Delft University of Technology

Digital technologies, human rights and global trade?

Expanding export controls of surveillance technologies in Europe, China and India

Wagner, Ben; Horth, Stéphanie

DOI
10.4337/9781035308514.00021

Publication date
2025

Document Version
Final published version

Published in
Research Handbook on Human Rights and Digital Technology

Citation (APA)
Wagner, B., & Horth, S. (2025). Digital technologies, human rights and global trade? Expanding export controls of surveillance technologies in Europe, China and India. In *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations, Second Edition* (pp. 242-261). Edward Elgar Publishing. https://doi.org/10.4337/9781035308514.00021

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Green Open Access added to TU Delft Institutional Repository
as part of the Taverne amendment.

More information about this copyright law amendment
can be found at https://www.openaccess.nl.

Otherwise as indicated in the copyright section:
the publisher is the copyright holder of this work and the
author uses the Dutch legislation to make this work public.

12. Digital technologies, human rights and global trade? Expanding export controls of surveillance technologies in Europe, China and India

Ben Wagner and Stéphanie Horth

Historically global trade has not had a strong value-based focus, whether on human rights or for that matter any other values in general. Trade-oriented institutions and legal mechanisms have historically been almost exclusively economically oriented, with human rights concerns either considered to be non-tariff trade barriers, or as non-binding guidelines such as the UN Guiding Principles on business and human rights. However, it should be noted that despite their voluntary nature, many non-binding mechanisms have developed considerable normative strength in recent decades, even though they do not have legally binding mechanisms attached.

Despite these challenges, concepts related to human rights have slowly been seeping into international trade. One aspect has been the public debates about international investment treaties such as the Transatlantic Trade and Investment Partnership (TTIP) and Trans-Pacific Partnership (TPP) at a multilateral level, or in individual bilateral investment treaties (BITs) such as between South Africa and Germany. Another important example is the increase in human rights language in export control regimes. Export control regimes such as the international Wassenaar Arrangement are typically focused on ensuring international security by limiting the trade in certain goods and services. However, in recent decades their scope has expanded from focusing on limiting the proliferation of military goods to ensure international security, to also limiting the spread of goods used for internal repression, a measure frequently justified by recourse to human rights or human security. How can this increased focus on human rights be understood and how does this shift impact export controls of digital technologies?

This chapter will provide an overview of the increasing role of human rights and digital technology in export control regimes over the past two decades and how this has led to the expansion of export controls of surveillance technologies. It will take a particularly close look at the EU debate on export controls, human rights and digital technologies, before looking at China and India which also implement similar restrictions of digital technologies. The EU is a particularly interesting case as it is the key norm-setter in the area of export controls for surveillance technologies. China and India, by contrast, are particularly interesting cases because they have spent decades implementing part of the Wassenaar Arrangement, including controls of digital technologies, without any meaningful ability to define the norms they were to a considerable extent abiding by. The chapter will then discuss challenges with export controls in the areas of human security, cryptography regulation, transparency, participation and governance, as well as the appropriate size and scope of the relevant regime. In conclusion, the chapter will suggest that while not a panacea for all challenges related to human rights in digital technologies, export controls of surveillance technologies can provide an important element of such protection.

At a more fundamental level, this chapter will argue that while export controls may not be the obvious mechanism of choice to govern digital technologies, they have become a powerful way of inserting human rights into international trade. In contrast to claims that the Internet is borderless and regulation fundamentally impossible, export controls provide a key example of how human rights norms can be embedded in technical Internet infrastructure by restricting the flow of surveillance technologies which are likely to have a negative human rights impact.

1. EXPORT CONTROLS AND HUMAN RIGHTS

1.1 Export Control Regimes After the End of the Cold War

Up until the end of the Cold War, there were only regional 'block-oriented' export control mechanisms, but no 'broad-based international treaty'.[1] Those export control mechanisms that did exist were limited to a focus on a narrow set of weapons defined in treaties between a limited group of like-minded states. These treaties, such as the Coordinating Committee for Multilateral Export Controls (COCOM) Cold War arms control treaty, were normally intended not just as a tool of arms control but also as a mechanism to keep access to key arms and technologies within a limited set of members of the club.[2] This changed rapidly after the end of the Cold War, when institutions such as COCOM morphed rapidly into organizations which focused on a broader membership basis from both sides of the Iron Curtain.

The most notable organization here is the Wassenaar Arrangement, which grew out of COCOM and is one of the largest organizations in the world for coordination of export control regulations. In 1994 and 1995, the members of COCOM and several other states came together in meetings referred to as the New Forum, in order to discuss new means of controlling international exports. The New Forum envisioned its role as 'custodian for maintaining the emerging world order'.[3] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies was the result of the New Forum, a consensus that a control list of goods should serve to help ensure regional and international stability.

What is perhaps most notable about the Wassenaar Arrangement is that it is a non-binding 'arrangement'. The Wassenaar Arrangement controls exports by cooperating to establish a common List of Dual-Use Goods and Technologies that is then voluntarily implemented to national laws by participating states. Participating countries also exchange information about specific denials and licences. Within the Arrangement, states simply develop joint sets of definitions of weapons or other dual-use items that they are not legally bound to enforce. Despite this, all of the member states and even several non-member states such as China enforce the majority of the restrictions on the Wassenaar List, making it a fascinating example

[1] Mark Bromley, Neil Cooper and Paul Holtom, 'The UN Arms Trade Treaty: Arms Export Controls, the Human Security Agenda and the Lessons of History' (2012) 88(5) *International Affairs* (1 September) 1031, available at https://doi.org/10.1111/j.1468-2346.2012.01117.x.

[2] Cecil Hunt, 'Multilateral Cooperation in Export Controls: The Role of CoCom' (1982) 14 *U. Tol. L. Rev.* 1285.

[3] Samuel A.W. Evans, *Revising Export Control Lists* (Flemish Peace Institute, 2014).

of international norm diffusion. Wassenaar is unusual not just because it is non-binding, but because even states not involved in the rule-making at all are willing to accept being bound by norms that they have not been involved in developing. The goal of the Wassenaar Arrangement is to contribute to international and regional security by promoting transparency and responsibility concerning the transfer of arms and dual-use goods, and to complement and reinforce the control regimes for weapons of mass destruction. Although other organizations, such as the OSCE or the European Union (EU), developed their own sets of export controls, the Wassenaar Arrangement has, since 1995, been the key international norm-setter in the area of export controls.[4]

In conclusion, it is possible to suggest that there has been a considerable increase in the number of multilateral export control regimes since the end of the Cold War. While these were previously mainly regional arrangements, they are increasingly agreed at an international level and thus encompass a far larger number of states.

