5 Normative market Europe?

The contested governance of cyber-surveillance technologies

Maximiliano Vila Seoane

Introduction

From 2011, the Arab Spring conveyed a beacon of hope for the potential democratisation of the region. However, journalists have unveiled that cyber-surveillance technologies, in many cases of European origin, played a key role in facilitating espionage on activists, which led to their interrogation and torture, such as in Bahrain (Arabian Business 2011). This and other examples have shed light on a shady aspect of the Fourth Industrial Revolution (see Introduction of this book), which opened the door to increased levels of surveillance. Although the contradiction between Western countries' allegiance to the defence of human rights, while exporting weapons to states that violate them is not new (Blanton 2000; Fuhrmann 2008; Yanik 2006), these incidents with digital technologies exposed a highly problematic double-speak by the European Union (EU), which claims to promote and protect human rights. Indeed, in the face of this inconsistency, the international dimension of the Cybersecurity Strategy of the European Union (2013) outlined the vision of promoting fundamental rights and freedoms in cyberspace, for instance, by monitoring the exports of cyber-surveillance technologies. In the same line, in 2014, the European Parliament (EP), European Commission (EC) and Council of the EU stated their intention of reviewing the Regulation (EC) No. 428/2009, which governs the control of exports of dual-use items. In 2016, the European Commission made public its proposal for updating the Union's regime for the 'control of exports, transfer, brokering, technical assistance and transit of dual-

use items' in order to include the regulation of cyber-surveillance technologies. This proposal takes a normative stance on what type of trade is desirable and lawful. Yet, the policy process of this regulation has been very contested by companies as well as some member states, which have put into question whether the EU can actually govern cyber-surveillance technologies in line with its Charter of Fundamental Rights.

The challenge that the EU confronts is part of the broader problem of regulating dual-use technologies. During the Cold War, these were defined as those that could be employed both for military and civilian uses, but since then, its definition has become broader in scope (Rath, Ischi and Perkins 2014). Indeed, new non-state actors and new dual-use technologies have made the debate more complex, such as the rise of biotechnologies (see Rychnovská, Chapter 10 and Farrand, Chapter 12 in this book) that led to the fear from bioterrorism and bioweapons, inspiring an academic literature investigating the challenges posed by the potential misuse of life sciences' knowledge by varied actors (Atlas and Dando 2006; Miller and Selgelid 2007; Rychnovská 2016). The rise of cyberweapons, a concept that includes cyber-surveillance technologies, adds a new chapter to these ongoing debates. Researchers believe that the governance of cyberweapons will be very difficult to implement in practice due to a number of specificities. First, cyberweapons are seen as important instruments in the arsenals of states, which would consequently be unwilling to limit their production (Stevens 2018). Second, authorities have far less choke-points to limit the proliferation of cyberweapons in comparison to nuclear or biological weapons (Lin 2016: 134). In effect, the skills and infrastructure to develop them are in general quite easy to access online and, thus, are hard to regulate (Lin 2016: 136). Third, in contrast to other dual-use items, cyber-surveillance technologies are easier to acquire, whether for commercial, personal or security reasons. For instance, firms selling spyware to snoop on loved ones or children, offer similar functionalities to those sold to states' security agencies (Brewster 2017). Therefore, the boundary between legitimate uses of cyber-surveillance technologies and malicious ones is far blurrier than with other dual-use items.

Despite the mistrust on the possibility of governing cyber-surveillance technologies, the EU's proposal assumes that it can overcome such challenges by updating the rules regulating the export of dual-use items. This EU's proposal has inspired a policy-oriented literature that explores its strengths and weaknesses (Alavi and Khamichonak 2016; Bohnenberger 2017; Kanetake 2019; Lavallée 2018). Yet, a more

theoretical analysis of these processes has lagged behind. In particular, the dual-use items regulation proposal speaks directly to the debates on the EU's identity as a global power, since many members of the European Parliament advocating for the initiative assume that the adoption of stringent rules on such trade may shape global norms. In other words, they believe that the EU should be a normative power in cyberspace (Manners 2002, 2006), shaping global norms on what type of trade is considered 'good'.

By examining the contested process of governing cyber-surveillance technologies in light of the 'EU as a Power' debates (Damro 2012, 2015; Manners 2002, 2006; Young 2015), this chapter departs from the explanations that cyber-surveillance technologies are very difficult to regulate (Bohnenberger 2017; Lin 2016; Stevens 2018), or the counter view, that the EU will inevitably succeed given its allegiance to protecting human rights. Instead, this chapter adopts the Normative Market Europe (NME) approach to argue that, despite an initial approach by the European Commission and the European Parliament to uphold human rights in the export of cyber-surveillance technologies in the new regulation, the final outcome has been contested and the possible result will be far more limited due to the influence of the private sector in the Council of the EU's negotiating position.

