117] 'Working Paper' (29 January 2018) (n 68) 2.

[118] ibid 4.

[119] While the 11 Member States did not claim that cyber surveillance controls should be dealt with by an autonomous regulation (as opposed to an amended dual-use regulation), the 11 member states still regarded cyber surveillance controls as a 'third pillar' of European export control, in addition to dual-use export control (first pillar), and anti-torture controls (second pillar): 'Working Paper' (29 January 2018) (n 68) 2, and fn 1.

6. Normative tensions within human rights law

Finally, the debates on the greater presence of human rights in export control shed light on the possible tensions embedded within international human rights law itself. The EU's efforts to address the human rights risks of cyber surveillance systems have been led primarily by their adverse impacts on civil and political rights. As the Commission's 2016 proposal makes clear, it was led by concerns over the risks posed to 'the right to privacy and the protection of personal data, freedom of expression, freedom of association, as well as, indirectly, freedom from arbitrary arrest and detention, or the right to life'.[120] A nexus between export control and these civil and political rights may be readily understood. For instance, the use of equipment to intercept individuals' mobile telecommunications directly interferes with the right to privacy.

Less recognisable, however, is the possible long-term and indirect impact of export control on economic and social rights. Cyber technology is no doubt an indispensable part of economic and social development and, in this sense, lays the foundation for the better realisation of economic and social rights in the long term. Consider, for instance, the multifaceted roles of intrusion software. To obtain such a device may be necessary not only for governments, but also for private entities, in order for them to develop technologies to avoid intrusion. Building robust data security systems creates a sound basis for business and private communications, which, in turn, creates better conditions for realising economic and social rights in the long run. While it is methodologically difficult to identify a concrete linkage between the control of digital exports and the economic and social conditions of destination countries, it is undeniable that digital technologies sustain secure business transactions and create economic opportunities. To strengthen the export control of cyber surveillance items may thus give rise to a normative tension between the protection of certain civil and political rights in the short term and the development of economic and social rights in the long term.

These multifaceted connections between digital technologies and human rights have been raised by DIGITALEUROPE, albeit in order to arm the voice of the digital industry. According to DIGITALEUROPE, while digital technologies 'may be used to violate human rights', such technologies also help people 'more fully realize their human rights', including economic, social and cultural rights that improve access to health and education.[121] Although the industry's contestation may well be motivated by economic incentives, it is indeed true that cyber technologies are critical in sustaining both civil and political rights and economic and social rights.

The intricate relationships between the export control of cyber surveillance technology and human rights risks, as well as the tension within human rights norms, have been somewhat overlooked in the process of the European Commission's initiatives to modernise dual-use export control. This is ironic precisely because the EU's discussion on human rights-based export control was introduced via the concept of 'human security' referred to in the Commission's Communication in April 2014.[122] Human security is a broad concept, which aspires to achieve not only 'freedom from fear', but also 'freedom from want'.[123] The use of the concept of human security was quickly abandoned in the process of modernising export control, presumably to avoid the concept's all-encompassing character and resulting uncertainties. At the same time, the deliberation at the level of the EU also substantially departs from human security's holistic approach, in that political priority was clearly given to 'freedom from fear' and, more specifically, the protection of a set of civil and political rights. While the use of cyber surveillance technologies immediately puts such rights in a vulnerable position, it must be acknowledged, at the same time, that the reform of export control was directed to the protection of a particular set of human rights and that there might be adverse consequences for some other dimensions of human rights protection. This is not to suggest that the immediate consequence for civil and political rights of allowing the use of surveillance technologies is comparable to a much more indirect impact of refraining from the export of such technologies on economic and social rights. What ought to be recognised, however, is the fact

[120] European Commission 'Proposal' (28 September 2016) (n 30) 6.
[121] DIGITALEUROPE (24 February 2017) (n 101) at 4.
[122] European Commission, 'The Review of Export Control Policy' (n 23) 6.
[123] 2005 World Summit Outcome, UN Doc A/RES/60/1 (24 October 2005), para 143.

that the debate on rights-based control involved the prioritisation of certain categories of human rights. Such prioritisation may need to be more explicitly justified in the EU's efforts to integrate human rights norms in its export control regimes.

7. Conclusion

The use of cyber technology often entails a trade-off, and so does the export of the technology to third countries. Cyber surveillance technology could be used in such a manner that undermines human rights, especially the right to privacy and the freedom of expression. The Arab Spring captured public interest regarding the interlinkages between, on the one hand, the export of surveillance technology and, on the other hand, the infringement of fundamental freedoms in countries of destination. The European Commission's proposal submitted in September 2016 is normatively consistent with the EU's commitment to respect human rights and fundamental freedoms in its external action.

At the same time, debates surrounding the proposal reveal some of the obstacles which hinder the integration of human rights norms in the EU's external action, especially in circumstances where a wide range of the EU's business sectors are affected. There are already a number of international guidelines, including the UN Guiding Principles for Business and Human Rights, that expect corporations to take into account human rights and conduct human rights due diligence. At the level of an abstract and general tenet, few may openly contest the importance of human rights considerations in business operations, including those abroad. Nevertheless, the debates surrounding the reform of dual-use export control shed light on a great deal of hesitation on the part of corporations and governmental authorities to situate private business entities as assessors of human rights risks. Concerns have been raised that companies are not in a position to predict the risks of their products when they are exported abroad. Thus, despite the maturity of the 'business and human rights' narrative at the international, EU and domestic levels, many exporters find it uncomfortable to play the role of human rights guardians in their day-to-day operations. Such hesitation can occur not only in the context of export control but potentially in many other contexts of the EU's external action.

Overall, the deliberation surrounding the Commission's proposal to reform the EU's dual-use export control is a necessary process to incrementally integrate human rights norms into the EU's international trade law and policies. The proposal for rights-based export control created deliberative space in which governmental officials, politicians, business leaders from various industrial sectors, human rights NGOs, academics and other stakeholders discuss the degree to which human rights should and could be accommodated in dual-use export control practices. Despite differences in opinion, the fact that stakeholders are considering the practical application of 'business and human rights' beyond rhetoric is a significant step forward. After all, the deliberation surrounding the Commission's proposal has already generated greater awareness on this important front. Namely, each decision to grant a licence entails a normative choice among competing demands and such a choice has consequences in some other part of the world.

Declarations and conflict of interests

The author declares no conflicts of interest.