1.2 Human Rights and Export Controls

The end of the Cold War coincided not just with an increase in the number and scope of export control regimes around the world, it also witnessed the increasing growth in claims to ethical foreign and trade policy. Key international actors such as the EU but also India and China want to be seen as ethical and responsible actors within the international community, promoting international security in both foreign policy and trade.[5]

However, as has been discussed extensively in academic literature, there remains a considerable distance between claims of ethical international policies and their actual implementation in practice. This distance leads commentators to see claims of ethics in foreign policy as simply 'cheap talk' with little grounding in state practices.[6] Some even go as far as describing such claims of ethics as 'organized hypocrisy'[7] when they are simultaneously combined with massive transfers of arms. In particular when, as is the case with many arms exporting countries, they have 'not exercised export controls so as to discriminate against human rights abusing or autocratic countries during the post-Cold War period',[8] they are likely to face considerable criticism.

[4] Ron Smith and Bernard Udis, 'New Challenges to Arms Export Control: Whither Wassenaar?' (2001) 8(2) *Nonproliferation Review* 81–92.

[5] Ian A.N. Manners, 'The Normative Ethics of the European Union' (2008) 84(1) *International Affairs* 45–60; Samuel J. Spiegel and Philippe Le Billon, 'China's Weapons Trade: From Ships of Shame to the Ethics of Global Resistance' (2009) 85(2) *International Affairs* (1 March) 323–46, available at https://doi.org/10.1111/j.1468-2346.2009.00796.x; Mira Sucharov, 'Security Ethics and the Modern Military: The Case of the Israel Defense Forces' (2005) 31(2) *Armed Forces and Society* 169–99.

[6] David Chandler, 'Rhetoric Without Responsibility: The Attraction of "Ethical" Foreign Policy' (2003) 5(3) *British Journal of Politics and International Relations* (1 August) 295–316, available at https://doi.org/10.1111/1467-856X.00108.

[7] Richard Perkins and Eric Neumayer, 'The Organized Hypocrisy of Ethical Foreign Policy: Human Rights, Democracy and Western Arms Sales' (2010) 41(2) *Geoforum* (March) 247, available at https://doi.org/10.1016/j.geoforum.2009.09.011.

[8] *Ibid*. 247.

It is in this gap between the claims and the reality of ethical trade and foreign policy that numerous civil society groups have stepped in to push for states to live up to their claims of 'ethical' trade and foreign policy. One of the key areas of civil society pressure is for governments to limit exports harmful to human rights, with a specific focus on the arms trade. Here, non-governmental organizations (NGOs) play both a crucial role in drawing awareness to arms deals which seem evidently unethical, while actively advocating changes to export control regulations around the world.[9]

Specifically, NGOs' advocacy was instrumental in ensuring an increased consideration of human rights concerns within the framework of export controls. They were most successful within the EU, leading to a wide consideration of human rights in the '1998 EU Code of Conduct on Arms Exports ('EU Code'), including language on preventing exports of arms that might prolong armed conflicts or be used to violate human rights'.[10] Despite its name, the EU Code not only covered the arms trade but also additional dual-use goods and other military goods beyond arms themselves, thereby setting up a framework for the consideration of human rights within EU export controls.

Civil society advocacy was also crucial in pushing for two of the most important changes to the international export control regime: the UN Arms Trade Treaty (ATT) which was adopted in 2013 and came into force in 2014, and the 2016 EU Commission proposal for a new EU Dual-Use Export Control Regulation.[11] Both documents explicitly recognize promoting and protecting human rights as a key policy goal, reflecting the strong pressure from civil society to include these concerns in their language.

Even broad multilateral arrangements such as the Wassenaar Arrangement have increasingly reflected human-rights concerns in their decision-making. While the original Wassenaar Arrangement from 1996 does not consider human rights concerns, an additional paper which acknowledges human rights concerns was approved by the Wassenaar Arrangement Plenary in 1998. This paper, titled *Elements for Objective Analysis and Advice Concerning Potentially Destabilising Accumulations of Conventional Weapons*, includes as part of its criteria based on which arms exports should be restricted that the 'weapons might be used for the violation and suppression of human rights and fundamental freedoms'.[12]

Thus, it is possible to suggest that multilateral export controls have significantly expanded their focus on human rights since the end of the Cold War. Each of the Wassenaar Arrangement, the European Union Code and the Arms Trade Treaty provide significant relevant examples of considering safeguarding human rights as a relevant policy objective within export control mechanisms.

[9] Lerna K. Yanik, 'Guns and Human Rights: Major Powers, Global Arms Transfers, and Human Rights Violations' (2006) 28(2) *Human Rights Quarterly* 357–88.

[10] Bromley, Cooper and Holtom, 'The UN Arms Trade Treaty', n. 1 above, 1036.

[11] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast)', COM/2016/0616 (2016), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0616:FIN.

[12] Federation of American Scientists (FAS), *Destabilising Accumulations of Conventional Weapons* (FAS, 1998), available at https:// fas .org/ asmp/ resources/ interntlorgs/ Wassenaar/ AccumulationCriteria.htm#paper.

2. SURVEILLANCE TECHNOLOGIES, HUMAN RIGHTS AND EXPORT CONTROLS

It is within this context that the human rights impact of the trade in surveillance technologies began to be more widely discussed. First public debates about the highly political role of surveillance technologies took place in Europe in 2009 and 2011, in the context of protests in Iran, Tunisia, Egypt and Syria.[13] While the claim that revolutionary uprisings are in some way 'caused' by digital technologies is highly problematic,[14] it does serve to illustrate the considerable potential for human rights harms that surveillance technologies pose. In particular, revelations that European companies had provided surveillance to the governments of Iran, Syria, Egypt and Bahrain caused widespread public outrage and condemnation. Specifically:

- Nokia Siemens had exported a monitoring system for telecommunications surveillance to Iran and was accused of complicity in Iranian human rights abuses after the uprisings in 2009;[15]
- Ethiopian activist groups were targeted by software sold by German company Gamma International;[16]
- Ethiopian journalists were targeted by software sold by Italian company Hacking Team;[17]
- Nokia Siemens had exported surveillance systems to Bahrain, which were used as part of the 'arrest and torture of political opponents'.[18]

This led to a stream of statements from European politicians in 2011, such as the German Foreign Minister Westerwelle, calling for 'technology for controlling the Internet to be included in sanctions regimes',[19] and Member of the European Parliament Marietje Schaake

[13] Ben Wagner, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (Brussels: European Union, 2012), available at www.europarl.europa.eu/activities/committees/studies.do?language=EN.