The chapter proceeds as follows. First, it introduces the Normative Market Europe approach, which synthesises two important contending perspectives to understand the specific features of the EU as a global power: Normative Power Europe and Market Power Europe. Second, it characterises the specificities of cyber-surveillance technologies and then, analyses the EU proposal to update its regime for the export of dual-use items. Afterwards, it discusses the different policy preferences and interests shaping it, followed by the intergovernmental divisions at the Council of the EU. Finally, it concludes, stressing the challenges for the implementation of the EU's proposal to govern cyber-surveillance technologies.

Normative market Europe as a conceptual framework

The European Commission's proposal to update the dual-use items regulation is an example of the interface between security and trade (Gebhard and Norheim-Martinsen 2011), which cannot be understood as being separate from the ongoing debates on the *sui generis* character of the EU as an international actor. In particular, in order to examine the

EU's governance of cyber-surveillance technologies, this chapter employs a Normative Market Europe (NME) approach, which is a synthesis of the Normative Power Europe (NPE) and the Market Power Europe (MPE) perspectives.

As regards the former, it was proposed by Manners (2002), who argued that after the Cold War, the EU's global influence derives from setting and disseminating norms to influence the international order, rather than by accumulating military or economic strength. Thus, NPE went beyond the previous (neo)realist understanding that mainly military power matters, or Duchêne's (1972) argument that the EU is a new type of civilian power in world politics. Instead, Manners identified five core norms that the EU aims to disseminate: peace, liberty, democracy, rule of law and respect for human rights and fundamental freedoms (Manners 2002: 242). According to Manners (2006), such normative power is precisely what is needed to overcome the destructive inter-state competition that characterised previous centuries. Despite its important contribution, NPE has not been exempt of criticism, for instance, for having a clear-cut division between norms and interests (Erickson 2013; Youngs 2004), or for neglecting the importance of non-state actors (Diez 2013). Thus, other approaches have been proposed to address such shortcomings.

The MPE is one such alternative conceptual framework (Damro and Friedman 2018; Damro 2012, 2015) that, in contrast to the NPE, suggests that the key feature of the EU as a global power is its capability to externalise its market-related policies beyond its borders, influencing other actors in the process. This derives from the fact that the European Single Market is one of the largest in the world, thus, its regulations have considerable external impact. In contrast to NPE, MPE does not accept an exceptional character for the EU's identity based on a specific set of norms written in its founding documents. Instead, it proposes a general framework, valid to empirically investigate any type of market power attempting to externalise its internal regulations, such as the USA or China. For this objective, it proposes to examine three dimensions (Damro 2012, 2015). First, the market size of the actor under analysis, assuming that the larger its size the greater its international influence is after setting a regulation. Second, the institutional features characterising the regulatory actor (Damro 2012), such as the varied types of stakeholders and networks that are part of the EU's processes of setting regulations, including EU member states and institutions, like the European Commission, the European Parliament, the Council of the EU,

the decision-making rules and the EU's regulatory capacity. Third, interest contestation (Damro 2015: 1343), which considers the various types of pressures that different actors or coalitions (both internal and external to the market power) might put on its policy processes and its potential externalisation.

It is important to observe that MPE can include a normative aspect as well. Indeed, the outcomes of the interest contestation process might arrive to a particular normative consensus. Thus, MPE should not be seen as merely a reductionist economic approach. For this reason, instead of thinking of the NPE and MPE as mutually exclusive, Geeraert and Drieskens (2017) speak of Normative Market Europe, since, in their view, elements of both approaches can be identified in practice. For example, by analysing the case of international sports governance, they argue that the EU's external actions are always grounded on normative intentions. However, its success depends on the particular institutional features and interest contestation processes that arise in the specific norms under study, which define whether the EU acts or not in a normative way (Geeraert and Drieskens 2017: 89). In particular, they incorporate in their analysis the internal cohesiveness of member states as the key variable determining whether or not the externalisation of a market regulation might take place (Da Conceição-Heldt and Meunier 2014; Geeraert and Drieskens 2017).

The rest of the chapter shows how the NME approach helps to understand the challenges faced by the proposal to update the EU's dual-use items regulation to incorporate cyber-surveillance technologies.

Cyber-surveillance technologies and the EU's proposal for their regulation

Surveillance technologies are not new (Privacy International 2016: 16), but their scale and thoroughness in the contemporary digital era is far more intense than before (Ball, Haggerty and Lyon 2014). This justifies the use of the new concept of cyber-surveillance technologies, which, although it does not have an internationally agreed upon definition (Bromley *et al*. 2016: 143; SIPRI and ECORYS 2015: 40), conveys the idea that they facilitate new types of accessing and/or manipulating digital data in illegal and/or non-consented ways, violating different human rights, namely, freedom of expression and the right to privacy, which affects other rights, like freedom of assembly and association.

