GLOBAL EXPORT CONTROLS OF CYBER SURVEILLANCE TECHNOLOGY AND THE DISRUPTED TRIANGULAR DIALOGUE

HEEJIN KIM*

Abstract The proliferation and abuse of cyber surveillance technology is a global policy problem. The Wassenaar Arrangement is a central platform of international cooperation for regulating dual-use goods and technologies and the so-called 'cyber' amendments to Wassenaar have created a multilateral control mechanism for the export of cyber surveillance technology. Following criticism of the repressive use of ICT-powered surveillance tools supplied by private companies in the early 2010s, Wassenaar States revised the Arrangement to regulate certain types of surveillance. This article begins by examining key features of the cyber amendments. Based on the analysis of recent export control law reforms in the three leading State actors in the production, sales and governance of cyber surveillance technology—namely the United States, China, and the European Union—the article identifies the diminishing importance of the Wassenaar Arrangement. It also shows how approaches in the three jurisdictions diverge not only from the terms of equivalent Wassenaar controls, but also from one another. They all aim to become a stronger and more autonomous entity in the regulation of cyber surveillance technology. In the face of escalating confrontation between the G2 concerning emerging technologies, it will be interesting to see how the EU's turn to a more human rights-centred approach to governing the export of cyber surveillance technology will be received by the US and Chinese governments in the long run and how it will interact with export control reforms designed with competing geopolitical, commercial and security agendas.

Keywords: public international law, the Wassenaar Arrangement, cyber surveillance technology, intrusion software, network surveillance systems, Export Control Reforms Act, Export Control Laws of the People's Republic of China, EU Dual-Use Regulation.

* Cyber Security Law Fellow & Stream Lead, The Allens Hub for Technology, Law and Innovation, UNSW Faculty of Law and Justice, heejin.kim@unsw.edu.au. I thank Damian Chalmers, Lyria Bennett Moses, and Marija Jovanovic for their comments and suggestions on earlier drafts. I also appreciate the work of two anonymous peer-reviewers and the editorial members of the ICLQ. This work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme. Supports from my CSCRC colleagues were essential at various stages of conducting this research. Nicholas Parker kindly provided research assistance. All errors that remain are my own.

[*ICLQ* vol 70, April 2021 pp 379–415] doi:10.1017/S0020589321000105

I. INTRODUCTION

The use of commercially marketed cyber surveillance technology by authoritarian governments is a global policy problem.[1] Its impact is not confined to the countries where advanced surveillance techniques are employed to repress the population as it easily crosses borders.[2] Concerns about the export of cyber surveillance technology to governments with questionable human rights records and a weak(er) rule of law were initially flagged by human rights activists, and local struggles quickly became a global cause. By restricting the supply side of cyber surveillance goods and technologies, export control mechanisms can provide one of the few options to effectively regulate its availability and transfer.[3]

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ('the Wassenaar Arrangement') is currently the only international agreement that provides a transnational legal framework for restricting the export of surveillance equipment, software and expertise.[4] This scheme captures an extensive list of dual-use goods and technologies for which States agree to adopt export control laws, empowering licensing authorities to approve, reject and review their transfer. Cyber surveillance technology has been the most controversial addition to this list since its adoption in 1996. The so-called 'cyber'[5] amendments to Wassenaar adopted in the course of the 2010s had a significant impact on subsequent dual-use export reforms in many parts of the world, including the United States (US), China, and the European Union (EU), who assume leading roles in the production, sales and governance of cyber surveillance technology.

The essence of the Wassenaar Arrangement is a list of dual-use goods and technologies laying out the detailed technical attributes of the controlled items. As the control list itself does not contain substantive treaty obligations, it has been a widely shared practice for both member States like the US and non-member States such as China to use this list as a key reference point to develop and update their domestic export control systems. While the updates to Wassenaar have been closely reflected in the equivalent mechanisms at national and regional levels, the addition of cyber surveillance technology has changed this narrative of broad acceptance and impact. The cyber amendments are a test case examining the (in)ability of conventional export control mechanisms to address various risks associated with the rapid

[1] UNCHR, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Surveillance and Human Rights' (28 May 2019) UN Doc A/HRC/41/35 paras 1–6 at 3–4.

[2] State-led targeted surveillance is not always 'territorially contained'. ibid 16.

[3] M Bromley, K Jan Steenhoek, S Halink and E Wijkstra, 'ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns' (2016) 2 Strategic Trade Review 37, 38–9.

[4] List of Dual-Use Goods and Technologies and Munitions List, Compiled by the Wassenaar Arrangement Secretariat, Public Documents (Dec 2019) Vol II ('Wassenaar Dual-Use List').

[5] See Section III.C for the scope and features of the cyber amendments.

technological development in highly sensitive dual-use items such as cyber surveillance technology.

As analysed below, the US, China, and the EU all aim to become a stronger and more autonomous regulatory entity in the global export control regime, and prefer to tighten restrictions on the use and transfer of cyber surveillance technology. It has increasingly become apparent that Wassenaar implementation strategies in this area have been significantly disrupted. Based on the recent developments of export control laws in these three jurisdictions, this article argues that their regulatory approaches to the export of cyber surveillance technology diverge not only from the terms of equivalent Wassenaar controls, but also from one another. The new laws and control categories adopted as a result of nation (region)-wide dual-use export reforms are eroding the very foundations of international cooperation for a more effective control of cyber surveillance technology.

Export controls on cyber surveillance technology and Wassenaar implementation in this area have been of interest to many legal scholars and human rights groups. Yet, their approaches are country-(or region) specific, and mainly focus on legal developments in the West, overlooking relevant legal reforms by emerging actors in export control governance such as China.[6] There are also interesting projects evaluating the terms of cyber amendments, but many do not examine subsequent updates renegotiated by Wassenaar States.[7] This article not only fills the gap in existing literature regarding these aspects, but also provides a bigger picture of global regulatory divergence among national, regional and international approaches to governing cyber surveillance technology. The article examines the many

[6] See F Bohnenberger, 'The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls' (2017) 3 Strategic Trade Review 81; M Bromley, 'Export Controls, Human Security and Cyber-Surveillance Technology: Examining the Proposed Changes to the EU Dual-Use Regulation' (Stockholm International Peace Research Institute (SIPRI) December 2017); M Bromley and G Maletta, 'The Challenge of Software and Technology Transfers to Non-Proliferation Efforts: Implementing and Complying with Export Controls' (SIPRI April 2018); M Kanetake, 'The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches' (2019) 4 BHRJ 155; P Lichtembaum, DW Addis and DO Hindin, 'Cyber-Surveillance Export Control Reform in the United States' [2018] WorldECR 75; T Maurer, E Omanovic and B Wagner, 'Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age' (New America Foundation, Digitale Gestellschaft and Privacy International, March 2014) 5–26; SIPRI and Ecorys, 'Data and Information Collection for EU Dual-Use Export Control Policy Review' (Submission, European Commission for Impact Assessment, 6 November 2015).

[7] See C Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies' (Access March 2015); S Bratus, DJ Capelis, M Locasto and A Shubina, 'Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How to Fix It' (9 October 2014) <https://www.cs.dartmouth.edu/~sergey/wassenaar/wassenaar-public-comment.pdf>; I 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; J Ruohonen and KK Kimppa, 'Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity' (2019) 16 Journal of Information Technology & Politics 169.

reasons for such regulatory divergence. A simple explanation would be the institutional weakness of the Wassenaar Arrangement due to its nature as soft law. Wassenaar implementation primarily depends on national discretion. A more substantial explanation can be obtained from examining the context (beyond Wassenaar) in which the US, China, and the EU redesign their export control systems. In developing a global export control regime for cyber surveillance technology, neither the common geopolitical positions that sustained Cold War-style technology transfer restrictions, nor long-standing commitments shared amongst member States for collective non-proliferation can be restored in the short term.

Discussion of the repressive use of cyber surveillance technology dates back to the early 2010s.[8] In the aftermath of the Arab Spring that swept across the Middle East and North Africa, the private surveillance industry, which used to evade public scrutiny, was brought into the spotlight for the first time. There was a strong connection between surveillance products marketed by many Western companies and human rights violations in importing countries that used these products for repressive purposes. The Egyptian case involving UK-based Gamma International and its subsidiary Finfisher is one example. After the fall of Mubarak, it was revealed that the Egyptian authority had deployed FinSpy, the company's signature spyware, to monitor and track down human rights campaigners, political dissidents and journalists.[9] Covertly installed on target devices, FinSpy monitors calls, messages and file transfers. It can turn on a web cam or microphone in the user's device, record all the keystrokes on the computer, and extract passwords typed into different browsers and communication platforms. The use of Internet monitoring and filtering technology has also been widespread, blocking and monitoring tens of thousands of Internet domains, redirecting traffic to inject malware, and/or compromising high-profile international media outlets. Illicitly obtained information on targeted individuals was used to subsequently detain and/or torture them. Some of the well-established cases involve network surveillance systems installed and maintained by Amesys in Libya, Blue Coat in Iran and Syria, Sandvine in Egypt, and Trovicor in Bahrain during the same period.[10] These companies are headquartered in France, the US, Canada and Germany respectively.

[8] M Schaake, 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries' (Report, 2014/2232(INI), 3 June 2015) paras 15–21; adopted as the European Parliament Resolution of 8 September 2015.

[9] T Timm, 'Spy Tech Companies & Their Authoritarian Customers: Part I: FinFisher and Amesys' (Electronic Frontier Foundation, 16 February 2012).

[10] Citizen Lab, 'Some Devices Wander By Mistake: Planet Blue Coat Redux' (Citizen Lab, 9 July 2013); Electronic Frontier Foundation, 'Swedish Telcom Giant Teliasonera Caught Helping Authoritarian Regimes Spy on Their Citizens' (Electronic Frontier Foundation, 18 May 2012); Human Rights Watch, 'They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia' (Human Rights Watch, 25 March 2014); J Penny, S McKune, L Gill and RJ Deibert, 'Advancing Human Rights-By-Design In the Dual-Use Technology' (2018) 71 JIntlAff 103;

State-led surveillance programs have increased in an expanding variety of destination countries. New industry actors and products have appeared in the surveillance sector. For example, in 2015, the Hacking Team, a prominent Italian company, was the victim of a cyberattack that exposed 400 gigabytes of data containing its client lists, contracts, invoices and source codes.[11] Its flagship product, the Remote Control System (RCS), was supplied to 21 States spread over different regions, many of which were found to use RCS in ways that led to serious human rights violations. While a global web of companies of Western origins dominated the early surveillance industry, China is now at the forefront of the stage, globally exporting its surveillance equipment and know-how.[12] China has employed surveillance technology on a massive scale in the domestic realm. Thanks to State-sponsored surveillance projects and research programmes, a new generation of Chinese surveillance companies is on the rise. They have taken steps to disseminate nationally tested surveillance models overseas, marketing products not only to authoritarian and semi-authoritarian governments but also to liberal democracies.[13] Their commercial and technological presence is evident from their many new government clients in Africa and Central and Southeast Asia.[14]

The cyber amendments to Wassenaar marked a timely international response to numerous incidents showing how the repressive use of cyber surveillance technology has enabled serious human rights violations. The expansion of the Wassenaar list was welcomed with a hope that it would lead to more effective control of problematic end-uses and end-users of surveillance tools. There is strong approval for expanding the list even further to cover a broader range of cyber surveillance technology. The agreed-upon entries of goods and technologies introduced by the cyber amendments does not capture many other (new) surveillance items that are unlisted but can be exploited to cause grave threats to security and human lives. The narrowly defined list also

Privacy International, 'Open Season: Building Syria's Surveillance State' (Privacy International 2016); V Silver and B Elgin, 'Torture in Bahrain Becomes Routine with Help of Nokia Siemens' Bloomberg (23 August 2011); P Sonne and M Coker, 'Firms Aided Libyan Spies First Look Inside Security Unit Shows How Citizens Were Tracked' Wall Street Journal (30 August 2011).