[14] Ben Wagner, 'The New Media and Social Networks: Pointers from the Arab Uprisings' in Frédéric Volpi and Richard Gillespie (eds), *Routledge Handbook on Mediterranean Politics* (London: Routledge, 2016).

[15] James Farrar, 'Nokia Siemens Networks Respond to Iran Human Rights Abuses Claims', *ZDNet* (2010), available at www.zdnet.com/article/nokia-siemens-networks-respond-to-iran-human-rights-abuses-claims/.

[16] Morgan Marquis-Boire *et al.*, *You Only Click Twice: FinFisher's Global Proliferation – Citizen Lab'* (Toronto: Citizen Lab, University of Toronto, 13 March 2013), available at https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

[17] Bill Marczak, John Scott-Railton and Sarah McKune, *Hacking Team Reloaded* (Toronto: Citizen Lab, University of Toronto, 9 March 2015), available at https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

[18] Vernon Silver and Ben Elgin, *Torture in Bahrain Becomes Routine with Help from Nokia Siemens* (2011), available at www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.

[19] Guido Westerwelle, *Auswärtiges Amt – Rede von Außenminister Guido Westerwelle bei der Konferenz Umbrüche in der arabischen Welt der SWP (englisch)* (Auswärtiges Amt DE, 2011), available at www.auswaertiges-amt.de/de/newsroom/111108-bm-swp/247752.

calling for an 'Inquiry into the role of European companies in human rights violations … and the export of dual-use technologies'.[20]

EU Member States were among the main proponents of stronger regulation of surveillance technologies at the level of the Wassenaar Arrangement. This led several EU Member States in 2012 and 2013 to submit modifications to the Wassenaar Arrangement to include:

(1) mobile telecommunications interception or jamming equipment (5.A.1.f);
(2) IP network communications surveillance systems (5.A.1.j);
(3) targeted surveillance technologies/intrusion software (4.A.5, 4.D.4, 4.E.1.c).

These products adopted by the Wassenaar Arrangement entered into force in the EU on 31 December 2014, meaning that EU Member States were required to regulate the export of goods in these categories. While considerable challenges in the implementation of these controls were acknowledged by the participating states, in particular ensuring an accurate definition of the relevant software and more broadly regulating something as easily (re-) distributable as software, the controls were nevertheless implemented by numerous EU Member States across Europe.

The goal of the addition of the new entries to the Control List was to prevent such equipment or technologies being used as means of repression and state surveillance and resulting in human rights violations. However, especially the last control on targeted surveillance technologies was heavily contested by the information security community as being too broad. Numerous experts suggested that the targeted surveillance technologies control would also catch typical information security technologies, in particular 4.E.1.c, which is defined as 'Technology' for the 'development' of 'intrusion software'.

The intrusion software clause was heavily criticised by Bratus *et al.*,[21] Eleanor Saitta[22] and Dullien *et al.*,[23] as part of a public consultation by the US Department of Commerce on the US implementation of the proposed changes to the Wassenaar Arrangement. While part of the criticism stems from the very broad implementation of Wassenaar proposed by the US Department of Commerce, which went far beyond the initial controls proposed within the Wassenaar Arrangement, it was also related to the controls proposed by Wassenaar itself. This negative response led the US delegation to Wassenaar to successfully renegotiate this control in December 2017, as a result of which the scope of the revision of existing controls was considerably limited.[24] Notably, the United States has to this day not implemented this control and it remains to be seen whether they will do so after the changes that have been negotiated.

[20] Marietje Schaake, *Parliamentary Question: VP/HR – Inquiry into Role of European Companies in Human Rights Violations (Part II) and the Export of Dual-Use Technologies* (2011), available at www.marietjeschaake.eu/en/parliamentary-question-vphr-inquiry-into-role-of-european-companies-in-human-rights-violations-part-ii-and-the-export-of-dual-use-technologies?color=secondary.

[21] S. Bratus *et al.*, 'Why Offensive Security Needs Engineering Textbooks' (2014) 39(4) *Login*, available at www.usenix.org/system/files/login/articles/02_bratus.pdf.

[22] See https://dymaxion.org/essays/wa-items.html.

[23] See https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file.

[24] See www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.

In parallel to these developments at Wassenaar, the European Commission used the regulation of the trade in surveillance technologies as one of their central justifications for revising the 2009 EU Regulation 428/2009 on export controls for dual-use technologies. This development took place in several steps:

- 2013: the first European Commission report on the implementation of the existing regulation only referred vaguely to 'cyber tools';[25]
- 2014: only a year later in the EU Commission's review of export control policy, the definitions used had developed considerably to encompass 'cybertools for mass surveillance, monitoring, tracking and interception';[26]
- 2016: in the proposed new regulation of export controls, surveillance technologies are extensively defined as 'items specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system'.[27]

However, what is notable about the European Commission's approach is not just the expanding definition, but also inserting additional regulatory mechanisms into the regulation which exclusively deal with surveillance technologies. These additional regulatory mechanisms are as follows.

(1) *An EU autonomous list for surveillance technologies*: in almost all cases of dual-use goods, the EU simply copies existing regulatory categories of items to regulate from the Wassenaar Arrangement. This is to ensure the widest possible number of countries end up regulating the same item, rather than any one country 'going it alone'. In the case of surveillance technologies, the EU has proposed to create an autonomous list specifically for surveillance technologies.

(2) *Targeted catch-all control*: almost all export controls are based on specific lists of clearly defined goods, to ensure legal certainty for exporters. The only exceptions that typically exist to this rule are items where there is a significant danger to international peace and security, such as items associated with chemical, biological or nuclear weapons, national arms embargos, or items likely to be used by the military. On top of these reasons for restricting the trade in dual-use items included in article 4 of the 2009 EU Regulation 428/2009, the new 2016 European Commission proposal includes additional language covering 'where there is evidence that the items may be misused by the proposed end-user for directing or implementing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination'.[28]

These two additional mechanisms are designed to show that the EU is serious about regulating the international trade in surveillance technologies. If either or both of these two measures are

[25] See http://trade.ec.europa.eu/doclib/docs/2013/october/tradoc_151857.pdf.

[26] See http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf.

[27] See http:// eur -lex .europa .eu/ resource .html ?uri = cellar: 1b8f930e -8648 -11e6 -b076 -01aa75ed71a1.0013.02/DOC_1&format=PDF.

[28] See http:// eur -lex .europa .eu/ resource .html ?uri = cellar: 1b8f930e -8648 -11e6 -b076 -01aa75ed71a1.0013.02/DOC_1&format=PDF.

implemented in the final EU Regulation they would go considerably beyond existing export control regimes elsewhere in the world in safeguarding human rights and limiting the spread of surveillance technologies.