Hence, the definition of cyber-surveillance technologies is usually list-based, for example, Bromley *et al.* (2016: 41) include the following technologies: mobile telecommunication interception equipment, intrusion software, IP network surveillance, monitoring centres, lawful interception systems, data retentions systems, digital forensics, probes and deep packet inspection. This approach can incorporate new technologies in the future, but it may also erroneously conflate very different types under a same category.

Cyber-surveillance technologies are developed by firms of different types, including large military contractors, big IT firms and also specialised SMEs (SIPRI and ECORYS 2015: 151), which sell to both military and civilian markets (see the Introduction of this book). These firms are located in countries that have a strong IT industry, such as the USA, UK, China, Germany, Israel, Italy and Russia. Privacy International (2016) identified 528 firms selling modern electronic surveillance technologies globally.[1] Although the USA has the largest amount of firms (122), as a whole, Privacy International (2016) reports that the EU has far more (279), distributed in 23 out of its 28 member states, that is, UK (104), France (45), Germany (41), Italy (18), Sweden (9) and Ireland (8). Thus, the EU represented more than 50 per cent of the market size of cyber-surveillance technologies acknowledged in the database. If the governance of biotechnologies puts a lot of focus on the community of scientists, their knowledge and facilities (Atlas and Dando 2006), these numbers also suggest that the proliferation of cyber-surveillance technologies could be curtailed significantly by regulating the firms specialising in their production. Notwithstanding, there is an illegal global market for zero-day vulnerabilities, which are errors in software unknown to its manufacturer and users (Stevens 2018). This is highly problematic because its suppliers are not always firms operating legally (Stockton and Golabek-Goldman 2013) and, thus, exist outside of any type of regulation.

In 2016, the EC made public its proposal for updating the Union's dual-use items regulation, which was based on different inputs from stakeholders and impact assessments, putting forward a number of key modifications, among which this chapter stresses two.

First, the proposal changed the definition of dual-use items in order to include a sub-item considering cyber-surveillance technologies that could be used to violate human rights, thus, incorporating a 'human security' perspective to the pre-existing military versus civilian definition of dual-use items. Second, the proposal adds new instruments

to regulate cyber-surveillance technologies such as an EU autonomous control list of technologies not considered at the multilateral level (European Commission 2016) and an EU harmonised 'catch-all' clause that would allow the addition of new items to the control list if there is proof that they are being used for human rights violations (European Commission 2016). In this way, technologies will be regulated without depending on a long negotiation process to update the control list. In line with social constructivist strands of Science and Technology Studies (STS) (Bijker 1995; Kline and Pinch 1996), these regulations can be understood as an attempt to socially shape the trade and use of cyber-surveillance technologies. In effect, the introduction of such a 'human security' approach in the legislation understands that there may be 'legitimate' uses for such cyber-surveillance technologies, but also that there may be other aims which are quite reprehensible that they require considerable limits to its export.

Nonetheless, the ordinary legislative process at the EU requires that the passing of a new or updated regulation proposed by the EC must be approved both by the EP and the Council of the EU. This specific institutional feature of the EU permits interest contestation. Indeed, the next sections detail how during the initial phases of the policy process, the EC and the EP advocated for a 'value-based trade policy' in crafting the new EU's proposal, rooted in the market size of Europe in dual-use items. Although this initial policy preference has not been without disagreements and setbacks, the discussion at the Council of the EU shows far more contentious positions among governments, with many siding with the private sector, posing a serious challenge to the new normative positions that the EC and EP have agreed upon.

The main actors and their policy preferences

As we will quickly show, the EC, the EP and the Working Party on Dual-Use Goods of the Council of the EU, together with multiple stakeholders from the private sector and civil society have been the key actors shaping the outcome of the policy process to update the Dual-Use Regulation. It is relevant here to highlight their tools and relations as well as their emerging practices to better understand what is at stake. On the one hand, the EC and Members of the European Parliament (MEP), together with civil society organisations defending human rights in the digital space have been the main actors advocating stricter regulations for the export of cyber-surveillance technologies. Besides upholding their

position in the ordinary legislative process, civil society organisations have released leaks to expose the double-speak of member states and the private sector. However, the policy process has also been moulded by the preferences of firms, which have been able to influence member states at the Council towards a negotiating position against new regulations for cyber-surveillance technologies.