[11] Citizen Lab, 'Mapping Hacking Team's "Untraceable' Spyware" (Citizen Lab, 17 February 2014).

[12] Many of these countries have also signed onto China's Belt and Road Initiative and its 'smart city' projects including mass surveillance program. See S Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 17 September 2019) 13–15; A Shahbaz, 'Freedom on the Net 2018: The Rise of Digital Authoritarianism' (Freedom House, 31 October 2018) 6–9.

[13] Feldstein, ibid 14; C Rolley, 'Is Chinese-Style Surveillance Coming to the West?' (Guardian 7 May 2019).

[14] D Cave, F Ryan and VX Xu, 'Mapping More of China's Technology Giants: AI and Surveillance' (Issues Paper Report No 24/2019, Australian Strategic Policy Institute (ASPI), 28 November 2019) 12–14; A Gwagwa, 'Exporting Repression? China's Artificial Intelligence Push into Africa' (Net Politics 17 December 2018); P Mozur, JM Kessel and M Chan, 'Made in China, Exported to the World: The Surveillance State' (The New York Times 24 April 2019); Shahbaz (n 12) 9.

cannot keep up with the rapid technological development in this area. In contrast, the private sector has voiced concerns over the overbroad control categories under Wassenaar. Many industry representatives and security researchers argued that export controls on the surveillance items as adopted in the control list would cripple legitimate cybersecurity research and hinder the information sharing necessary to identify and quickly counter cybersecurity threats.[15] Being at the forefront of developing and testing various cyber surveillance products, these stakeholders have lobbied their home governments to limit the scope and impact of Wassenaar implementation. Accordingly, difficult questions remain for States on how to tailor their export control regulations to address concerns about overreach without sacrificing the goal of addressing security threats and human rights concerns.

Against this backdrop, Part II clarifies the meaning of cyber surveillance technology and examines key features of the surveillance industry. Part III analyses three Wassenaar control classes created to regulate cyber surveillance technology. In Part IV, the article examines how leading State actors in the global surveillance industry and governance—namely the US, China, and the EU—have led their export control reforms. As Part IV shows, Wassenaar implementation strategies in this area seemed to work well initially, but eventually proved far less successful than implementing controls on many other Wassenaar-listed dual-use items. Finally, Part V summarises the analysis of how the US, China, and the EU differ in their approaches to regulating the export of cyber surveillance technology.

II. CYBER SURVEILLANCE TECHNOLOGY AS DUAL-USE ITEMS AND THE BOOMING GLOBAL SURVEILLANCE INDUSTRY

While there is no generally agreed definition of cyber surveillance technology, this term has been discussed among legal academics, practitioners and legislators in works examining surveillance goods and technologies as dual-use items.[16] This article uses the term 'technology' to encompass not only finished products of equipment and software, but also the provision of expertise required to create those items and facilitate their application. 'Cyber surveillance technology' can be understood as equipment, software and expertise used by intelligence and law enforcement agencies or by network operators acting under their direction to covertly monitor, exploit and/or analyse data that is stored, processed and transferred through ICT means.[17] It has civilian applications due to its ostensibly legitimate use such as law

[15] See Section III.C.2 and IV.A.1 for the backlash from the industry and academia.
[16] Bromley (n 6) 6–10; SIPRI and Ecorys (n 6) 143.
[17] The definition cannot be entirely static as new technologies are introduced to the market, and a wider variety of communications devices and networks are involved in actual surveillance operations.

enforcement and computer security projects, but can also be deployed to enhance military capabilities. ICT-powered surveillance tools can easily be used in the violation of the rights to privacy and freedom of expression and political association. Monitoring, collecting and disrupting individuals' communications through these tools can also lead to other human rights violations including arbitrary arrest and detention, torture and extrajudicial killings.

With exponential growth in the use of various Internet-based communication tools, individuals generate and exchange an ever-growing amount of data. Rapid technological advances and diversification of online communication have led intelligence and law enforcement authorities to reconsider traditional intelligence-gathering and interception methods, many of which are incapable of meeting novel challenges arising from these changes. On the regulatory front, State authorities may request device manufacturers, service providers and network operators to cooperate with the process as set pursuant to a judicial or administrative order. For example, manufacturers may be required to decrypt encrypted data in a target's device. Network operators may be asked to provide data concerning their users to a monitoring centre operated by an enforcement agency. At the same time, States gradually equip themselves with surveillance technology, which can give them direct access to relevant communications data. Governments across the world have relied on the private sector in obtaining those tools.

As many countries lack home-grown technological capabilities and telecommunications infrastructure required for extensive surveillance operations, companies find lucrative business opportunities in assisting these States to realise their ambitions for technologically-enabled intelligence and law enforcement. The surveillance sector is a burgeoning industry consisting of a wide variety of companies in terms of size and technological expertise.[18] The sector spans a variety of participants, each providing their own technical capabilities to consumers. For example, military contractors supply a range of cyber surveillance technology, whereas technology giants such as Ericsson, Huawei and Nokia produce telecommunications networks.

As a part of operational requirements, network providers are often required to maintain interception systems and monitoring centres. Hundreds of smaller companies are specialised in the development and sales of surveillance products, from commercially available items that are sold to private users to more sophisticated systems that are marketed exclusively to intelligence and law enforcement authorities. The Surveillance Industry Index (SII), the largest publicly accessible database on the surveillance sector, has

[18] SIPRI and Ecorys (n 6) 42–54; Privacy International, 'The Global Surveillance Industry' (Privacy International, July 2016) 16–22 ('Surveillance Industry Report'); PH O'Neil, 'The Fall and Rise of a Spyware Empire' (MIT Technology Review, 20 November 2019).

documented 526 companies in detail.[19] From this it appears that the US, the UK, France, Germany, Israel, and Italy are the six countries in which surveillance companies are most likely to be headquartered and have offices. Another study finds that 87 per cent of companies are based in States that are OECD members.[20] Meanwhile, Chinese firms have been increasingly prominent in the industry.[21]

III. THE WASSENAAR ARRANGEMENT AND CYBER SURVEILLANCE TECHNOLOGY

A. The Creation and the Development of International Export Control Mechanisms

Export controls are measures instituted by States to supervise export flows. The export control mechanism was originally devised to address 'military' risks in the proliferation of biological, chemical and nuclear weapons and other conventional arms.[22] The strict civil–military distinction embedded in the traditional export control regime was incapable of accommodating rapidly changing geopolitical, military and technological circumstances in the global security scene. States gradually abandoned the dichotomy and modernised the regime by expanding its coverage to a variety of dual-use items.[23] There are four main international legal instruments aiming at non-proliferation of various types of goods and technologies: the Nuclear Supplier Group (NSG), the Australian Group, The Missile Technology Control Regime (MTCR), and the Wassenaar Arrangement.[24] Under these multilateral schemes developed over many decades, States establish export restrictions and licensing procedures concerning transfer of the controlled items. Companies seeking to make a transfer need to obtain licenses from the designated authorities. The Wassenaar Arrangement identifies and regulates items enumerated in the Munitions List and the List of Dual-Use Goods and Technologies. Categories 4 and 5 deal with cyber surveillance technology.

The core component of the Wassenaar Arrangement is a list of items agreed by consensus between 42 countries. Members include Argentina, Australia,

[19] See the SII compiled by Privacy International at <https://privacyinternational.org/blog/54/privacy-international-launches-surveillance-industry-index-new-accompanying-report>.

[20] Surveillance Industry Report (n 18) 22.

[21] Cave, Ryan and Xu (n 14) 4–8; Feldstein (n 12) 6–9; Shahbaz (n 12) 13–15.

[22] O Meier, 'Dual-Use Technology Transfers and the Legitimacy of Non-Proliferation Regimes' in O Meier (ed), *Technology Transfers and Non-Proliferation: Between Control and Cooperation* (Routledge 2014) 3.

[23] M Kanetake, 'Balancing Innovation, Development, and Security: Dual-Use Concepts in Export Control Laws' in N Craik, CSG Jefferies, S Seck and T Stephens (eds), *Global Environmental Change and Innovation in International Law* (Cambridge University Press 2018) 180; J Rath, M Ischi and D Perkins, 'Evolution of Different Dual-Use Concepts in International and National Law and Its Implications on Research Ethics and Governance' (2014) 20 Science and Engineering Ethics 769.

[24] DH Joyner, 'Restructuring the Multilateral Export Control Regime System' (2004) 9 JC&SL 181, 183; Meier (n 22) 3; Ruohonen and Kimppa (n 7) 3–4.

Canada, India, Japan, Mexico, South Africa, South Korea, the US, the UK and almost all EU Member States and Russia, with the notable absence of China, Israel and Singapore. While those nations do not participate in Wassenaar, they have domestic legislation that partially incorporates the list of goods and technologies identified by the Arrangement.[25] The institutional predecessor of Wassenaar was the Coordinating Committee for the Control of Multinational Trade (COCOM), created in 1950 by the US and its close allies during the Cold War.[26] COCOM left a legacy of State-to-State cooperation and coordination regarding trade in strategically sensitive goods. Until its dissolution in 1994, COCOM States maintained a common control scheme to prohibit transfers of arms, nuclear-related products and some sensitive dual-use technologies to the Soviet bloc, specifically the Warsaw Pact countries.[27] In contrast, Wassenaar controls do not target any State or a group of States. The initial 33 members of the Arrangement included many of the former Warsaw Pact countries.

The Wassenaar Arrangement is a soft law mechanism, and thus does not create legally binding obligations.[28] Member States do not automatically impose export restrictions and licensing requirements on certain items simply by virtue of the inclusion of those items in the Wassenaar list. This is different from COCOM which had a stronger implementation mechanism along with some oversight rules such as mandatory prior notification and a veto system regarding export of certain items listed as sensitive.[29] The Cold War context behind COCOM strengthened common strategic interests in maintaining a multilateral control mechanism based on unified national export control standards among them. That unifying foundation no longer exists in the Wassenaar era. Nevertheless, most member States have updated their export control systems to make them consistent with Wassenaar lists.[30]

B. The 'Cyber' Amendments

As discussed in Part 1, Wassenaar States have extended the scope of the Arrangement to cyber surveillance technology. The cyber amendments have two main goals: creating controls on specific surveillance items and

[25] Surveillance Industry Report (n 18) 53; T Maurer and J Diamond, 'Data, Interrupted: Regulating Digital Surveillance Exports' (World Politics Review, 24 November 2015) 5.