3. IMPLEMENTING EXPORT CONTROLS OUTSIDE THE 'WASSENAAR CLUB': INDIA AND CHINA

However, it is possible that much of what is developed in export control frameworks is just a rhetorical smoke screen.[29] Indeed, there are frequent claims that both arms and export control frameworks are not actually implemented in any meaningful way and thus serve simply as a fig-leaf to feign interest in international peace and security and human rights.[30] While there are doubtless numerous deficits in existing export control and arms control frameworks, it is also too simple to simply dismiss them out of hand as playing no role whatsoever in safeguarding either international peace and security or human rights.

This does not mean that claims of 'organized hypocrisy'[31] with regard to the frequent exports of arms to heavily human rights infringing countries are necessarily false, but rather that existing export control policies do not support claims of ethical foreign policy agendas. States continue to follow economic self-interest in how they operate, however, they may in some cases be willing to limit this self-interest in order to safeguard human rights. As Bromley *et al.* suggest:

> [a]rms trade agreements do not have to be grand moral projects … they are more likely to succeed when the security subjectivities of policy-makers and ethical ideals of campaigners are complementary.[32]

A question which is equally relevant that should be asked in this context is what international trade would look like without any forms of export control present at all. Here, one of the crucial questions is related to the implementation of export controls, i.e., the willingness of states to actively implement their widely-stated commitments to safeguard both international peace and security and human rights. While this data is patchy, there is some indication that some states implement numerous export controls even though they are not explicitly required to restrict those items under international law.

This even extends to non-members of the Wassenaar Arrangement, such as China or India which have no control over the norms that are set within the Wassenaar Arrangement, but still choose to implement them. As a result, these two countries provide a fascinating case to explore further in order to understand the quality of implementation of export controls outside of countries which have passed legally binding legislation, such as the EU Member States. The following section will look at the implementation of multilateral export control regimes in general before focusing on specific provisions for surveillance technologies.

[29] This section was developed with support from Stéphanie Horth.

[30] Chandler, 'Rhetoric Without Responsibility', n. 6 above.

[31] Perkins and Neumayer, 'The Organized Hypocrisy of Ethical Foreign Policy', n. 7 above, 247.

[32] Bromley, Cooper and Holtom, 'The UN Arms Trade Treaty', n. 1 above, 1034.

3.1 India

Export control laws in India provide statutory authority to its licensing and enforcement departments. India's current legal framework is on a par with global best practices in export controls. Parts of the regulation are adapted from legislation worldwide; many changes have been made in the last decade.[33] The procedures are defined, implemented and regulated by the Directorate General of Foreign Trade (DFGT) within the Department of Commerce and Industry. The main laws regulating export control are the amended Foreign Trade (Development and Regulation) Act No. 22 of 1992 (which was amended in 2010[34]). The Act attributes to the DFGT the power to define items on the Indian Tariff Classification (ITC) list and also license the import and export of items found on the list. There is also a list specifically dedicated to dual-use technologies; the list is referred to as the Special Chemicals, Organisms, Materials, Equipment, and Technologies (SCOMET) list.[35] Export of cybersurveillance technologies could either fall within the SCOMET list under 'Category 7 Electronics, computers, and information technology including information security',[36] or the regular export list. The list does not yet include the items that were recently added to the Wassenaar Arrangement, such as 'intrusion software, telephone interception, jamming and monitoring equipment, etc.'.

Since India has expressed its interest in joining the Wassenaar Arrangement as well, we can assume that they will be implementing the changes, as they have with other export control regimes in order to adhere to the international export control regimes. If the Government of India wishes to join the multilateral export control regimes, it must adapt its own regime and adjust the national control list and SCOMET list with all the multilateral regimes. Currently, the Indian legislation does not explicitly address deemed technology exports; for the Wassenaar Arrangement, it could expand the scope of its technology transfer and brokering in order to apply it to conventional arms-related as well as dual-use activities.[37]

In the summer of 2015, India officially applied to become a member of the Missile Technology Control Regime (MTCR), a group that currently counts 34 members. The goal of the regime is to limit the risks of proliferation of weapons of mass destruction through control of the transfers. Even though India is not yet a member, it has still pledged to adhere to its guidelines.[38] India's wish to join the MTCR and other international export regimes was backed up by a powerful ally; Barack Obama declared during a state visit to India in 2010, that he supported India's aim to join several important export control regimes: the Nuclear Suppliers Group, the Missile Technology Control Regime, the Wassenaar Arrangement, as well as the

[33] See www .kcl .ac .uk/ sspp/ departments/ warstudies/ research/ groups/ csss/ pubs/ India -export -control.pdf.

[34] See http:// dgft .gov .in/ exim/ 2000/ Foreign _Trade _(Development _ & _Regulations) _Amendment_Act_2010.pdf.

[35] See http://cis-india.org/internet-governance/blog/export-and-import-of-security-technologies -in-india.pdf.

[36] See http://cis-india.org/internet-governance/blog/export-and-import-of-security-technologies -in-india.pdf.

[37] See www .securustrade .com/ India's %20Export %20Controls _Article _ _July _10 _2011 _FINAL.pdf.

[38] See www.nti.org/learn/treaties-and-regimes/missile-technology-control-regime-mtcr/.

Australia Group (AG).[39] The United States, however, requires that for India's adhesion to the AG and Wassenaar Arrangement, India must reflect the existing regimes in its own legislation in order to be considered for full membership – all items listed in those regimes should therefore be covered by India. This support was once again reiterated in January 2015,[40] which led to a 2017 application by India to join the Wassenaar Arrangement which was accepted at the 2017 plenary meeting on 7 December 2017. As a result, India joined the Wassenaar Arrangement following all procedural changes on 8 December 2017.

Regarding the addition of cyber-technology to the Wassenaar Arrangement's dual-use control list, Indian officials have expressed concern that this could have a negative impact on India's cybersecurity programme, both software and hardware, as they would fall under the export control regime and it may result in denying products to Indian organizations.[41] Some have expressed concern that the recent modifications of the Wassenaar rules regarding cybersecurity could result in a difficult bilateral dialogue on issues concerning cybersecurity and Internet governance, and have questioned whether the political costs of adhering to these new regulations would be strategically worth it for India.[42]

3.2 China

Since the mid-1990s, China has undertaken several steps to regulate and limit the export of military-related products, chemicals, biological agents, and missile-related technologies. This was a major change in direction in comparison with the early 1980s, when the export controls on WMD (weapons of mass destruction) goods and technologies was severely lacking. Due in part to increasing international pressure, and a desire to improve its international reputation, the Chinese government decided to take steps in order to improve its export control regime. This resulted in new domestic decrees and regulations, as well as the amelioration of its administrative structures for non-proliferation and arms control. Another important factor was the recognition by Chinese officials that promoting multilateral, regional and bilateral agreements of all kinds plays a key role.[43]

Nonetheless, many doubts remain regarding China's current and long-term export control policies and whether they align with existing international instruments. In some cases, although the Chinese government made changes domestically in order to closely simulate international instruments, it still remains an outsider. In 2002, China created export control regulations that are said to be parallel to the structures of the Missile Technology Control Regime (MTCR). Its membership has, however, been under review since then. Similarly, in 1998, China expanded

[39] See www.whitehouse.gov/the-press-office/2010/11/08/joint-statement-president-obama-and-prime-minister-singh-india.