With its proposal, the European Commission (2016) aims to protect human rights globally, while keeping a balance with the security and trade interests of the Union. Indeed, Cecilia Mälstrom, the EU trade commissioner, said that '… the introduction of a human security dimension that explicitly incorporates human rights into export controls reflects our commitment to a true value-based trade policy' (European Parliament 2018). This statement repeats the position of the "Trade for All" communication (European Commission 2015), which stresses the importance of trade policy for advancing the EU's interests and values, reinforcing development and foreign policies. Likewise, the EU's Cybersecurity Strategy stresses the importance of protecting fundamental rights and freedoms in cyberspace (European Commission 2013). Therefore, the EC understands that regulating Europe's market of cyber-surveillance technologies can shape the global regulation of such dual-use items in line with the protection of human rights.

The MEPs largely shared the Commission's proposal. In effect, after introducing amendments to the EC proposal, in 2018, the majority of the MEPs voted in favour of starting the Trilogue negotiations – 571 in favour, out of 629 votes (Stupp 2018). Two of the most vocal policy entrepreneurs in the review process have been: Klaus Buchner, the German rapporteur from the Green European Free Alliance, who was in charge of coordinating the proposal at the EP Committee on International Trade, and Marietje Schaake, Dutch shadow rapporteur from the Alliance of Liberals and Democrats for Europe Party, who has been very outspoken since the Arab Spring to update the EU's dual-use export control regime. Indeed, she has maintained that if European firms keep on facilitating human rights violations through their exports of cyber-surveillance technologies, they will damage the credibility of the EU's foreign policy to protect human rights (Schaake and Vermeulen 2016: 83). Likewise, updating the regulation is also important in terms of national security, since the export of cyber-surveillance technologies may pose a security risk to European firms and citizens abroad (Schaake and Vermeulen 2016: 82). The following fragments of Schaake's (2018)

speech at the EP before voting for the proposal are illustrative of the consensus reached by MEPs:

> The billion-euro commercial market in ready-made surveillance systems remains largely unregulated. And that is astonishing in light of the capabilities that companies and surveillance, hacking and exfiltration technologies are further and further developing. While many politicians claim to be concerned with cybersecurity, anyone who can afford it can buy systems that collect massive amount of data, can break into people's devices without the consent of the user, and information can be removed unnoticed. This is unacceptable, and as I said, regulation lags behind. The digital surveillance market should worry us in Europe. But the consequences of exports to dictatorships, where the rule of law are absent, are even more grave and unacceptable. […] It is taken long for EU action, but I am very glad we found broad consensus to update the dual use regulation that would tackle this toxic trade with targeted measures on the basis of human security. Surveillance systems will require licenses before exports, human rights will become clear criteria to assess before a license is granted, and definitions will be clear so that private sector will not suffer or be hindered unnecessarily, and we in turn count on their cooperation.
>
> (Schaake 2018)

This statement is in line with the idea of NPE, since it identifies a global problem caused by the unregulated market of cyber-surveillance technologies, where the EU could intervene by protecting human rights and fundamental freedoms, which is one of the norms identified in the NPE approach (Manners 2002: 243).

This main policy preference was influenced by the demands of a coalition of actors from civil society, the Coalition Against Unlawful Surveillance Exports (CAUSE),[2] that, in 2015, distributed a report that advanced many of the initiatives that would later appear in the first EC proposal. For instance, it requested a stricter evaluation of the potential end-user of cyber-surveillance technologies, together with an exempt of encryption technologies and other defensive legitimate uses (CAUSE 2015: 16). Furthermore, CAUSE (2015) criticised regulating cyber-surveillance technologies through the Wassenaar Arrangement (WA), because it preserves the Cold War logic of considering dual-use items as either for military or civilian purposes, a division not well suited for cyber-surveillance technologies. Accordingly, CAUSE preferred a unilateral regulation by the EU, which, if successful, should then become

the base for shaping global norms at the multilateral level through the WA, where it has 28 out of 41 members (CAUSE 2015: 15).

Corporate actors have been critical of the EC proposal even before it was made public. Due to its lobbying efforts (Stupp 2016), the proposal of the Commission released in 2016 excluded a number of technologies[3] from the autonomous list that firms considered to be too broad. Not surprisingly, even after this 'success', they still disputed many of the main amendments introduced in the EP's final proposal. Take the case of Digital Europe,[4] that still disapproved of the definition of cyber-surveillance technologies as being too ambiguous and broad, and opposed a unilateral European definition of dual-use items that would depart from the coordinated one with other multilateral arrangements (Digital Europe 2017: 2). Digital Europe also understands that a 'catch-all' control based on the potential misuse of cyber-surveillance technologies to harm human rights is a 'disproportionate measure' (Digital Europe 2017: 2), which exceeds the capabilities of the private sector to assess the end-user. Instead, they believe that states should make such judgements. These criticisms reveal the preference of the European digital industry for preserving the usual military versus civilian division of understanding dual-use items and rejecting the incorporation of extra human rights criteria in the regulation (Kanetake 2019). In their view, the new proposal would only harm the European digital industry, since buyers would still be able to obtain surveillance technologies from other less regulated markets (Digital Europe 2017: 4). Hence, they oppose the main changes introduced by the EC and the EP, undermining the intended update of the regulation to govern cyber-surveillance technologies. Although the corporate sector was unsuccessful in including all these claims during the discussion at the EP, the situation changed at the Council of the EU.