[26] J Jaffer, 'Strengthening the Wassenaar Export Control Regime' (2002) 3 Chicago Journal of International Law 519, 521; M Lipson, 'The Reincarnation of COCOM: Explaining Post-Cold War Export Controls' (1999) 6 The Nonproliferation Review 33.

[27] KA Dursht, 'From Containment to Cooperation: Collective Action and the Wassenaar Arrangement' (1997) 19 CardozoLRev 1079, 1098; Pyetranker (n 7) 159.

[28] Joyner (n 24) 190–3.

[29] Dursht (n 27) 1113–14; Jaffer (n 26) 521–3; Ruohonen and Kimppa (n 7) 6–7.

[30] See below Sections IV.A and IV.C; implementation of the Wassenaar lists is one of the obligations of participating States. Wassenaar Arrangement Guidelines and Procedures, including the Initial Elements, Compiled by the Wassenaar Arrangement Secretariat, Public Documents (December 2019) Vol I, 5–6.

achieving a certain level of coherence among domestic export regulations on these newly covered goods and technologies.

Nothing in the terms directly associates the uncontrolled proliferation of cyber surveillance technology with human rights violations. Nevertheless, it is implicitly recognised that the export of sensitive surveillance technology must be better regulated because the repressive use of such tools has given rise to real concerns about serious human rights violations in many importing countries.[31] Exporting States were also urged to consider whether there is 'a clearly identifiable risk' that the controlled items might be used 'to commit or facilitate the violation and suppression of human rights and fundamental freedoms'.[32] To some extent, the cyber amendments have made some changes to a strong national security foundation embedded in the Wassenaar scheme.

C. *Three Categories of Cyber Surveillance Technology under Wassenaar*

The Wassenaar Arrangement does not use the term 'cyber surveillance technology' as a separate category to the dual-use control list. It takes an item-by-item approach defining the specific types of surveillance equipment, software and technology subject to Wassenaar. Three categories have been added through a series of amendments: certain types of mobile telecommunications interception equipment (added in 2012), intrusion software-related items, and IP network surveillance systems (both added in 2013). These items are designed to provide and facilitate extensive surveillance capabilities. They are more or less exclusively sold to State intelligence and law enforcement authorities. Major network operators may also obtain them for compliance purposes.

There was little debate over the introduction of controls on the first item, but the 2013 amendment concerning the latter two categories was both praised and criticised by various stakeholders ranging from civil society to academics and security professionals. The major source of discontent was that the definitions provided by the 2013 amendment were either over-inclusive or under-inclusive of the covered items. As a response to mounting concerns from many Wassenaar States in the following years, decontrol notes and technical clarifications were added to the original 2013 amendment.

[31] Wassenaar Arrangement 2013 Plenary Meeting, 'Export Controls for Conventional Arms and Dual-Use Goods and Technologies' (Public Statement,4 December 2013); see also Amnesty International, Digitale Gesellschaft, FIDH, Human Rights Watch, New America Foundation, Privacy International and Reporters sans frontieres, An Open Letter to the Members of the Wassenaar Arrangement (1 December 2014) <https://www.hrw.org/news/2014/12/01/open-letter-members-wassenaar-arrangement>.

[32] Wassenaar Arrangement, 'Elements for Objective Analysis and Advice Concerning Potentially Destabilising Accumulations of Conventional Weapons' (Explanatory Note, revised 2011) at 2.

1. Mobile Telecommunications Interception—5.A.1.f-based Controls

Mobile telecommunications interception technology is used to track, identify, intercept and record mobile and satellite phones.[33] Such interception equipment was added to the Wassenaar list at the 2012 Plenary Meeting. Even prior to 2012, some States had placed controls on the equipment of this kind, yet their usage and interpretation of the term varied. According to 5.A.1.f, a range of 'mobile telecommunications interception or jamming equipment' is subject to Wassenaar controls. One of these is IMSI (International Mobile Subscriber Identity) catchers. The second sub-provision of 5.A.1.f defines them as 'interception equipment designed for the extraction of client device or subscriber identifiers, signaling, or other metadata transmitted over the air interface'. Typically used in a 'Man in the Middle Attack' by faking a legitimate cell tower or base station, IMSI catchers capture and log all the IMSI numbers of mobile phones in the nearby area as these mobiles connect to it.[34] It can intercept the location and traffic information of thousands of mobile phones at the same time. More advanced versions can even intercept calls and text-messages and disrupt the availability of certain Internet services.

2. Intrusion Software-related Items—Controls based on 4.A.5, 4.D.4 and 4.E.1.c

Wassenaar controls associated with intrusion software are built upon two sets of rules: a multi-tiered structure of conceptualising the controlled items, and general exemptions. Notably, the Arrangement does not control intrusion software *per se*. Instead of restricting the whole class of intrusion software, it opts for targeted controls on specific equipment, software and technology that are used to generate, install and instruct intrusion software.

The initial wording of the 2013 amendment was criticised for being overly broad, and thus having (unintended) chilling effects on the security industry and security research.[35] Many security experts feared that technical attributes used to define this control class would imprudently control equipment, software and expertise used for essential cyber security processes. For

[33] The Coalition Against Unlawful Surveillance Exports (CAUSE), 'A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation' (Report, CAUSE, June 2015) 13.

[34] See generally R Saini, M Khari and M Wadhwa, 'Vulnerabilities and Attacks in Global System for Mobile Communication (GSM)' (2011) 2(3) International Journal of Advanced Research in Computer Science 139, 141.

[35] Bohnenberger (n 6) 86–7; Bratus *et al.* (n 7) 3; T Dullien, V Iozzo and M Tam, 'Surveillance, Software, Security and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting' (WA-CAT Draft, 2 October 2015) 10–14; N Martin, 'Google, the Wassenaar Arrangement, and Vulnerability Research' (Google Online Security Blog, 20 July 2015); Microsoft Cybersecurity Policy Team, 'Whitepaper: Rethinking Intrusion Software' (Whitepaper, Microsoft, 2016) 3–8; Ruohonen and Kimppa (n 7) 12.

example, according to the initial terms, when 'exploit'[36] researchers identify vulnerability in the software platforms of foreign vendors, they are prohibited from notifying those vendors of the identified risks unless they first obtain export licenses for the export of such technology. The use of many defensive security products such as penetration testing products, auto-updating antivirus programs and forensic exploit toolkits would also be subject to Wassenaar controls. As examined below, several revisions were made to meet these concerns of the IT security community. Many US technology companies in particular lobbied their government for renegotiation of intrusion software-related controls.[37]

a) Conceptualising the scope of covered items

Intrusion software is specially designed or modified to avoid detection by 'monitoring tools' or to defeat 'protective countermeasures' in order to execute code safely on a computer or network-capable device.[38] It also needs to show software implementations performing either of the following functions:

> (a) the extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or (b) the modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

In response to concerns that this definition inhibited ordinary means of software implementation, a technical note was later added to exclude the following from control: debuggers, Software Reverse Engineering tools, Digital Rights Management software, and asset tracking or recovery software that is installed by manufacturers, administrators or users. Intrusion software can be installed through a range of channels, such as a vulnerability that allows an attacker to covertly install it on the device, and phishing attacks that convince a user to open a disguised executable file or otherwise authorise the installation of a seemingly legitimate application.

The defined class of intrusion software is not itself a controlled item. Wassenaar controls apply only to the systems, equipment, components, software and technologies that have certain relations with intrusion software.

(i) Control categories 4.A.5 and 4.D.4

The controlled class of items has two parts: one covers systems, equipment, and components (4.A.5) or software (4.D.4) specially designed or modified 'for the

[36] An exploit is a piece of code or a software solution designed to take advantage of a security flaw or vulnerability in a computer(ised) system. It is typically used to break into and gain control of the computer system with malicious purposes such as installing spyware, but also employed for non-malicious, legitimate purposes such as security testing, security analytics, and intrusion detection.

[37] See Section IV.A for more discussion regarding US industry pushback against cyber amendments.

[38] Wassenaar Dual-Use List (n 4) 80, 224.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

generation, command and control, or delivery of' intrusion software.[39] A technical note containing exclusion criteria is added to limit the scope of 4. D.4 application. Wassenaar controls do not apply to software specially limited to provide 'software updates or upgrades' authorised by the owner or administrator of the system receiving them (as defined in 4.D.4).

(ii) Control category 4.E.1.c

The second sub-category of intrusion software-related control is technology 'necessary for the development' of intrusion software (4.E.1.c).[40] The meaning of 'development' encompasses a range of processes including design, design research and analyses, assembly and testing of prototypes.[41] Providing technical assistance also falls within the 4.E.1.c scope of development, which encompasses forms of instruction, training, and consulting services which involve the transfer of essential technical information such as blueprints, plans, engineering designs, manuals and instructions. The development and testing of advanced intrusion software is a complex process that often requires site visits, specialised installation procedures and technical support from highly skilled experts. While some surveillance companies offered network analysis, on-site installation of hardware, and software and technical training for local staff, others demonstrated needs assessments and integration design that were necessary to set up intrusion software infrastructure in those countries.[42]

In 2017, several technical notes were added to reshape the scope of application of 4.E.1.c.[43] Wassenaar States relaxed control parameters for essential cyber security tools that inappropriately fell within the meaning of initial cyber amendment. Upon revision, 4.E.1.c no longer applies to necessary technical assistance and research activities in the process of 'analyzing, identifying, reporting or communicating' software vulnerability. 'Exchanging information on a cyber security incident' with individuals or organisations responsible for addressing such an incident is also excluded.

b) General exemptions

General exemptions are specified in the General Software Note and the General Technology Note. By exempting certain types of items, these provisions prevent Wassenaar controls from being imposed in an overly broad manner. The General Software Note carves out software that is 'available to the public' at retail and can be installed by the user without 'substantial support from the vendor', as well as software 'in the public domain' that is freely available upon its further dissemination.[44] The General

[39] Wassenaar Dual-Use List (n 4) 80.
[40] ibid 81.
[41] ibid 219.
[42] Anderson (n 7) 14; CAUSE (n 33) 7.
[43] Wassenaar Dual-Use List (n 4) 81, 219, 236.
[44] ibid 3.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

Technology Note offers two exemption rules that apply to the items laid out in 4.E.1.c: technologies that are 'in the public domain' or for 'basic scientific research'.

3. IP Network Communications Surveillance Systems—5.A.1.j-based Controls

Along with the (ab)use of intrusion software, IP network surveillance received a great deal of attention during the 2013 Plenary Meeting. 'IP network communications surveillance' was added as a new control class under Category 5, Part 2.[45] IP network surveillance is generally conducted through Internet traffic analysis systems that classify and collect communications data flowing in and out of a network. The covered items are 'systems or equipment, specially designed components' that satisfy all of the conditions stipulated in 5.A.1.j. This control class carries two sub-provisions and one decontrol note.[46] In addition, exemption provisions in the General Software and Technology Notes also apply to the class of IP network communications surveillance.

a) Technical attributes of the controlled items

The provided definition of 'IP network communications surveillance' is straightforward, but extremely narrow. First, according to the first sub-provision (5.A.1.j.1), the covered items perform all of the following three functions on 'a carrier class IP network':

> (a) Analysis at the application layer (Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1); (b) Extraction of selected metadata and application content (e.g. voice, video, messages and attachments); and (c) Indexing of extracted data.