[40] See www.whitehouse.gov/the-press-office/2015/01/25/us-india-joint-statement-shared-effort-progress-all.

[41] See www.thehindubusinessline.com/info-tech/new-export-control-law-could-threaten-indias-cyber-security-programme/article6130704.ece.

[42] See www.thehindu.com/opinion/columns/wassenaars-web-a-threat-to-technology-transfer/article7499748.ece.

[43] For more information, see www.gov.uk/government/publications/analysis-of-chinas-export-controls-against-international-standards/bridging-the-gap-analysis-of-chinas-export-controls-against-international-standards.

its export control of dual-use chemicals, nonetheless it is not yet a member of the AG. Additionally, although China has iterated its intention to limit the export of dual-use goods and technologies, it is not yet a member of the Wassenaar Arrangement.[44] A considerable obstacle is the lack of comprehension on the part of the international community of the Chinese export control regime, with little material available in English and a complex and not very transparent decision-making process; it is difficult to accurately compare the regime with existing multilateral agreements such as the MTCR, AG and the Wassenaar Arrangement.

The export control of dual-use items and technologies in China has been developing in recent years; in 1998, the State Council adopted its first set of export control regulations, which covered 183 dual-use goods and technologies. In 2002, it amended the regulations to widen its span and include the majority of the Wassenaar Arrangement's List of dual-use goods and technologies. In 2010, the Index of Management of Import and Export Permits of Dual-Use Items and Technologies came into effect and covered nuclear, biological, chemical and missile-related dual-use goods and technologies. Another recent development was announced by the new Bureau of Industry Security, Import, and Export Control, indicating that a new control list for conventional arms and dual-use goods and technologies is being worked on and should be released shortly. The list is periodically reviewed and updated. As an example, in January 2015, China's dual-use control list had 816 items, whereas the Wassenaar Arrangement had a little over 1,000 items.[45]

In order to improve its enforcement mechanism for dual-use items, the Chinese government has taken several important steps: in 2002, it created a 'watch list' listing companies that made illegal transactions of sensitive items; in 2004, a computer-based control system for the export of sensitive items was created, and in its approval step the Ministry of Commerce created a national expert support system, hence creating a network allowing scholars and exports from different sectors to exchange, and thus enhancing the decision-making on some licence applications that require in-depth knowledge. The Ministry of Commerce has also reached out to industry in order to raise knowledge of export control regulations and policies, also holding seminars to give better insight into the political aspects of export control and providing training on more technical aspects.[46]

A workshop was held in September 2015, and present at this workshop were the Technical Expert Working Group (TEWG) made up of 12 policy experts and practitioners from Russia, the United Kingdom, the United States, Korea and China, who emphasized the importance of having an up-to-date control list of dual-use items and technologies. The participants agreed that China has already adopted advanced procedures for dual-use export control, and that international practices such as appointing a legal authority in charge of controlling the export of dual-use items and technologies, licensing processes, coordination between different agencies, end-user certification, as well as catch-all mechanisms, are already applied in China. It was nonetheless remarked that China's dual-use export control is still in a development phase and

[44] See www .gov .uk/ government/ publications/ analysis -of -chinas -export -controls -against -international-standards/bridging-the-gap-analysis-of-chinas-export-controls-against-international -standards.

[45] See www .saferworld .org .uk/ resources/ view -resource/ 873 -expanding -and -sustaining -dialogue-between-china-and-the-wassenaar-arrangement.

[46] See www .saferworld .org .uk/ resources/ view -resource/ 873 -expanding -and -sustaining -dialogue-between-china-and-the-wassenaar-arrangement.

that several challenges remain before China reaches the next phase of export control policy; the technical experts therefore agreed to continue sharing information on best practices in export licensing mechanisms.

For example, the experts agreed that it was key for China to maintain an up-to-date control list that corresponds to existing international regimes, mainly the Wassenaar Arrangement. It was also noted that communication and information sharing between China and key international regimes should be improved.[47] Additionally, a further two-day workshop on strengthening the implementation of dual-use and arms trade control was held in January 2016. The workshop was attended by Chinese practitioners, officials and academics, as well as some Wassenaar Arrangement Participating States.[48] The goal of the workshop was to increase dialogue and cooperation between the two export control regimes, the Chinese and the Wassenaar Arrangement.

China's export control regulations on conventional arms are largely consistent with the control policies of the Wassenaar Arrangement; the list for dual-use goods and technologies, however, does not yet cover the comprehensive list of the Arrangement. A more complete list is needed, and Chinese officials have mentioned that since its list of conventional arms mostly covers the items of the Arrangement, some fail to see the point in joining the Wassenaar Arrangement – it seems that the failed attempt at becoming a member of the MTCR has left many doubting if they should apply to be part of the Wassenaar regime.

At the same time, China's export control regime has considerable weaknesses. One of the main weaknesses of China's export controls is the lack of enforcement – monitoring, investigation of violations, and penalization is lacking. Often the authorities merely react to intelligence data received from the United States, the United Kingdom, or the European Union. Furthermore, Chinese officials do not actively pursue investigations concerning large state-owned businesses, and lack of transparency is often an issue which makes it difficult to accurately assess the enforcement of export control policies. Chinese officials have declared their wish to increase their enforcement efforts; an example of recent enforcement occurred when two companies were penalized for having had initial contact with the Libyan government in 2011.[49]

To encourage China's participation in export control regimes, dialogue is key. Members of the international community must continue their outreach and assist China in further developing, implementing and enforcing its control list to reflect international standards; furthermore, capacity-building activities should be prioritized between experts, practitioners, and officials and participants from China in order to encourage sharing knowledge and promoting efficient enforcement of export control policies.[50]

[47] See www .saferworld .org .uk/ resources/ view -resource/ 1026 -sharing -perspectives -on -achievements-and-challenges-relating-to-export-controls-of-dual-use-items-and-technologies.