Intergovernmental divisions at the Council of the EU

Despite the fact that the contestation of interests at the EP sided with a normative approach, stark divisions have emerged among member states during the negotiations at the Council of the EU, which seriously put into question whether or not the new additions for the governance of cyber-surveillance technologies will remain.

Leaks of documents from the German delegation, which has taken the lead in regulating cyber-surveillance technologies, revealed strong

opposition by other states to the introduction of a catch-all clause and a specific European autonomous list for cyber-surveillance technologies. Indeed, on 28 January 2018, Germany, France and other groups of countries, released a document to the Working Party on Dual-Use Goods, to start negotiating a common position vis-à-vis the proposal voted at the EP. In contrast to the legislation received from the EP, this document says '… there is no need for additional catch-all controls' (Moßbrucker 2018), a neglect in line with the demands of the BDI (2017), the influential Federation of German Industries .The leaks suggest that excluding the catch-all clause was a concession to states opposing all new measures in order to reach a compromise that would have at least led to an EU autonomous list of cyber-surveillance technologies (Moßbrucker 2018).

However, even after this concession, unwavering opponents (Cyprus, Czechoslovakia, Estonia, Finland, Ireland, Italy, Poland, Sweden and the United Kingdom) to the new regulation gave additional reasons for rejecting an EU-autonomous list. Among the most relevant arguments, they expressed that:

> For EU companies, the EU-autonomous list would mean they were no longer operating on a level playing field in the global market, where sustained competitiveness is key for survival. Related to the issue of level playing field, it is important to point out that the effect of EU-only controls would be symbolic rather than preventative: those seeking cyber-surveillance technology have no shortage of non-EU vendors from which to choose. While EU industry has strengths in this area, it is far from having a global majority market share on high-end technology in the rapidly developing cyber-security sector. Controls on EU exports without parallel measures in the other major economies would serve only to push the development and production of relevant technologies outside of the EU.
>
> (Moßbrucker 2018)

This quote again echoes the position of the European cyber industry. Likewise, the countries opposing the EU autonomous list stressed the fact that the EU has always complied strictly with international regimes and should not do otherwise in this case. Therefore, they disapprove of taking a unilateral approach to govern cyber-technologies (Moßbrucker 2018).

Finally, in July, the Council of the European Union (2019) released its negotiating position, which deleted all the new proposals introduced by

the EC and the EP to regulate cyber-surveillance technologies (Moßbrucker 2019). This document confirms that the member states – including Germany – finally sided with the policy preference of the private sector. Indeed, the BDI (2019) welcomed the rejection of the catch-all clause and specific treatment for cyber-surveillance technologies. Contrarily, Klaus Buchner criticised the fact that no effective tools were included to regulate cyber-surveillance technologies, exhibiting that 'Industry has done a great job' (Buchner 2019).

After initiating the move in 2015 to introduce stricter regulations for the export of cyber-surveillance technologies (Stupp 2015), it seems paradoxical that Germany also supported the Council's document. What explains such a reversal? The BDI has been an undeniable influence that criticised most of the additional measures to regulate cyber-surveillance technologies along the whole process. Yet, its success in shaping the policy preferences was contingent on the dynamics of German national politics. Actually, since 2013, Germany's government has been led by a grand coalition (*Große Koalition*) made up by the Christian Democratic Union (CDU), the Christian Social Union in Bavaria (CSU) and the Social Democratic Party (SPD). The pledge for a new regulation for cyber-surveillance technologies was initiated during the leadership of Sigmar Gabriel (SPD) at the Federal Ministry for Economic Affairs and Energy. However, after the 2017 German elections, a new Grand Coalition was formed, which in March 2018 assigned the Federal Minister for Economic Affairs and Energy to Peter Altmaier (CDU). This change coincides with the U-turn in the German negotiating position, suggesting the CDU's choice for defending the German industries' policy preferences. Indeed, Saskia Esken (SPD), member of the German Bundestag, asserted that 'The Federal Government has watered down the important initiative of our former Minister of the Economy Gabriel for the strict export control of digital dual-use goods and almost reversed it' (Meister 2018).