In view of function (a), the covered items operate at the seventh layer in the OSI model called the 'application layer', which concerns networking processes at the application level. The OSI model divides communications data into seven abstract layers and standardises protocols into groups of networking functionality to ensure interoperability within the communication system regardless of the technology type, vendor and model used. Layer 7 is the uppermost layer that interacts with end users directly.[47] Function (a) carves

[45] ibid 88.

[46] According to the decontrol note to 5.A.1.j, IP network surveillance systems specially designed for marketing, Network Quality of Service (QoS) or Quality of Experience (QoE) purposes are exempted from Wassenaar controls.

[47] Layer 7 manages application-specific networking requirements, identifies networking entities to facilitate networking requests from end users, synchronises communications, and identifies constraints at the application level including user authentication, privacy, and quality of service and data syntax. Some examples of the applications that operate at Layer 7 are web browsers (eg Chrome and Safari) and programs (eg Outlook and Office).

out IP network surveillance products that work at layers other than Layer 7. This requirement is problematic as its focus is primarily on traditional Internet communications via web and email. Some experts argue that this narrows the scope of 5.A.1.j merely on network surveillance conducted through analysis of the 'content' of Internet communications, and items such as 'monitoring of statistical information on the use of particular applications, blocking of sites, or tracking what IP addresses a user exchanges traffic with' may not be covered under the current language.[48]

Functions (b) and (c) concerning 'extraction' and 'indexing' further narrow down the scope of the 5.A.1.j control class: the covered technology retrieves metadata and application content in the traffic and at the same time, stores them for the purpose of indexing. Since these functions need to be carried out on the carrier class IP network, which is used to refer to 'national grade IP backbone', 5.A.1.j excludes detection and prevention systems operating at the same layer but includes smaller networks such as local area networks or other types of communications network that have limited data processing capacities.

In addition, the second sub-provision (5.A.1.j.2) attaches two more conditions that further frame the scope of 5.A.1.j application. The covered items are designed to perform the following:

> (a) Execution of searches on the basis of 'hard selectors', and (b) Mapping of the relational network of an individual or of a group of people.

There is a broad spectrum of network surveillance tools, many of which conduct Internet traffic analysis in a way that satisfies the terms of the first sub-provision. Among them, there is a fairly large group of products with the ability to search personally identifying information based on 'hard selectors' such as names, email and street addresses, phone numbers and affiliations.[49] In contrast, identifying the patterns and correlation of extracted data in the traffic for 'mapping' is a highly sophisticated function that is used only in limited kinds of surveillance products such as the products specifically marketed for intelligence activities.

However, many experts warn that this definition is too narrow to cover many other network surveillance systems that should have been regulated by the Wassenaar Arrangement.[50] These systems are designed to intercept communications and conduct high performance Internet traffic analysis. They have also been reported as being deployed in repressive contexts. It is fair to say that the current Wassenaar controls on network communications

[48] Anderson (n 7) 27.

[49] Wassenaar Dual-Use List (n 4) 222.

[50] Anderson (n 7) 23; Bohnenberger (n 6) 85; Maurer, Omanovic and Wagner (n 6) 31; Ruohonen and Kimppa (n 7) 10–11; A Weber *et al.*, 'IP Network Communications Surveillance Systems: Deciphering Wassenaar Arrangement Controls' [2015] WorldECR 39.

surveillance systems are targeted at an inadequately narrow class of products. The under-inclusiveness of 5.A.1.j.2 creates a critical regulatory loophole.

IV. THREE REGULATORY APPROACHES TO GOVERNING EXPORT CONTROLS OF CYBER SURVEILLANCE TECHNOLOGY—A COMPARATIVE ANALYSIS

Part IV identifies a global regulatory divergence among national, regional and international approaches to governing the export of cyber surveillance technology. The cyber amendments to Wassenaar have affected subsequent dual-use export reforms in many parts of the world, including the US, China, and the EU. However, as discussed in each sub-section, they show different forms and degrees of Wassenaar implementation concerning cyber surveillance technology. The legislative backgrounds against which their export control laws have developed for the regulation of emerging technologies (including cyber surveillance technology) also vary significantly. Moreover, export controls are increasingly leveraged in a way to strengthen their positions in ongoing power struggles at the intersection of global trade, technology and security. This further affects the ways in which they create and use export controls to achieve a broader national and regional agenda.

Notably, all three jurisdictions have undergone extensive rebuilding of their own export control frameworks. The timing of the adoption of US Export Control Reform Act (ECRA)[51] and the proposed modernisation of the EU Dual-Use Regulation[52] have coincided with the development of the Export Control Law of the People's Republic of China (中华人民共和国出口管制法, ECL) which is the first omnibus export control law for China.[53] Based on the analysis of these three legal systems, Part IV shows that their approaches to export controls of cyber surveillance technology are only becoming more divergent, and may lead to a significant erosion of the global norms governing the use and transfer of emerging technologies.

A. The New Face of US Technology Export Regulation

Since August 2009, the US export control regime has been subject to an extensive inter-agency review under the Export Control Reform Initiative

[51] The US Congress passed the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA) in August 2018 with bipartisan support to mandate the executive branch to counter China's growing impacts globally. As parts of 2019 NDAA, the Foreign Investment Risk Review Modernization Act (FIRRMA, Sections 1701–1728) and the ECRA (Sections 1741–1793) were enacted under Title XVII—Review of Foreign Investment and Export Controls.

[52] Council Regulation (EC) 428/2009 on setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items [2009] OJ L134, Ann 1.

[53] Original Chinese version and unofficial translation of Export Control Law (ECL) provided at Congressional Research Service, 'China Issues New Export Control Law and Related Policies' (Insight Report, Congressional Research Service, 26 October 2020).

launched by the Obama administration.[54] This Initiative sought to develop a single control list, create a more coordinated export control enforcement, establish a single licensing agency and a single IT system for license processing. Under the Trump administration, many parts of the initial reform plan were redesigned in a way that changes the regulatory foundation of US export controls. The traditional narrative of the US export control regime has been modified especially in the export of certain types of technologies.

In recent years, competition between the US and China over technological supremacy has intensified as China quickly builds capabilities in many advanced technology sectors under its long-term State-directed industrial planning strategy.[55] In the midst of growing tension between the two sides, the US government took extensive legislative action aimed at targeting China's growing technological and commercial prowess. The ECRA of 2018 and the recent expansion of the Entity List were clearly adopted in a context where the US is seeking to prevent a group of specific Chinese firms from acquiring certain types of vital technologies originating from US citizens and companies.[56] US export control measures are increasingly used as a protectionist tool to reinvigorate domestic industry concerning 'emerging and foundational technologies' and to guard its dominance against growing foreign actors in the global technology market, specifically by controlling access to the US technology market, and providing a policy blueprint for friendly States to follow.

While the new system under the ECRA is still in the process of updating and implementing regulations that will clarify the scope of new control classes, it is clear that the fate of export restrictions on cyber surveillance technology will be subject to this new scheme. Meanwhile, it remains to be seen whether and to what extent the new Biden administration will adhere to this regulatory stance introduced by the preceding administration.

1. The US Export Control Regime and the Wassenaar Arrangement

The US export control regime consists of different statutes and operates under several licensing and enforcement bodies. The Export Administration Regulations (EAR) provide the main legal framework for controlling exports of dual-use and less sensitive military items.[57] They contain the Commerce Control List (CCL) and implement the Export Controls Act (ECA) at a

[54] Congressional Research Service, *The U.S. Export Control System and the Export Control Reform Initiative* (Report, 5 April 2019) 9–11.

[55] S Mori, 'US Technological Competition with China: The Military, Industrial and Digital Network Dimensions' (2019) 26 Asia-Pacific Review 77, 80–1; see also Section IV.B.3 for the analysis of this new government strategy called, 'Made in China 2025'.

[56] ibid 79; European Parliamentary Research Service (EPRS), 'Briefing, United States: Export Control Reform Act' (22 November 2019) 2.

[57] EAR, 15 CFR. 730ff.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

practical level regarding certain types of controlled technologies.[58] The CCL is a list of controlled items as well as foreign persons and end-uses 'that are determined to be a threat to the national security and foreign policy of the United States'. The Bureau of Industry and Security (BIS) in the Department of Commerce (DOC) is mandated to establish the CCL and carry out export licensing and enforcement functions based on EAR rules.

The US has been at the centre of creation, development and global implementation of international export control mechanisms such as the Wassenaar Arrangement and their multilateral approach to non-proliferation. It is a long-standing stance of the US that most items listed in the CCL are controlled in accordance with its commitments to four major multilateral control regimes including the Wassenaar Arrangement.[59] Based on those internationally agreed lists, the relevant executive bodies have complied and updated the US control lists. The effectiveness of the EAR-based control has been enhanced by it being 'maintained as part of [the] multilateral control arrangement' and almost all items on Wassenaar list are incorporated in the CCL. EAR states that the US dual-use control scheme is 'consistent with the United States' international obligation' as a Wassenaar member.[60]

Regarding the domestic implementation of cyber amendments, BIS has maintained the same position. Upon the adoption of amendments at Wassenaar, BIS submits its own amendment proposal along with a newly compiled control list adopting Wassenaar amendments, but occasionally with some modifications to fit within the existing CCL scheme. BIS then launches a review process inviting various stakeholders, including industry actors and civil society groups, to provide comments on the implications of the amendments for national security, economic and foreign policy interests of the US.

The implementation process for the 2012 cyber amendment (5.A.1.f) adding mobile communications interception equipment such as IMSI catchers went smoothly.[61] Under the old rules, devices for mobile communications interception used to be restricted only in two specific circumstances: when such equipment was specially designed or modified for military use or when such equipment included a cryptanalytic functionality. In implementing 5. A.1.f, new rules were introduced to control the export of interception devices that do not necessarily fit into either of those two categories. This update to BIS Rule was to 'harmonize' national export control practice with the Wassenaar list.[62]

[58] ECRA contains the Export Controls Act of 2018 (ECA) and the Anti-Boycott Act of 2018.
[59] ECRA, Sections 1752(2)(4)(10), 1753(b)(3), 1758(c).
[60] EAR, Sections 730.6, 742.15.
[61] Bureau of Industry and Security, 'Wassenaar Arrangement 2012 Plenary Agreements Implementation: Commerce Control List, Definitions, and Reports' (BIS Rule, Federal Register 78 FR37371, 20 June 2013).
[62] ibid.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

In contrast, this was not the approach for the 2013 cyber amendment. In July 2015, BIS published the first Proposed Rule to incorporate intrusion software-related items and IP network surveillance systems into the CCL.[63] It received an unprecedented number of public comments on the Proposed Rule, virtually all of which were negative. There was a strong backlash from IT industry and security experts especially about intrusion software-related items.[64] Critics feared that the language used by Wassenaar and BIS could lead to 'unintended capture', with a high risk of restricting legitimate cyber defence strategies and other key security processes such as vulnerability disclosure and incident response, and that these controls would lead to an extensive financial licensing burden for security companies.[65] The Proposed Rule was retracted. Instead, BIS followed up with a plan to introduce additional amendments to Wassenaar 'in order to minimize the negative impact of the intrusion software-related entries would have'.[66] This was to hold on to its commitment to regulate cyber surveillance tools through a multilaterally coordinated control mechanism.