[48] For more information, see www .saferworld .org .uk/ resources/ view -resource/ 1059 -strengthening-technical-and-operational-capacity-to-implement-and-enforce-dual-use-and-arms -trade-controls.

[49] See www .gov .uk/ government/ publications/ analysis -of -chinas -export -controls -against -international-standards/bridging-the-gap-analysis-of-chinas-export-controls-against-international -standards.

[50] For policy recommendations, see www .saferworld .org .uk/ resources/ view -resource/ 873 -expanding-and-sustaining-dialogue-between-china-and-the-wassenaar-arrangement.

3.3 India and China: Conclusion

The implementation of export control regimes is obviously difficult outside of binding regimes such as the EU. This is particularly the case when countries like China or India are not even part of the regimes which define the norms, i.e. they are signing up to be part of technology arrangements where they themselves do not control the norm-setting. On the face of it, this is highly perplexing behaviour in the international environment. This is one of the great misunderstandings of export control regimes such as the Wassenaar Arrangement, which are assumed to be completely ineffectual, or as Innokenty Pyetranker put it, an 'umbrella in a hurricane'.[51] On the basis of simply a rational economic or institutional analysis, there seems to be no good reason for either China or India to implement export controls such as those proposed in Wassenaar. The question that should be asked in this context is why they adhere to the Wassenaar Arrangement at all. After all, why should states agree to be bound by regularly updated norms that they do not even themselves control?

The answer to this question perhaps lies in a dual wish to be a 'good actor' within the international community, as well as genuine self-interest to prevent complete proliferation of all technologies without any restrictions. Assuming at least some genuine self-interest of states exists, the Wassenaar Arrangement becomes a useful norm-setter that reduces the costs of developing a state's own set of norms in a way that is broadly agreed internationally. For sure, this does not mean that economic interests may not also exist, but rather that these interests may sometimes be limited. Even in countries that implement export controls well, the significant majority of requests to export goods or services are accepted rather than rejected, a percentage that is likely to be even higher in countries with low quality implementation of export controls. The reason for export controls is not to try to completely stop trade, but rather to make the misuse of certain goods more difficult. Thus, overt assumptions of perfect compliance and complete adherence are part of the problem, a point acknowledged by Pyetranker, who went on to admit that '[h]aving an umbrella in a hurricane is better than having nothing at all'.[52] In fact, given the strong economic incentives that oppose it and its weak institutional framework, the Wassenaar Arrangement has been remarkably successful in spreading the norms that are set by it.

In the case of China and India, the reasons behind adherence to the Wassenaar regime are different but lead to significant levels of compliance greater than zero. Both countries have been put under pressure by other countries around the world and civil society to improve their export controls, pressure which seems to be bearing fruit. However, this pressure alone is clearly not enough, and some degree of self-interest to prevent mass instability in international peace and security can also be expected. With India, this even led to India eventually becoming a Wassenaar participating state, joining the Arrangement in December 2017. China has not gone this far but is clearly making additional efforts to improve the state of export controls in the country. While neither country seems willing to call into question their fundamental economic or national security interests in order to do so, it does seem that there is a basic

[51] Innokenty Pyetranker, 'An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement' (2015) 13 *Nw. J. Tech. and Intell. Prop.* 153.

[52] *Ibid*. 180.

willingness to limit technology exports and actively enforce in a multilateral control regime, even if neither country was not until very recently formally part of it.

4. ONGOING CHALLENGES IN EXPORT CONTROL REGIMES OF SURVEILLANCE TECHNOLOGIES

Beyond questions of general implementation, there are numerous other challenges related to the regulation of the trade in surveillance technologies through export controls. These challenges can also be seen as a roadmap for relevant next steps in the debate. If export controls are to ensure their international legitimacy and effectiveness, some additional considerations may be helpful.

4.1 Human Security versus Human Rights

One of the most notable shifts within the debate about export controls is from human security to human rights. In order to understand where this shift comes from, however, it is first important to understand the development of the human security concept.[53] A narrative focused on security alone can have adverse consequences on human rights when it leads to states altering laws and upgrading capabilities that allow them to interfere with the freedom of expression and the right to privacy. A different narrative that has gained attention among academics and practitioners alike is that of human security. According to Simon Dalby, the concept of human security has four key characteristics. First, much like human rights, it is a universal concept without geographical restrictions. Second, it understands various aspects of security as mutually interdependent. Third, human security is closely related to the notion of risk, and operates through the logic of prevention. Fourth, human security introduces a narrative shift of the referent object of security from the state to the individual level, making it about people.[54]

However human security has also been heavily criticized as a vehicle for a securitization of human rights narratives.[55] These concerns are shared by many in the civil society sector, who continue to feel uncomfortable with the term. 'Despite such conceptual difficulties, many NGOs have actively referenced human security language and principles in a wide range of campaigns.'[56]

Notably, the human security justification was at the core of the European Commission's review of export control policy in 2014, where the Commission proposed to shape its entire export control policy around the concept of human security in suggesting that: 'The Commission will consider evolving towards a "human security" approach recognising that security and human rights are inextricably interlinked'.[57] However, in the final Commission

[53] Parts of this section were developed with support from Thomas Behrndt.

[54] Simon Dalby, *Geopolitical Change and Contemporary Security Studies: Contextualizing the Human Security Agenda* (Institute of International Relations, University of British Columbia, 2000).

[55] S. Watson, 'The "Human" as Referent Object?: Humanitarianism as Securitization' (2011) 42(1) *Security Dialogue* (March) 3–20, available at https://doi.org/10.1177/0967010610393549.

[56] Bromley, Cooper and Holtom, 'The UN Arms Trade Treaty', n. 1 above.

[57] See http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf.

Proposal of an export control regulation in 2016, human security is nowhere to be found.[58] This is in no small part due to pressure from civil society to emphasize human rights rather than human security, and pressure from EU Member States concerning a vague and unspecific concept. It seems that both civil society and the EU have learnt from previous extensive usage of the concept of human security and based on the widespread criticism[59] decided to focus on human rights instead.

Interestingly, this criticism in many ways mirrors similar concerns that exist about the term 'cyber'.[60] Like human security, which attempts to shift the referent object of security from the state to human beings, cybersecurity attempts to expand the concept of security beyond security of devices to also encompass human beings, states and societies. Also similarly to cybersecurity, human security brings a heavy danger of securitizing all objects it touches and is only able to function 'within the logic of militarism from above'.[61] Finally, there is the not entirely unreasonable claim that both the concept of cybersecurity and human security have been co-opted and institutionalized to a considerable degree, as a result of which both should be treated with considerable caution with regard to potential effects and side-effects.[62] Both have become so broad and vague that they are increasingly indeterminate, as it is possible to justify a vast number of potential actions within their scope. Happily, many of the most recent export control regimes in the EU and under the Wassenaar Arrangement recognize this, as a result of which the concept of human security is increasingly being side-lined in favour of human rights.