Overall, the Council of the EU has arrived to a negotiating position that expresses policy preferences in line with those of private industry. The exclusion of all the new additions proposed by the EC and the EP to advance with a human-rights-based approach to govern the trade of cyber-surveillance technologies presages a difficult Trilogue, which, in the worst case, may end up with no new measures to regulate such dual-use items (Moßbrucker 2019). Therefore, despite the initial normative inclination of the regulation, the final outcome will possibly be steered by the European business preferences.

Conclusions

This chapter has explored the proposal to review the EU's regulation regime for dual-use items, in particular its aim to govern the exports of cyber-surveillance technologies, an industry in which many European firms have an edge. Two opposing trends have been detected. On the one hand, during the first phase of the discussions within the EC and the EP, a normative approach prevailed, which has introduced new restrictions on the exports of cyber-surveillance technologies to prevent their likely misuse to harm human rights. Indeed, the institutional features of the EU allowed the advancement of these normative policy preferences, initially advocated by civil society actors and politicians defending human rights. On the other hand, the space for interest contestation in the EU's policy process has been stark at the Council of the EU, where, at first some states, but then all, have firmly opposed the most normative aspects of the proposal approved by the EP, mirroring the policy preferences of the European cyber industries. Accordingly, the new values-based proposals to govern cyber-surveillance technologies have been – so far – undermined.

In sum, this case sheds light on the EU's identity in governing new technologies, which seems to follow the NME approach. Indeed, in spite of a usual initial attempt to regulate new technologies in line with the Union's fundamental values, whether or not it succeeds, depends on the interest contestation that takes place during the policy process. Concomitantly, this depends on whether or not there is internal cohesiveness among member states to advance with such a normative position. Otherwise, as this case shows, the preferences of the private sector may influence the Council of the EU far from a stance that may threaten its interests. Despite the importance of the review to update the regulation to tackle new risks to human rights, these political challenges do not indicate an easy future for a human-rights-based approach to govern cyber-surveillance technologies at the EU. Nonetheless, they do show that its governance is possible, though highly dependent upon a new political consensus among member states.

Notes

1 It is worth pointing out that the NGO explains that the number of firms from China and Russia might be understated.

2 The critical report was composed by Amnesty International, Digitale Gesellschaft, FIDH, Human Rights Watch, Open Technology Institute, Privacy International, Reporters without Borders and Access.

3 The proposal of the Commission released in 2016 excluded a number of technologies, specifically: biometrics, location tracking devices, probes and deep packet inspection (DPI) systems were removed from the leaked draft version of the Commission's proposal.

4 Digital Europe represents the most important corporations and national associations of the European digital industry.

References

Alavi, H. and Khamichonak, T. (2016) A European Dilemma: The EU Export Control Regime on Dual-Use Goods and Technologies. *DANUBE: Law and Economics Review* 7(3): 161–172. DOI: 10.1515/danb-2016-0010.

Arabian Business (2011) Western Spy Tools Aid in Crackdown on Arab Dissent. At: www.arabianbusiness.com/western-spy-tools-aid-in-crackdown-on-arab-dissent-417624.html (accessed 10 July 2018).

Atlas, R.M. and Dando, M. (2006) The Dual-Use Dilemma for the Life Sciences: Perspectives, Conundrums, and Global Solutions. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 4(3): 276–286. DOI: 10.1089/bsp.2006.4.276.

Ball, K., Haggerty, K.D. and Lyon, D. (eds) (2014) *Routledge Handbook of Surveillance Studies*. Paperback. London: Routledge.

BDI (2017) EU Dual-Use Reform: EC Proposed Regulation COM(2016). April. Berlin, Germany: Bundesverband der Deutschen Industrie e.V. At: https://english.bdi.eu/media/user_upload/20170401_BDI-Positioning_Dual_Use_Reform_Proposal.pdf.

BDI (2019) EU-Dual-Use Regulation: Council Mandate. At: https://e.issuu.com/embed.html?d=20190903_bdi_position_dual-use_en_final&hideIssuuLogo=true&u=bdi-berlin.

Bijker, W.E. (ed.) (1995) *Of Bicycles, Bakelites and Bulbs: Toward a Theory of Sociotechnical Change*. Cambridge, MA: The MIT Press.

Blanton, S.L. (2000) Promoting Human Rights and Democracy in the Developing World: U.S. Rhetoric versus U.S. Arms Exports. *American Journal of Political Science* 44(1): 123–131. DOI: 10.2307/2669298.

Bohnenberger, F. (2017) The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls. *Strategic Trade Review* 3(4): 81–102.