As a result of US negotiation efforts during the 2016 and 2017 Wassenaar Plenary, a number of changes and some clarification of technical terms were made to intrusion software controls.[67] As discussed earlier, intrusion software-related controls no longer apply to vulnerability disclosure or cyber incident response. Another decontrol rule has been added for software implementations involving certain types of software updates or upgrades. In 2018, BIS finalised a new regulation updating the CCL as part of the implementation of the remaining cyber amendments. The new version is still under review, signalling 'a retreat by the US government from asserting control over those tools'.[68] While BIS' regular CCL updates have incorporated the most up-to-date version of the Wassenaar lists, the two control classes created as a result of the 2013 amendment have not been included in the CCL.

[63] Bureau of Industry and Security, 'Wassenaar Arrangement 2013 Plenary Agreements Implementation: 'Intrusion and Surveillance Items: A Proposed Rule' (BIS Proposed Rule, Federal Register 80 FR 28853, 20 May 2015).

[64] US House of Representatives Committee on Oversight and Government Reform (Subcommittee on Information Technology) and the Committee on Homeland Security (Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies), 'Compilation of Witness Statements, Hearings on Wassenaar: Cybersecurity and Export Control' (12 January 2016) <https://www.hsdl.org/?view&did=795893>; see also Ruohonen and Kimppa (n 7) 14.

[65] See (n 35).

[66] Statement of Rob Joyce, then White House cybersecurity coordinator on US negotiating success in this regard, quoted by Lichtembaum, Addis and Hindin (n 6) 3.

[67] Bromley and Maletta (n 6) 16; see Section III.C.2.

[68] Lichtembaum, Addis and Hindin (n 6) 3.

2. Leveraging export controls to win the geopolitical, economic and technology race—The advent of the ECRA era and its impact on the US Technology Export Regulation

Notwithstanding failed attempts to add intrusion software-related items and IP network surveillance systems to the CCL, it is likely that there will be a new channel of leveraging export controls to govern cyber surveillance technology (possibly) including those two control classes. As mentioned earlier, ECRA was passed under the auspices of the National Defense Authorization Act for Fiscal Year 2019 in the midst of escalating US–China competition over commercial and technological dominance in the ICT sector.[69] This authorisation gives the President a broad range of constitutional authority to govern export control activities. Under Part I of ECRA titled ECA, an 'interagency process' is created to identify and regulate the new category of 'emerging and foundational technologies' that are not otherwise specified in the existing list.[70] This is to update the US technology export regulation 'without impairing national security or hampering the ability of the US commercial sector to keep pace with international advances in emerging fields'.[71]

As authorised under ECRA, BIS establishes controls on 'the export, re-export or in-country transfer' of these emerging and foundational technologies subject to US jurisdiction, whether by US persons and corporations, or foreign entities.[72] BIS may also impose interim controls on relevant technologies on a case-by-case basis.[73] ECRA's application is extraterritorial; regardless of their business locations, non-US companies are subject to ECRA when re-exporting US-originated goods and technologies. Even non-US made products may be subject to ECRA control if their usage of controlled technologies originating from the US exceeds a certain threshold.

In November 2018, BIS published an Advanced Notice of Proposed Rulemaking (ANPRM) for the 'Review of Controls for Emerging Technologies' and invited public comments to develop criteria for identifying 14 categories of technologies.[74] Six of the 14 categories listed by BIS replicate some of the ten technology industries prioritised by 'Made in China 2025'. One of these new BIS categories is 'Advanced surveillance technologies', and this could encompass a plethora of surveillance tools including items enumerated in the cyber amendments to Wassenaar. Most recently in January 2020, the first in a series of BIS Rules setting out licensing requirements for emerging technologies was published. This Interim Rule regulates certain types of

[69] Mori (n 55) 79.
[70] ECRA, Section 1758.
[71] Bureau of Industry and Security ANPRM, Review of Controls for Certain Emerging Technologies (Federal Register 83 FR58201, 19 November 2018).
[72] ECRA, Section 1753.
[73] ibid, Section 1758(b)(1).
[74] Bureau of Industry and Security ANPRM (n 72).

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

'geospatial imagery software' utilised in artificial intelligence and machine learning applications.[75]

The ECRA scheme re-conceptualises the nature of the US export control system with respect to certain types of critical technologies. A group of 'commodity, software and technology'[76] that would fall under 'emerging technologies' need to be deemed 'essential to the national security'.[77] There is no additional clarification about how to determine what is considered essential to national security and no proper legislative guidance on identifying specific national security concerns that the ECRA control aims to address. The class of emerging technologies seems to cover a broad range of technologies even including items that may be only remotely related to the protection of national security. According to the ANPRM list, 'emerging technologies' are not required to have the distinctive features of military or dual-use items that traditionally invoke export control measures. Neither would items such as brain modelling, computer vision and speech and audio processing (under the category of 'machine learning technology') or adaptive camouflage and functional textiles (under the category of 'advanced materials') be traditionally conceived as having national security implications.

There is another indication that the US export control system is going through a significant change with regard to technology exports. While ECRA does not provide a clear definition of emerging technologies, BIS and other relevant agencies involved in the ECRA's new interagency process need to consider three factors in developing the class of emerging technologies: 'development' of emerging technologies in foreign countries, 'the effect export controls may have on the development' of such technologies in the US, and 'the effectiveness of export controls on limiting the proliferation' of emerging technologies in foreign countries.[78] These factors depend on where the key US industrial actors in respective sectors of emerging technologies stand in the global market as compared to their foreign competitors, especially based in China. The same administrative and legislative attempts targeting Chinese technology companies are also found in a series of EAR amendments in 2019 and 2020 that have added Huawei Technologies and nearly a hundred of its non-US affiliates to the Entity List due to 'activities contrary to the national security or foreign policy interests' of the US.[79]

ECRA allows the US government to define controlled technologies in a unilateral manner without seeking any multilateral alignment strategy. The

[75] Bureau of Industry and Security, 'BIS Interim Rule with Request for Comments, Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification (BIS Interim Rule, Federal Register 85 FR 459, 6 January 2020).

[76] ECRA, Section 1742(7). [77] ibid, Section 1758(a). [78] ibid, Section 1758(a)(2)

[79] Bureau of Industry and Security, 'Addition of Entities to the Entity List, Federal Register' (BIS Rule, Federal Register 84 FR 22961, 16 May 2019); Bureau of Industry and Security, 'Addition of Entities to the Entity List and Revision of Entries on the Entity List' (BIS Rule, Federal Register 84 FR43493, 19 August 2019).

US regulatory stance on dual-use export control has become more inward-looking than ever. Its concerns about losing technological and commercial dominance in the global technology market are evident in the terms of recently introduced reform regarding technology export regulation. It is also problematic that ECRA gives excessive discretion to the DOC, especially its implementation agency for export controls, BIS. BIS has an authority to unilaterally designate certain technologies for ECRA control. There are no clear standards which guide BIS in removing or revising items contained in its technology categories. Technically, BIS can remove or revise existing controls on such items 'as appropriate'.[80] It can even determine 'whether national security concerns warrant continued unilateral export controls' over the new control class of emerging technologies.[81] With the passage of ECRA, the US might show greater determination to impose export restrictions on cyber surveillance technology, albeit at the risk of a broad range of cyber surveillance items being subject to controls based on ambiguous and unpredictable standards under the ECRA scheme.

B. The Future of Chinese Export Controls on Cyber Surveillance Technology —The 'Made in China 2025' and the 'Military-Civil Fusion' Strategy as a Guiding Spirit

The past several years represent a pivotal period for the Chinese export control regime: China has developed and passed its first omnibus export control law, the ECL. With regard to technology export regulation, the ECL shows Chinese attempts to (legally) enable tit-for-tat regulatory response to similar technology export controls that are already adopted or could be introduced by the US under the ECRA scheme. Many terms in the 2018 US law are used in the equivalent Chinese legislation. As some observers explain, China has refined and strengthened its export control law in part to counter recent US export control measures targeting Chinese-based technology companies.[82]

As the ECL only provides the key principles of an export control system, and sets out procedures for export licensing and enforcement, many parts of this new scheme will have to be clarified by the subsequent implementation of regulations. There is no reference to an ECRA-like category of 'emerging and foundational technologies' or to a specific technology sector such as cyber surveillance technology as in the case of the EU Dual-Use Regulation. The future of Chinese export controls on equipment, software and expertise involving cutting-edge surveillance technology will be shaped under 'Made

[80] ECRA, Section 1758(b)(5).

[81] ibid Section 1758(b)(4).

[82] Y Jing, Q Chen and B Lihui, 'Analysis of the Latest Amendments and Highlights of the Export Control Law of the People's Republic of China (Draft)' (China Law Insight, 2 January 2020) <https://www.chinalawinsight.com/2020/01/articles/law-popularity/《中华人民共和国出口管制法(草案)》最新修改/>.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

in China 2025' and its core strategy called 'civil-military integration' (军民融合 or translated as 'military-civil fusion (MCF)').[83]

1. *The Chinese Export Control Regime and its relationship with the Wassenaar Arrangement*

Up until the mid-1990s, China imposed export restrictions on ad hoc basis without any legal parameters. It gradually adopted laws and regulations to control the export of strategically sensitive items, beginning with certain types of chemicals, biological agents, missiles and missile-related items, and nuclear-related materials and technologies.[84] The current Chinese regime consists of a patchwork of multiple laws and administrative regulations.[85]

The Chinese government has made efforts to consolidate existing export control-related laws. Most importantly, the ECL underwent three rounds of drafting, which finally took effect from December 2020. The Ministry of Commerce (MOFCOM) submitted the first draft of the ECL in June 2017, and the second draft was released by the Standing Committee of National People's Congress (NPC) in December 2019.[86] A third draft was passed into law by the NPC on 17 October 2020.[87] The enacted legislation consisting of 49 provisions across five chapters revises the MOFCOM version in part and creates a more centralised system for the licensing, investigation and enforcement of export controls. State Council and the Central Military Commission (CMC) undertake the role of State Export Control Administrative Departments (SECADs).[88] They are also empowered to designate specific government agencies for ECL implementation.[89] The ECL is significantly shorter than the export control laws of the US and the EU, leaving many terms and conditions of the controlled items and licensing procedures to be determined by implementing regulations.

The Chinese export control regime has maintained an interesting relationship with multilateral control instruments including the Wassenaar Arrangement.