4.2 Whither 'Crypto' in Export Controls?

The 'historic sin' in the context of technology regulation by export controls are the measures to regulate cryptography in the mid-1990s. As part of what were termed the 'crypto-wars' in the 1990s, there were numerous steps to limit the spread of encryption technologies, with export controls of cryptography and publicly enforced key escrow mechanisms two of the key measures to implement restrictions of cryptography.[63] These measures were not only highly harmful to the development and spread of cryptography at the time, they had negative effects even decades later. This is because some of the cryptographic technologies developed

[58] See http:// eur -lex .europa .eu/ resource .html ?uri = cellar: 1b8f930e -8648 -11e6 -b076 -01aa75ed71a1.0013.02/DOC_1&format=PDF.

[59] See e.g., David Chandler and Nik Hynek (eds), *Critical Perspectives on Human Security: Rethinking Emancipation and Power in International Relations* (Routledge, 2010).

[60] Ben Wagner and Kilian Vieth, 'Was Macht Cyber? Epistemologie Und Funktionslogik von Cyber' (2016) 9(2) *Zeitschrift Für Aussen- Und Sicherheitspolitik* 213–22.

[61] Mandy Turner, Neil Cooper and Michael Pugh, 'Institutionalised and Co-Opted: Why Human Security has Lost Its Way' in David Chandler and Nik Hynek (eds), *Critical Perspectives on Human Security: Rethinking Emancipation and Power in International Relations* (Routledge, 2010) 87.

[62] *Ibid*.; Wagner and Vieth, 'Was Macht Cyber?', n. 60 above.

[63] Whitfield Diffie and Susan Landau, *The Export of Cryptography in the 20th Century and the 21st* (Sun Microsystems, 2001); EPIC, *Cryptography and Liberty 1999: An International Survey of Encryption Policy* (1st edn, Washington, DC: EPIC, 1999).

in a manner to allow them to be exported in the 1990s were still in use several decades later, making it very easy for these 'export grade' implementations to be attacked technically.[64]

The resulting attacks may not have been a surprise for some companies, who freely admit that they wouldn't 'touch EXPORT-grade cryptography with a 20ft stick',[65] however, it does exemplify how regulations on cryptography had served to make communications on the Internet insecure. This also had a negative effect on human rights, as cryptography is a key technology to safeguard many important human rights.[66] This is because key rights such as privacy, free expression or even human dignity require a technical foundation. One of the key components of this technical foundation is cryptography, as it allows human beings to have access to a protected space in which their thoughts, ideas and interactions are genuinely private. As more and more forms of human interaction and communication transition online, they are increasingly subject to a wide variety of surveillance. Without technical safeguards against such cryptography, it is essentially impossible to have meaningful access to both privacy and other key human rights in a digital age.

Notably, it was the US Department of Commerce that began implementing regulations of cryptography unilaterally in 1996. By contrast, the 'OECD Guidelines on Cryptography Policy and the European Commission expressed strong support for the unrestricted development of encryption products and services'.[67] Similar national statements of support for cryptography without regulation were made by Canada, Ireland, Finland and France,[68] suggesting strong international opposition. Despite considerable international opposition, the Wassenaar Arrangement passed restrictions on 'encryption software and hardware having keys longer than 56-bits'.[69] To a considerable degree, these encryption controls are still in force to this date, with the Wassenaar Arrangement continuing to regulate 'cryptography for data confidentiality' having 'in excess of 56 bits of symmetric key length'.[70]

Having been the main proponent of regulating encryption at an international level and restricting internationally traded cryptography to 56-bits in 1998, the United States then decided two years later to liberalize its own national export controls in January 2000.[71] Barely 13 months after they had convinced large parts of the rest of the world to regulate cryptography in the Wassenaar Arrangement, they then decided that they would no longer apply the rules they had fought for. While this was 'seen by industry as a victory',[72] as well as by civil society

[64] David Adrian *et al.*, 'Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice' in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (ACM, 2015) 5–17.

[65] Filippo Valsorda, 'Logjam: The Latest TLS Vulnerability Explained', Cloudflare Blog, 20 May 2015, https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained/.

[66] EPIC, *Cryptography and Liberty 1999*, n. 63 above; Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/23/40 (Geneva: United Nations, 2013).

[67] EPIC, *Cryptography and Liberty 1999*, n. 63 above.

[68] *Ibid*.

[69] See http://gilc.org/crypto/crypto-survey-99.html.

[70] See www .wassenaar .org/ wp -content/ uploads/ 2017/ 12/ 2017 _List _of _DU _Goods _and _Technologies_and_Munitions_List.pdf.

[71] Diffie and Landau, *The Export of Cryptography in the 20th Century and the 21st*, n. 63 above.

[72] *Ibid*.

which had been fighting hard to lift these restrictions, the victory was primarily limited to the United States. As the Wassenaar Arrangement had not changed, it was used by numerous states in Europe and around the world as an excuse to regulate cryptography.

This state of affairs was not challenged until more recent debates about export controls of surveillance technologies in Europe, as part of which both civil society, industry and the European Parliament actively fought for the relaxation of restrictions on cryptography within the 2016 revised export control regulation. Specifically, it was suggested to provide a European Union General Export Authorization (EU GEA) for cryptographic products, thereby ensuring that export controls would not apply to them. This also explicitly intends 'to delete cryptography items from the relevant international control lists as soon as possible'.[73] While such controls are still part of the Wassenaar Arrangement, this move represents a considerable step towards actually ending the regulation of cryptography through export controls, not just in the United States but everywhere else in the world as well.

4.3 Transparency, Participation, Governance

The post-Cold War expansion of export controls brought with it a considerable expansion of transparency in the way that export controls are managed. Particularly, the Wassenaar Arrangement and the European Union made a strong effort to be as transparent as possible in the way they managed their export control lists. This was a considerable step for the post-COCOM regime Wassenaar, which had been used to keeping the goods it controls secret. This sea-change in transparency meant that it was now acceptable to make publicly available the dual-use list of items being controlled, including key elements of numerous arms being controlled and parts of chemical and nuclear weapons whose export was being restricted.