Brewster, T. (2017) Meet the 'Cowboys of Creepware' – Selling Government-Grade Surveillance to Spy on Your Spouse. At: www.forbes.com/sites/thomasbrewster/2017/02/16/government-iphone-

android-spyware-is-the-same-as-seedy-spouseware/#1d828bcf455c (accessed 18 August 2018).
Bromley, M., Steenhoek, K.J., Halink, S. *et al*. (2016) ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns. *Strategic Trade Review* 2(2): 37–52.
Buchner, K. (2019) Europäischer Rat veröffentlicht Position zu Handel mit Überwachungstechnolgie (Dual-Use). At: https://klaus-buchner.eu/europaeischer-rat-veroeffentlicht-position-zu-handel-mit-ueberwachungstechnolgie-dual-use/ (accessed 23 September 2019).
CAUSE (2015) *A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation*. June. Coalition Against Unlawful Surveillance Exports.
Da Conceição-Heldt, E. and Meunier, S. (2014) Speaking with a Single Voice: Internal Cohesiveness and External Effectiveness of the EU in Global Governance. *Journal of European Public Policy* 21(7): 961–979. DOI: 10.1080/13501763.2014.913219.
Council of the European Union (2019) Proposal for a Regulation of the European Parliament and of the Council Setting Up a Union Regime for the control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (recast) – Mandate for Negotiations with the European Parliament. At: www.consilium.europa.eu/media/39555/mandate-for-negociations.pdf.
Damro, C. (2012) Market Power Europe. *Journal of European Public Policy* 19(5): 682–699. DOI: 10.1080/13501763.2011.646779.
Damro, C. (2015) Market Power Europe: Exploring a Dynamic Conceptual Framework. *Journal of European Public Policy* 22(9): 1336–1354. DOI: 10.1080/13501763.2015.1046903.
Damro, C. and Friedman, Y. (2018) Market Power Europe and the Externalization of Higher Education: MPE and the Externalization of Higher Education. *JCMS: Journal of Common Market Studies* 56(6): 1394–1410. DOI: 10.1111/jcms.12749.
Diez, T. (2013) Normative Power as Hegemony. K. Nicolaïdis and R.G. Whitman (eds), *Cooperation and Conflict* 48(2): 194–210. DOI: 10.1177/0010836713485387.
Digital Europe (2017) Brussels, Belgium: Digital Europe. At: www.digitaleurope.org/wp/wp-content/uploads/2019/01/FINAL%20-%20DIGITALEUROPE%20paper%20on%20recast%20regs%20dual%20use[1].pdf.
Duchêne, F. (1972) Europe's Role in World Peace. In R. Mayne (ed.), *Europe Tomorrow: Sixteen Europeans Look Ahead*. London: Fontana, 32–47.
Erickson, J.L. (2013) Market Imperative Meets Normative Power: Human Rights and European Arms Transfer Policy. *European Journal of International Relations* 19(2): 209–234. DOI: 10.1177/1354066111415883.
European Commission (2013) European Commission and High Representative of the European Union for Foreign Affairs and Security Policy Cybersecurity

Strategy of the European Union: an Open, Safe and Secure Cyberspace. At: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

European Commission (2015) Trade for All: Towards a More Responsible Trade and Investment Policy. At: http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf.

European Commission (2016) 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). 28 September. Brussels, Belgium. At: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0616.

European Parliament (2018) Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Debate). At: www.europarl.europa.eu/doceo/document/CRE-8-2018-01-16-ITM-014_EN.html?redirect.

Fuhrmann, M. (2008) Exporting Mass Destruction? The Determinants of Dual-Use Trade. *Journal of Peace Research* 45(5): 633–652. DOI: 10.1177/0022343308094324.

Gebhard, C. and Norheim-Martinsen, P.M. (2011) Making Sense of EU Comprehensive Security Towards Conceptual and Analytical Clarity. *European Security* 20(2): 221–241. DOI: 10.1080/09662839.2011.564613.

Geeraert, A. and Drieskens, E. (2017) Normative Market Europe: The EU as a Force for Good in International Sports Governance? *Journal of European Integration* 39(1): 79–94. DOI: 10.1080/07036337.2016.1256395.

Kanetake, M. (2019) The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches. *Business and Human Rights Journal* 4(1): 155–162. DOI: 10.1017/bhj.2018.18.

Kline, R. and Pinch, T. (1996) Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States. *Technology and Culture* 37(4): 763–795. DOI: 10.2307/3107097.

Lavallée, C. (2018) The EU's Dual-Use Exports: A Human Security Approach? In Eva Pejsova (ed.), *Guns, Engines and Turbines. The EU's Hard Power in Asia*, Chaillot Papers (EUISS), November, 43–50. www.iss.europa.eu/sites/default/files/EUISSFiles/CP_149_Asia.pdf.