[83] PRC State Council, 'Notice on Issuing "Made in China 2025"' (State Council No 28, 8 May 2015) <http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm>.

[84] JD Yuan, 'The Evolution of China's Nonproliferation Policy since the 1990s: Progress, Problems, and Prospects' (2002) 11 Journal of Contemporary China 209; ES Medeiros, 'Chasing the Dragon: Assessing China's System of Export Controls for WMD-Related Goods and Technologies' (RAND Corporation, 26 September 2005) 5–19.

[85] T Aoi, 'Historical Background of Export Control Development in Selected Countries and Regions' (CISTEC, 6 April 2016) 41–2; Foreign and Commonwealth Office Counter Proliferation Programme (FCOCPP), *"Bridging the Gap": Analysis of China's Export Controls Against International Standards* (Final Project Report, April 2012) 4–5.

[86] The Federation of German Industries (BDI), 'Beijing Recasts Its Draft for an Export Control Law' (2 April 2020); Covington & Burling, 'China Releases Second Draft of Export Control Law for Public Comments' (14 January 2020); Global Compliance News, '2019 Updates to China's Draft Export Control Law' (11 January 2020); the US-China Business Council, 'Comments on the Export Control Law' (26 January 2020) 1–11; J Xie, 'China Revises Draft of Its Export Control Law' [2020] WorldECR 86. [87] Xie (n 86) [88] ECL, art 5. [89] ibid art 5.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

Among those four key agreements, China has only joined the NSG. While it is not unprecedented for China to highlight its commitment to international non-proliferation standards,[90] there has been no legal recognition of such commitment. Nevertheless, the Chinese lists of controlled items largely correspond with international control lists covering various nuclear, biological, chemical and missile-related items. China has largely aligned its export control measures with Wassenaar.[91] China seems to perceive that global standard-setting and cooperation to restrict controlled items is essential to (or at least not contrary to) its national security interests, yet the Chinese implementation of the Wassenaar Arrangement is superficial.

The ECL explicitly recognises China's commitment to multilateral export control regimes.[92] This inclusion alone will not alter its reluctance to join multilateral control agreements. Despite its ever-growing presence in the production, development, and sale of cyber surveillance technology, China remains formally outside the Wassenaar mechanism.

2. China's first omnibus Export Control Law—key features

This section focuses on the four aspects in the new Chinese rules under the ECL. Export controls are applied to items that are either enumerated in the control lists, or as unlisted items under special circumstances as defined by a 'catch-all' provision. The ECL identifies eight classes of items that are subject to export restrictions.[93] Controlled items are characterised as 'dual-use items, military, nuclear or other goods, technologies, services, and items relating to the maintenance of national security and national interests, and performance of anti-proliferation and other international obligations'.[94] The ECL also clarifies that 'technical information and other data related to the items' fall under the definition of controlled item.[95]

The first three classes are simply defined.[96] With respect to items under the 'defending national security and national interests', the government can impose an embargo, prohibit their transfers to specific destinations, individuals or entities, and apply temporary controls for up to two years.[97] The final wording differs from prior drafting by including a specific reference to 'national interest', thereby allowing the furtherance of a broader political agenda and interests through the ECL. The catch-all provision extends the scope of controls to the items which are not listed, but may 'endanger national security or national interests', be used in the 'design, development, production or use' of WMDs and their means of delivery, or be used for 'terrorist purposes'.[98] This represents a broadening of the provision compared

[90] Medeiros (n 84) 19, 77–80. [91] FCOCPP (n 85) 10–11; Medeiros (n 84) 19, 44, 60.
[92] ECL, arts 1 and 2. [93] ibid art 2. [94] ibid. [95] ibid. [96] ibid.
[97] The decisions are subject to approval of the State Council and the CMC. ECL, art 10.
[98] ibid art 12.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

to original drafts, namely by offering the SECADs a practically unencumbered discretion to determine items that endanger national security, or could be used for terrorist purposes. Meanwhile, pursuant to Article 18, the ECL introduces a separate category similar to the Entity List under the US export control scheme.[99] The SECADs can place specific 'importers' and 'end users' on this Article 18-based restriction list, if they violate 'the management of end users and end uses,' 'endanger national security or national interests,' or use controlled items 'for terrorist purposes'.[100]

Second, the ECL introduces new concepts in defining what constitutes an 'export' for the Chinese regime. Importantly, the concepts of US style 'deemed export' and 're-export' are added. Pursuant to the ECL's broad understanding of 'export', both Chinese and foreign nationals and entities can be the exporting parties. 'Export' typically means any transfer of controlled items, including cross-border supply of products and technology transfer from the territory of the People's Republic of China (PRC). Added to this definition, any provision of items to foreign organisations and individuals by Chinese citizens and legal entities will now also constitute controlled exporting activities, irrespective of where the transfer occurs.[101] This part is similar to a 'deemed export' under US law and may have a significant impact on foreign technology companies that maintain a substantial business presence in China. 'Re-export' controls may apply when foreign persons and legal entities export Chinese-originated controlled items or foreign-made products containing 'a certain percentage of the value' of Chinese-originated controlled content from one foreign jurisdiction to another.[102] Accordingly, the re-export controls expand the extraterritorial scope of ECL's application.

Third, compared to the initial draft submitted by MOFCOM, the ECL imposes heavier compliance requirements on the part of exporters and makes a significant increase in the penalty for non-compliance.[103] It is mandatory for exporters to submit end-user statements and end-use certificates when applying for an export licence.[104] They need to be issued by end users or the competent government authorities where end users are located, rather than the importing entities, as stated in the initial draft. Exporters may also maintain 'internal export compliance review system'.[105] After the issuance of a licence, exporters need to conduct a review of end users and the actual use of the exported items, and 'immediately report' any change to the competent authorities if they become aware there may be such a change.[106] When changing the stated end-user or end-use, the end-users are required to obtain approval from the relevant Chinese government authorities. Under the 2019

[99] See (n 80). [100] ECL, art 18. [101] ibid art 2. [102] ibid art 45.
[103] Xie (n 86); see also for the table of revised penalties, Covington & Burling (n 86) 5–6; ECL, Ch 4.
[104] ECL, art 15; these documents contain end-user's commitment to stick to the stated end-use and not to transfer covered items to third parties without permission. Previously this process was not compulsory. Covington & Burling (n 86) 4. [105] ECL, art 14. [106] ibid art 16.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

draft, exporters face higher fines and enhanced penalties, and the provision for penalty mitigation in the case of voluntary disclosure of certain offences has been deleted.[107] For example, fines for 'export without licence' have been raised tenfold from the initial sum of RMB 50,000. Exporters transacting with any entities that are blacklisted by the authority would need to pay five to ten times or ten to 20 times greater fines depending on the size and features of illegal business revenues.

Finally, one of the significant changes in the final legislation from prior drafts is the direct consideration given to 'reciprocal' retaliatory measures under the ECL. Pursuant to Article 48, the ECL authorises reciprocal measures in the event that the Chinese Government believes another country or region 'abuses export control measures to endanger the national security and national interests of the PRC'.[108] The addition of explicit provisions enabling such reciprocal measures shows the influence of ongoing competition between the US and China in the technology sector upon export control reform.

3. Export controls on cyber surveillance technology under the ECL scheme

Issued by State Council in 2015, the 'Made in China 2025' Notice sets targets for higher levels of 'domestic production and innovation' of high-end goods, value-added services and emerging technologies.[109] It also specifies targets that Chinese companies in prioritised sectors need to achieve in terms of their domestic and international market shares.[110] Ramping up cyber capabilities is extensively discussed in this context as an industrial priority and a key to military modernisation.[111]

'Made in China 2025' has played a critical role for the development of the cyber surveillance technology industry in China. The rapid growth of this sector is a result largely of the government's military-civil fusion (MCF) strategy, which was introduced as a project to modernise military hardware in the 1990s and elevated to a national strategy as one of the initiatives pursued under the 'Made in China 2025' Notice.[112] MCF incentivises the civilian sector to enter the defence market by supporting relevant industrial actors with tax reductions and other financial subsidies. It encourages commercial and defence sectors to combine resources to develop dual-use technologies for greater efficiency and growth, 'with a particular emphasis on assimilating private innovation into the defense industrial base'.[113] Against this

[107] ibid Ch 4.
[108] ibid art 48.
[109] Office of the Secretary of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019, A Report to Congress Pursuant to the National Defense Authorization Act' (2 May 2019) 9–11.
[110] The US-China Business Council, 'Unofficial USCBC Chart of Localization Targets by Sector Set in the Made in China 2025 Key Technology Roadmap' (2015) 1–8.
[111] Mori (n 55) 82–4.
[112] Office of the Secretary of Defense (n 109) 21.
[113] ibid 96; see also Mori (n 55) 82–3.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

background, various Chinese technology companies have become an integral part of the defence market, and advanced surveillance technology is one of the key sectors that produces a wide variety of products and expertise having both industrial and military utility.

On its face, 'Made in China 2025' is a nationwide industrial planning strategy adopted to stimulate domestic development of prioritised technology sectors, and to maintain a competitive edge over strategic competitors. Its guidelines shape the business activities of a range of industrial actors (eg producers, developers and the exporters) in these sectors. The implications of 'Made in China 2025' are more than industrial. This top-down industrial goal-setting statement serves to dictate the legislative and administrative narrative justifying the imposition of tighter controls on the transfer of Chinese-originated cutting-edge technologies. What China seeks to achieve through the adoption of the ECL is one of these examples. As examined above, the ECL (legally) enables the government to impose tit-for-tat export control measures, and, with ECL's extraterritorial application, implements the spirit of 'Made in China 2025' overseas. As with the US Entity List, the ECL also creates a formal procedure to blacklist certain importers and end-users as a result of, for example, actions against 'endangering national security'.[114]

Many terms in the 2018 US law are similarly used in the equivalent Chinese legislation. More than half of ten key technology sectors selected for prioritised government support in the 'Made in China 2025' list replicate those on the US BIS list of emerging technologies. There is a possibility that Chinese technology export regulation will become more aggressive and targeted towards users and exporters of certain origins, particularly the US.

C. Strengthening the Human Rights Dimension in the Export Regulation of Cyber Surveillance Technology—EU Reform after an Impasse

The EU's export control regime for dual-use goods and technologies has undergone an extensive multi-year revision. Unlike in the US and China, the EU export control reform was initiated by revelations in the early 2010s that EU-originated surveillance products and expertise had been sold to and used by authoritarian regimes.[115] This legislative background developed in the Arab Spring context aptly explains the human rights orientation of subsequent reform proposals. The EU's reformative angle in this regard is often described as 'rights-based export controls', 'people-centered security' or the 'human security approach'.[116]

[114] ECL, art 18.

[115] Parliament Resolution (EP) 2011/2113(INI) of 10 May 2012 trade for change: the EU trade and investment strategy for the Southern Mediterranean following the Arab Spring revolutions [2012] OJ C261E; Schaake (n 8) paras 13–34.