However, what may have seemed to be wide-ranging transparency in the early 1990s for a post-Cold War regime is far from the rigorous standards of transparency expected of public sector organizations in 2018. As time progresses, this increasingly makes the Wassenaar Arrangement look like a Cold War dinosaur, with closed door meetings that are impossible to attend and where neither minutes nor agendas nor lists of participants are publicly available. In comparison even to other international organizations also focused on security, like the Organization for Security and Co-operation in Europe (OSCE), the Wassenaar Arrangement is far from a model of transparency. This is in part because the organization has not yet embraced its new role of also dealing with non-military questions of dual-use. As questions of dual-use technologies become more and more societally relevant, they cannot be made behind closed doors by an organization that only publishes the results of its deliberations. The same goes for the participation of non-state actors, something that has become par for the course in many international organizations but is still viewed as unimaginable within the context of the Wassenaar Arrangement.

While far from perfect models of participation and transparency, the OSCE, the United Nations and even the International Telecommunication Union (ITU) demonstrate that it is perfectly possible for international organizations to negotiate international agreements transparently and integrate non-state actors into their deliberations. This is particularly evident

[73] See https://marietjeschaake.eu/en/european-parliament-adopts-position-on-export-control-reform.

within the European Union, which is at pains to consult all relevant stakeholders, and involve them in the process of assessing and developing new regulations in the area of dual-use. For Wassenaar to function in the future it will need to become similarly transparent and ensure it takes the participation of a broad set of stakeholders seriously.

This also extends to greater transparency in the export control licensing decisions of Wassenaar member states. If the United Kingdom and Finland are capable of publishing their licensing decisions on the Internet, there is no reason why Germany and India cannot do the same. Greater transparency in actual export control licensing decisions both increases the legitimacy of the export control decision-making process and shows other Wassenaar member states that the state which is making the decisions transparent takes its international commitments seriously.

Finally, providing public access to export control licensing decisions makes a more accurate assessment of the overall quality of export control implementation more meaningfully possible. Initial provisions for better information exchange between states are present in the 2016 revision to the EU dual-use export control regulation, but far more needs to be done to ensure actual transparency both in the EU and among Wassenaar member states.

4.4 Expanding and Developing the Wassenaar Arrangement

While the EU and other regional organizations can doubtless be improved, the centrality of the Wassenaar Arrangement in global export controls means that Wassenaar, more than any other international agreement, defines the quality of the international export control regime. This also means that considerable changes can and should be made within the existing arrangement to improve the overall global export control regime.

The first and perhaps most important step is inviting new members to join the Wassenaar Arrangement. Here, India is an excellent example, which in 2015 was rumoured to be interested in 'at some point' joining the Arrangement, and by the time the first edition of this chapter had been completed in 2018 it had already joined the Wassenaar Arrangement. This swift process is by no means typical, and Wassenaar member states, in the spirit of their block-oriented Cold War COCOM past, often still see the Wassenaar Arrangement as their own private club. This will need to change dramatically to ensure that other countries which are leading exporters of dual-use goods, such as Israel or China, can join the club. In order to do this, Wassenaar should both more actively attempt to include new member states, and improve the accession process to make it easier to move from complete or close regulatory alignment that already exists to a considerable degree in countries like Israel or China, to full membership of the Arrangement. Membership of the Wassenaar Arrangement should not be misused as a political bargaining chip – it is also an essential instrument to safeguard international peace and stability and increasingly to protect human rights.

4.5 Expanding the Arms Trade Treaty to Include Dual-Use Items

In the long term, however, there is another mechanism that could well – in decades to come – take over from the Wassenaar Arrangement as the central instrument of dual-use export controls. The Arms Trade Treaty (ATT) has several key advantages over the Wassenaar

Arrangement which in the long term could make it a more feasible mechanism for negotiating international export controls:

(1) the ATT has a far broader base of member states than Wassenaar, with 92 states having ratified the treaty;
(2) the ATT is a legally binding international treaty rather than a non-binding arrangement like Wassenaar;
(3) the ATT treaty organization is a UN framework organization, meaning that it exists within a stable international framework and follows UN rules and procedures. This inherently provides for greater transparency and access by non-state actors than is the case in the Wassenaar Arrangement.

However, at present the ATT does not regulate dual-use goods but simply conventional arms. In order for the ATT to do this, an additional protocol would be required to also apply the ATT to dual-use goods, the development and ratification of which is likely to take decades rather than years. At the same time, the fundamental value of such a long-term project means that it seems perfectly plausible and achievable, if some Wassenaar and ATT member states are willing to take a long-term perspective to ensure an effective international export control regime. While this is, of course, a challenging long-term issue, it also illustrates the time that it takes to develop institutions at an international level.

5. CONCLUSION: NOT A PANACEA

While the future development of export controls seems hard to ascertain, this chapter has attempted to provide an overview of the development of export control regimes in the last two decades, with a focus on the role of human rights and digital technologies.

While many of the steps suggested to improve existing export control regimes are likely to take considerable time to implement, they are anything but impossible and are reflective of what remain relatively 'young' regimes (by international standards) which only began to flourish and meaningfully consider human rights several decades ago. Only by taking a very long-term perspective is it possible to effectively ensure the development of international institutions in this area, as such changes take years or even decades to agree on and implement.

Export controls are not a panacea for all of the human rights challenges associated with modern technologies, there are also many other measures states can and should take to contribute to international peace and security and promote human rights.[74] While they may not be the obvious mechanism of choice, they have become a powerful way of inserting human rights into international trade. Thus, export controls, when implemented correctly, can meaningfully contribute to limiting the spread of surveillance technologies.[75]

In an era in which states like to claim there is little they can do to safeguard human rights online, it is possible to remind them that this is one of the key mechanisms they do have

[74] For an overview, see Wagner, *After the Arab Spring*, n. 13 above.

[75] See Lasse Skou Andersen and Laura Dombernowsky, *Danmark åbner for eksport af netovervågning til Kina* (Information, 2016), available at www.information.dk/indland/2016/07/danmark-aabner-eksport-netovervaagning-kina.

control over. In reminding states of their human rights obligations, international civil society should continue to be wary of the human security concept and its ability to safeguard human rights. This does not mean, however, that it is not worth working together with established institutional structures. If anything, the experience with export controls suggests that support for human rights norms can come from the most unlikely places and through mechanisms that are not immediately obvious.

If the urgency of the challenges associated with the Internet and human rights are taken seriously, however, the mainstreaming of human rights across all domains becomes even more important. No regulation, law or arrangement can claim to be separate from or outside of the scope of these challenges, whether they are related to security, global trade or foreign policy. This does not mean that institutional failure or conflicting interests do not exist, but rather that the meaningful and systematic consideration of human rights can and should happen at all levels. Only by acknowledging this need and systematically addressing it, is it possible to respond to the challenges of the Internet and human rights in a sustainable and effective manner.