Lin, H. (2016) Governance of Information Technology and Cyber Weapons. In E.D. Harris (ed.), *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge, MA: American Academy of Arts & Sciences, 112–157.

Manners, I. (2002) Normative Power Europe: A Contradiction in Terms? *JCMS: Journal of Common Market Studies* 40(2): 235–258. DOI: 10.1111/1468-5965.00353.

Manners, I. (2006) Normative Power Europe Reconsidered: Beyond the Crossroads1. *Journal of European Public Policy* 13(2): 182–199. DOI: 10.1080/13501760500451600.

Meister, A. (2018) Reaktionen auf Dual-Use-Leaks: ‘Offenbarungseid der Bundesregierung’. At: https://netzpolitik.org/2018/reaktionen-auf-dual-use-leaks-offenbarungseid-der-bundesregierung/.

Miller, S. and Selgelid, M.J. (2007) Ethical and Philosophical Consideration of the Dual-use Dilemma in the Biological Sciences. *Science and Engineering Ethics* 13(4): 523–580. DOI: 10.1007/s11948-007-9043-4.

Moßbrucker, D. (2018) Überwachungsexporte: Bundesregierung stellt Industrie vor Menschen-rechte. *Netzpolitik.org*. At: https://netzpolitik.org/2018/ueberwachungsexporte-bundesregierung-stellt-industrie-vor-menschenrechte/.

Moßbrucker, D. (2019) EU States Unanimously Vote Against Stricter Export Controls for Surveillance Equipment. *Netzpolitik.org*. At: https://netzpolitik.org/2019/eu-states-unanimously-vote-against-stricter-export-controls-for-surveillence-equipment/.

Privacy International (2016) *The Global Surveillance Industry*. Privacy International. At: www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

Rath, J., Ischi, M. and Perkins, D. (2014) Evolution of Different Dual-Use Concepts in International and National Law and Its Implications on Research Ethics and Governance. *Science and Engineering Ethics* 20(3): 769–790. DOI: 10.1007/s11948-014-9519-y.

Rychnovská, D. (2016) Governing Dual-Use Knowledge: From the Politics of Responsible Science to the Ethicalization of Security. *Security Dialogue* 47(4): 310–328. DOI: 10.1177/0967010616658848.

Schaake, M. (2018) Plenary Speech on Update of the Dual-Use Regulation. At: https://marietjeschaake.eu/en/plenary-speech-on-update-of-the-dual-use-regulation (accessed 25 July 2018).

Schaake, M. and Vermeulen, M. (2016) Towards a Values-Based European Foreign Policy to Cybersecurity. *Journal of Cyber Policy* 1(1): 75–84. DOI: 10.1080/23738871.2016.1157617.

SIPRI and ECORYS (2015) Final Report for the European Commission. Data and Information Collection for EU Dual-Use Export Control Policy Review. At: http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154962.PDF.

Stevens, T. (2018) Cyberweapons: Power and the Governance of the Invisible. *International Politics* 55(3–4): 482–502. DOI: 10.1057/s41311-017-0088-y.

Stockton, P.N. and Golabek-Goldman, M. (2013) Curbing the Market for Cyber Weapons. *Yale Law & Policy Review* 32(1): 239–266.

Stupp, C. (2015) Germany Leaves Brussels Behind on Surveillance Tech Export Controls, Euractiv. At: www.euractiv.com/section/digital/news/germany-leaves-brussels-behind-on-surveillance-tech-export-controls/.

Stupp, C. (2016) Juncker Postpones Controversial Export Control Bill on Surveillance Technology. At: www.euractiv.com/section/trade-society/news/juncker-postpones-controversial-export-control-bill-on-surveillance-technology/.

Stupp, C. (2018) MEPs Approve Export Controls Tailored to Stop Government Surveillance. At: www.euractiv.com/section/cybersecurity/news/meps-approve-export-controls-tailored-to-stop-government-surveillance/.

Yanik, L.K. (2006) Guns and Human Rights: Major Powers, Global Arms Transfers, and Human Rights Violations. *Human Rights Quarterly* 28(2): 357–388. DOI: 10.1353/hrq.2006.0026.

Young, A.R. (2015) The European Union as a Global Regulator? Context and Comparison. *Journal of European Public Policy* 22(9): 1233–1252. DOI: 10.1080/13501763.2015.1046902.

Youngs, R. (2004) Normative Dynamics and Strategic Interests in the EU's External Identity. *JCMS: Journal of Common Market Studies* 42(2): 415–435. DOI: 10.1111/j.1468-5965.2004.00494.x.