[116] See Kanetake (n 6); Rath *et al.* (n 23); Schaake (n 8); EU-wide efforts to incorporate human rights was acknowledged by many NGOs. Accessnow, 'Shared Statement on the Update of the EU

After prolonged negotiations between the European Commission, Parliament, and Council, compromise over the text of the proposed amendments was finally reached in November 2020. There was broad agreement among Member States that the EU should be a more accountable actor in the global trade in cyber surveillance technology, however division arose over the extent to which human rights considerations should be invoked as an explicit justification to restrict the export of cyber surveillance items. Some preferred a more limited amendment to the existing export control legislation. As examined below, this division is also found in the different reform proposals delivered by those three EU institutions. The Council's negotiating mandate rejected almost all amendment proposals that could broaden the scope of controls on cyber surveillance technology beyond what was already agreed at Wassenaar.

1. Wassenaar implementation and the legislative process for the 'Recast' EU Dual-Use Regulation

EU Member States have maintained a common legal framework for export controls since the 1990s.[117] Centralising dual-use controls across the EU, Council Regulation (EC) No 428/2009 ('Dual-Use Regulation') was adopted under the Common Commercial Policy, one of the areas of exclusive EU competence.[118] It provides for the free transfer of dual-use items—with some exceptions—within the EU single market, and imposes various restrictions on the export, brokering, transit and transfer of dual-use items.

The current Dual-Use Regulation envisions several avenues for the imposition of export restrictions on cyber surveillance technology. Its dual-use control list corresponds with the lists maintained by various multilateral export control mechanisms, including the Wassenaar Arrangement.[119] In December 2014, the three control classes of the cyber amendment were added to Annex 1A of the Dual-use Regulation.[120] All the subsequent updates to the initial cyber amendment have been incorporated.[121] Pursuant

Dual-Use Regulation' (May 2017) <https://www.accessnow.org/cms/assets/uploads/2017/05/NGO_Sharedstatement_dualuse_May2017.pdf>.

[117] I Davis, *The Regulation of Arms and Dual-Use Exports: Germany, Sweden and the UK* (Oxford University Press, 2002) 45; AG Micara, 'Current Features of the European Union Regime for Export Control of Dual-Use Goods' (2012) 50 JCommonMktStud 578, 581.

[118] Micara (n 117) 579.

[119] R Atlas, 'Toward Global Harmonization for Control of Dual-Use Biothreat Agents' (2008) 35 Science and Public Policy 21; SIPRI and Ecorys (n 6) 142.

[120] Commission Delegated Regulation (COM)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 L371.

[121] Commission, 'Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009' COM (2019) 562 final (2019) 2.

to Article 8, States are also allowed to restrict dual-use items not specified in the list 'for reasons of public security or human rights considerations'. In theory, (unlisted) surveillance items may thus be controlled nationally depending upon the manner and context in which they are transferred and deployed. Currently, at the EU level, the export of certain mobile telecommunications interception equipment, intrusion software-related items, and IP network surveillance systems are controlled in uniformity across all Member States, even without assessing their impact on public security or human rights within the meaning of Article 8.

The ill-controlled use and spread of cyber surveillance technology has been a driving force of the reform proposal for the Dual-Use Regulation.[122] The amendment process is subject to the ordinary legislative procedure involving a 'trilogue' among the European Commission, Parliament and Council.[123] In April 2014, the three institutions published a joint statement articulating how the EU should modernise the export control regime in order to 'keep up with new threats and rapid technological changes'.[124] The 2014 joint statement urged the introduction of restrictions on certain ICT equipment, software, and expertise that can be used 'in connection with human rights violations' and in a way that undermines the EU's 'security interests'.[125] The proposed reform also sought to enhance EU-wide uniformity across the application of domestic export control measures, and facilitate information sharing among Member States.

In September 2016, the European Commission published a proposal to 'recast' the Dual-Use Regulation.[126] The Commission's amendment proposal was submitted to the Parliament, which appointed the Committee for International Trade (INTA) to draft a set of amendments to the Commission's proposal. Following the adoption of INTA's final report containing 98 amendments to the proposal, the Parliament voted by an overwhelming majority to adopt them during a Plenary Session in January 2018.[127]

[122] Statement of Cecilia Malmström, EU Commissioner for Trade, Debate at European Parliament in Strasbourg on 24 November 2014, quoted by Bromley *et al.* (n 3) 39.

[123] EPRS, 'Briefing: EU Legislation in Progress, Review of Dual-Use Export Controls' (November 2019) 1.

[124] Commission, 'Joint Statement by the European Parliament, the Council and the Commission on the Review of the Dual-use Export Control System' COM (2014) 151 final.

[125] ibid.

[126] 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 ('Commission Proposal').

[127] Draft European Parliament Legislative Resolution in: European Parliament, '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 (COM(2016) 0616 – C8-0393/2016 – 2016/0295(COD)), European Parliament, Committee on International Trade, A8-0390/2017' (Report 2016/0295(COD), 19 December 2017) ('Parliament Proposal'); see for a detailed account of this process, Bromley (n 6) 16.

2. *Different views over the amendment of the EU Dual-Use Regulation—Implications for the export of cyber surveillance technology*

The Commission's amendment proposal showed a regulatory turn to strengthen EU-wide export controls on cyber surveillance technology, and the core components of its proposal were largely endorsed by the Parliament. The proposed control scheme combines a list of items identified under a new control category called 'cyber surveillance items',[128] with a catch-all clause for such items that are not specifically listed but used in connection with serious human rights violations as identified by the competent bodies. However, these reform proposals were met by the Council's counterproposal rejecting many of substantive provisions relating to cyber surveillance technology and human rights.

There are three key areas of amendment addressed by the Commission and subsequently updated by the Parliament. First, a new control category was created for cyber surveillance items, with an 'autonomous' EU list introduced for cyber surveillance technology that emphasised its connection to serious human rights violations. While Article 2(1)(1)(b) defines the scope and meaning of cyber surveillance items, the Parliamentary amendment updates the Commission's version to some extent. It provides a number of technical attributes of the items that fall under the category of cyber surveillance items:

> hardware, software and technology, which are specially designed to enable the covert intrusion into information and telecommunication systems and/or the monitoring, exfiltrating, collecting and analyzing of data and/or incapacitating or damaging the targeted system without the specific, informed and unambiguous authorization of the owner of the data.

It then clarifies specific manners and contexts in which the covered items may be used:

> (…) and which can be used in connection with the violation of human rights, including the right to privacy, the right to free speech and the freedom of assembly and association or which can be used for the commission of serious violations of human rights law or international humanitarian law, or can pose a threat to international security or the essential security of the Union and its Members.

The Parliament's proposal is also in line with the Commission's position to create an autonomous list for cyber surveillance items. As Article 16(2)(b) states, the list shall be amended if it is 'necessary due to risks that the export of cyber surveillance items may pose as regards the commission of serious violations of human rights or international humanitarian law or the essential

[128] The Parliament changed the term from cyber surveillance technology to 'cyber surveillance items'. Parliament Proposal (n 128) Amendment 26 on art 2(1).

security interests'.[129] Items such as data retention systems and digital forensics were newly added to Annex IB as 'other items of cyber surveillance technology'. These items do not fall under the three categories incorporated into the dual-use list as a result of the EU's Wassenaar implementation in 2014.

Second, the human rights dimension is incorporated into Article 4(1), which creates a catch-all control for the export of non-listed items in certain situations. Article 4(1) was initially proposed as an 'emergency brake' to be applied for dual-use items in general,[130] but the Parliament's amendment reduced its scope to cyber surveillance items. Cyber surveillance items that are not listed in the Regulation may be subject to control if used:

> in connection with violations of international human rights law or international humanitarian law in countries where serious violations of human rights have been identified by the competent bodies of the UN, the Council of Europe and the Union, or national competent authorities.

In addition, there must be 'reason to suspect' that these items 'may be used for the purpose of directing or implementing such violations' by the end-user. Regarding any of the uses that invoke the catch-all control on cyber surveillance items, Article 4(2) imposes 'due-diligence' obligations on the part of exporters.

Third, the element of human rights assessment is integrated into the export licensing procedure for cyber surveillance items. The amendment proposal expands Article 14's licensing criteria by requiring States to take into account human rights situations in importing countries. Among six sub-provisions, there are three human rights-related considerations, two of which explicitly concern cyber surveillance technology. Namely, licensing authorities are required to consider 'the occurrence of violations of human rights law, fundamental freedoms and international humanitarian law' in the country of final destination as established by the UN, the Council of Europe, or the Union.[131] Member States also need to consider the 'intended end-use' of cyber surveillance items and assess the risk that those items, 'will be diverted or re-exported under undesirable conditions or be diverted to unintended military end-use or to terrorism'.[132]

For its part in the trilogue procedure, the Council adopted a negotiating mandate for reviewing the Dual-Use Regulation in July 2019. The Council's negotiating mandate shows a significant disagreement between the Council and the rest of institutions in the trilogue process.[133] Up until late 2020, it was unclear to what extent the key innovations proposed by the Commission and the Parliament would be accepted. First, the Council's mandate dismissed any references to creating an autonomous EU list for cyber surveillance items. Second, it rejected a human rights-based catch-all clause

[129] The Commission is in charge of adding and removing such items to Annex 1B. Parliament Proposal (n 128) Amendment 64 on art 16(2)(ba).
[130] Commission Proposal (n 126) 5.
[131] Parliament Proposal (n 128) Amendment 56 on art 14(1)(ba).
[132] Parliament Proposal (n 128) Amendment 60 on art 14(1)(f).
[133] EPRS (n 123) 9–10.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

for unlisted cyber surveillance items (Article 4(1)), and the idea of due diligence obligations for exporters (Article 4(2)). Finally, the new requirement for human rights assessment was removed from export licensing criteria. Instead, the Council merely referred to the existing EU-wide policy commitment to consider human rights violations as one of the reasons for imposing export restrictions. In particular, the Council's mandate reinstated a reference to Common Position 2008/944/CFSP ('Common Position') containing human rights-related provisions concerning arms exports.[134] This move indicated a far more limited application of human rights than what was pursued by the proposed amendment passed by the Parliament.

Moreover, many Member States repeatedly expressed reluctance to go beyond what had been agreed multilaterally at Wassenaar.[135] They made it clear that the unilateral expansion of export controls on cyber surveillance items was unacceptable, and that until such a time comes, the EU should not work 'in isolation'.[136] In other words, the EU control list should continue to be maintained through incorporating the control lists of international agreements, including the Wassenaar Arrangement. From another perspective, many researchers and stakeholders in EU-based technology companies expressed growing concern regarding self-inflicted damage. The human rights-oriented recast of the export control regime would create stricter restrictions on cyber surveillance technology, and with such an approach, the EU might lose business competitiveness over other leading States—especially the US and China. The proposed amendment, if adopted unchanged, would undermine innovation and disrupt supply chains in the cyber surveillance industry. As the US and China had gone through extensive rebuilding of export control rules concerning cutting-edge ICT, including cyber surveillance technology, it was argued it would not be wise for the EU to finalise the reform process and risk setting their position in stone.

3. Compromise reached—The prospect for the human rights-based approach to technology export regulation

Following extensive trilogue negotiations, a provisional agreement was finally reached on the 'final compromise text' in November 2020.[137] Overcoming

[134] Council Common Position (EC) 2008/944/CFSP on Defining Common Rules Governing the Control of Exports of Military Technology and equipment, [2008] OJ L335/99.

[135] Various Delegations, 'Working Paper: EU Export Control – Recast of Regulation 428/2009' (29 January 2018) Working Party on Dual-Use Goods WK 1019/2018 INIT, 2–3; Various Delegations, 'Working Paper: Paper for Discussion – For Adoption of an Improved EU Export Control Regulation 428/2009 for Cyber Surveillance Controls Promoting Human Rights and International Humanitarian Law Globally' (15 May 2018) Working Party on Dual-Use Goods WK 5755/2018 INIT, 4.

[136] Various Delegations Paper of 29 January 2018, (n 135), 2.

[137] EPRS, 'Review of Dual-Use Export Controls (January 2021) 1; see also Commission, 'Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009' COM (2021) 42 final.

significant differences among multiple amendment proposals, the proposed Dual-Use Regulation of 2020 achieves two goals with regard to cyber surveillance technology: enhancing the EU's capacity to regulate trade flows in a wider range of cyber surveillance items, and strengthening human rights considerations in the EU export licensing architecture. The compromise text subsequently received endorsement at the Ambassadors of the Member States meeting. The Parliament is expected to vote on the adoption of the agreed text at first reading in early 2021.

This section focuses on three important amendments agreed in the compromise text.[138] First, the term 'cyber-surveillance items' is now defined under dual-use items. According to Article 2(21), cyber-surveillance items means:

> dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems;

The new definition is simplified compared to wording suggested by the Commission's proposal and no longer defines specific manners and contexts in which the covered items may be used. The Commission also proposed to add 'monitoring centres' and 'data retention systems or devices' under a newly created group of controlled items (Annex IB). This category no longer remains in the compromise text. Except in the case of regular updates introduced in line with the EU's commitment to implementing Wassenaar, there is no change concerning cyber-surveillance items in the EU control list.

Second, Article 4a of the compromise text creates human rights-based catch-all controls for cyber-surveillance items that are not listed in the Dual-Use Regulation. Most of the proposed amendments suggested and updated by the Commission and the Parliament in this regard remain intact. The Council's position rejecting the creation of catch-all controls for cyber-surveillance items did not prevail. Relevant authorisation is required for the export of any cyber-surveillance items 'not listed in Annex I' to the regulation,[139]

> if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law.

Under Article 4a, the exporter of non-listed cyber-surveillance items needs to conduct 'due diligence findings', and if the exporter is aware that those items 'are intended, in their entirety or in part, for any of the uses' described above, the exporter bears obligations to notify the competent authority, 'which shall

[138] European Council, '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) (Proposal 2016/0295 (COD) 13 November 2020) ('Compromise Text').

[139] Compromise Text (n 138) art 4a(1).

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

decide whether or not to make the export concerned subject to authorization'.[140] Due diligence obligations on the part of the exporter were among the amendment proposals rejected by the Council. This compromise not only strengthens human rights considerations in the export licensing process, but also shows a greater expectation for the role of the private sector (including commercial surveillance companies) in dealing with the risks posed by the proliferation and abuse of cyber surveillance technology. Interestingly, the amendment proposals suggested and updated by the Commission and the Parliament went further and clarified specific standards of due diligence exercise required for the exporter.[141]

Finally, the compromise text strengthens reporting rules aimed at increasing transparency and information sharing regarding trade in dual-use items. Article 24(2) requires the Commission to produce a publicly available report detailing the actual implementation of the Dual-Use Regulation by Member States. Under the new sub-provisions introduced by the compromise text, this report has to include information on export authorisations (in particular the number and value of items by type and destination), denials, and prohibitions under the Regulation, and other information as required in Article 24(2). There is also an additional reporting requirement concerning the export of cyber-surveillance items. The report requires 'dedicated information on authorisations, in particular on the number of applications received by items, the issuing Member State and the destinations concerned by these applications, and on the decisions taken on these applications'.

The application of human rights concerns to export controls has not been an alien concept in EU-wide practice. In fact, 'respect for human rights' was among the most frequently used assessment criteria when national licensing authorities of Member States denied export licenses for cyber-surveillance items.[142] Human rights-related abuse and risks are no longer a marginal consideration in regulating the export of sensitive dual-use goods and technologies.[143] With the adoption of the 2020 compromise text, the EU goes further by placing human rights considerations at the centre of decision-making for export controls of cyber-surveillance items. The proposed Regulation makes it clear that these items exported from the EU market 'may be misused by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law'.[144] At different stages of export restrictions and licensing, strengthening human rights considerations is recognised as key to dealing with technological and security challenges posed by the proliferation of ICT-powered surveillance tools.

[140] Compromise Text (n 138) art 4a(2).
[141] See Parliament Proposal (n 128) Amendment 31 on art 2(1)(23a).
[142] SIPRI and Ecorys (n 6) 181.
[143] Kanetake (n 6) 157–8.
[144] Compromise Text (n 138) Recital 5.

https://doi.org/10.1017/S0020589321000105 Published online by Cambridge University Press

V. CONCLUSION

The Wassenaar Arrangement is a central platform of international cooperation for regulating dual-use items, and the cyber amendments to Wassenaar have created a multilateral mechanism designed to govern the use and transfer of cyber surveillance technology. Following severe criticism of the repressive use of cyber surveillance technology supplied by commercial surveillance firms, Wassenaar States reached an agreement to extend the scope of the Arrangement to cover certain types of surveillance tools. It was expected that such collective efforts to develop and coordinate export controls under a common legal framework would stop the kinds of abuse that made these companies (in)famous over the past decade. Notably, the realisation of this vision depends on regional and domestic implementation of the cyber amendments.

The US, China, and the EU have played a leading role in the production, sales and governance of cyber surveillance technology. They have used the Wassenaar Arrangement (at least) as a template to create and/or strengthen (new) export controls on cyber surveillance technology. However, based on the analysis of recent export control reforms in these three jurisdictions, Wassenaar implementation strategies concerning cyber surveillance technology have been far less successful than the cases of many other Wassenaar-listed items. In the US, the implementation process has long been delayed except in the case of certain mobile telecommunications interception. China seemed to perceive that global standard setting and cooperation to restrict the controlled items under the auspices of Wassenaar were essential to (or at least not contrary to) its national security interests, yet the Chinese implementation of the Wassenaar Arrangement is flimsy as it is not a party to Wassenaar. In the EU setting, the cyber amendments in their entirety have been incorporated into the EU export regulation framework, with EU lawmakers going far beyond what was agreed at Wassenaar.

The timing of the US ECRA and the proposed modernisation of the EU Dual-Use Regulation have coincided with the development of China's first omnibus export control law. As analysed in Part IV, their new export control rules and new control categories adopted as a result of nation (region)-wide reforms show a significant degree of regulatory divergence. All three jurisdictions aim to become a stronger and more autonomous regulatory entity in governing the use and transfer of cyber surveillance technology. In the US and Chinese settings, export controls are not just a traditional mechanism for the non-proliferation of sensitive dual-use items such as cyber surveillance technology, but have become a key front for political, commercial and security confrontations concerning emerging technologies, especially between these States.

The escalating G2 competition at the intersection of global trade, technology and security has affected the minds of policymakers in ongoing debates over

export control challenges associated with cyber surveillance technology. To be more specific, with the advent of the ECRA era, the US technology export regulation is increasingly inward-looking and is overly permissive of the unilateral application of export controls.

The US focus on controlling the export of US-originated 'emerging and foundational technologies' indicates that with respect to cyber surveillance technology—which is one of the 14 categories in the 'emerging' technology list identified by the BIS—the US is no longer at the centre of creation, development and global implementation of the Wassenaar controls. Its concerns about losing technological and commercial dominance in the global technology market are also manifest in the terms of the ECRA adopted in 2018. In China, the ECL shows Chinese attempts to (legally) enable tit-for-tat regulatory responses to similar technology export controls adopted and/or possibly introduced by the US under its new export control law. Some of the most significant changes in the final legislation from prior ECL drafts broaden the scope of export control justifications that allow the furtherance of a broader political agenda of the government through the ECL.

In contrast, the EU's approach to the same matter is entirely different. The reform discourse for the EU Dual-Use Regulation has been framed so as to recognise the linkage between human rights violations and the repressive use of ICT-powered surveillance tools, as well as the importance of export control measures in breaking that linkage. After years of prolonged negotiations, the EU has successfully adopted new export control rules for cyber surveillance technology. These rules are explicitly built around human rights considerations. The proposed control scheme combines a list of items under the newly defined dual-use category of 'cyber-surveillance items', with a catch-all clause for such items that are not listed but used in connection with certain situations involving human rights violations. Such a progressive catch-all clause is absent in the Wassenaar terms. Moreover, the EU Member States have consistently strengthened a global coalition of democracies committed to adopt a more human rights-centred approach to governing the export of cyber surveillance technology. Nevertheless, it is unclear how the EU's collective regulatory turn will be received by the US and Chinese governments in the long run and how it will interact with export control reforms designed with different geopolitical, commercial and security agendas.

The surveillance industry is the 'first line of defence' to prevent the proliferation and abuse of cyber surveillance technology.[145] However, one cannot wholly rely on private surveillance companies to exercise self-regulation and conduct human rights risk assessments for certain end-uses and end-users of their products. It is not unprecedented that some of these

[145] Comment of Valdis Dombrovskis, current Executive Vice President of the European Commission and Commissioner for Trade, quoted in Press Release, 'Commission welcomes agreement on the modernization of EU export controls' (9 November 2020).

companies circumvent controls by exploiting differences in national export controls and licensing procedures. They also relocate their businesses and/or change distribution channels to States having more lenient rules.[146] Therefore, States urgently need to revive administrative and legislative efforts to implement the Wassenaar controls on certain types of cyber surveillance technology.

It should be noted that there are no effective remedies for civilian victims in cases where State-led mass surveillance is conducted in connection with serious human rights violations. Given that the local justice system is not likely to provide any successful course of action for demanding accountability,[147] the export control mechanism could be one of the few avenues able to address their human rights concerns to some extent. Ideally, with respect to cyber surveillance technology, policymakers should integrate human rights considerations into the process of assessing the security risks associated with certain end-users and end-uses at different stages of export control licensing and enforcement. Making those surveillance products and expertise subject to an export control scheme will lead government authorities and private surveillance companies to act more responsibly in transferring cyber surveillance tools—many of which have fallen into the wrong hands.

[146] States with stricter licensing requirements may have to risk the fleeing of surveillance companies that generate a huge amount of revenue every year, and this potentially leads to a 'race to the bottom'. See S Boazman, 'How We Revealed the Surveillance World's Illegal Trades' Al Jazeera (10 April 2017); Bromley (n 6) 12; CAUSE (n 33) 14; Maurer and Diamond (n 25) 6; Privacy International, 'Surveillance Companies Ditch Switzerland, but Further Action Needed' (5 March 2014).

[147] Citizen Lab, 'Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry' (Last updated 4 November 2020) <https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/>.