Emerging Technologies and Competition in the Fourth Industrial Revolution: The Need for New Approaches to Export Control

BRIGITTE DEKKER AND MAAIKE OKANO-HEIJMANS[1]

Abstract

Amid intensifying Sino-U.S. competition for technological leadership and geopolitical hegemony, the U.S. government in August 2018 announced the Export Control Reform Act (ECRA) tailored to so-called emerging technologies. This unilateral push caused uncertainty with governments worldwide as well as within the current Multilateral Export Control Regimes (MECRs), in particular the Wassenaar Arrangement (WA). This article posits that innovative approaches to export control are needed to deal with new challenges posed by today's emerging technologies. Lacking a broad consensus on the potential military and civilian uses of emerging technologies, these technologies are arguably "omni-use" rather than "dual-use" in character. Moreover, the rise of new security concerns and ethical considerations – including related to human rights – is blurring the lines between economic and national security. A case study of the Netherlands, a global leader in various high-tech sectors, illustrates the challenges of dealing with these changes and the U.S. push for action. Voluntary, principles-based arrangements are needed to complement governments' efforts within the formal export control regimes. Building on theories of transnational global governance, trusted communities are highlighted as a particularly valuable instrument to engage relevant stakeholders, in particular from the private sector.

[1] Brigitte Dekker, MA, is a Research Fellow at the Netherlands Institute of International Relations "Clingendael" in The Hague. Her research focuses on various dimensions of EU–Asia relations, with a specific interest in South-East Asia and China. Maaike Okano-Heijmans, PhD, is a Senior Research Fellow at the Netherlands Institute of International Relations "Clingendael" in The Hague. She is also a Visiting Lecturer at the University of Leiden and a Scientific Coordinator of the Asia–Pacific Research and Advice Network, advising EU institutions. Her research primarily focuses on connectivity and global economic governance in EU–Asia relations.

Introduction[1]

Export control is best defined as restrictive measures that governments implement to limit the spread and/or use of certain goods and services with the ultimate aim of protecting national security and promoting foreign policy. It is a supply-side measure, originally established by the United States and its allies to control the outflow of military equipment and dual-use items – items that can be used for both military and civil purposes – to the Communist bloc during the Cold War. Today's negotiations about export control are complicated by greater interdependence of the U.S., Chinese, and European markets, meaning that new export controls will have far greater implications for existing trade flows. Since then, four multilateral export control regimes (MECRs) have been established and over 50 countries have developed comprehensive export controls on dual-use items drawing upon the lists of the MECR.[2]

Today, emerging technologies pose a new challenge to the existing MECRs, particularly for the Wassenaar Arrangement (WA) which deals with conventional arms and dual-use goods and technologies. Emerging technologies, as such, are not a new phenomenon – the world has seen tremendous technological developments in recent decades. Three key characteristics of emerging technologies today, however, distinguish them from the technologies for which the existing export control measures were originally designed. These are the digital, intangible nature of the emerging technologies; the fact that the private sector plays the lead role in developing emerging technologies; and the use of these intangible technologies in a broad range of civil and military applications, making them increasingly omnipresent in society. These characteristics are key reasons why the existing regimes – and the traditional, government-led approach to export control – are increasingly challenged to adjust norms and regulation in a way that keeps up with rapid changes in the nature and origin of technologies, as well as modes of power.

While traditional export control mechanisms – customs and licensing – are increasingly unfit tools to regulate fast-changing digital technologies, the changing context is adding a further challenge to the MECRs. Historically, export control regimes have been established to counter possible security threats related to the export of certain items to specific end-uses, users, and destinations of concerns. Now the stakes are even larger as the norms and standards for the use of the now-emerging technologies are not yet defined, leading to a race for technological supremacy. This changing context seems to be at the core of the Sino-American trade-tech conflict and is an important explanatory factor as to why the United States has, since late 2018, has been pushing the debate forward by way of its Export Control Regulation Act (ECRA). ECRA lists fourteen technology categories that the U.S. government may subject to export control regulations in the future. This unilateral push complicates any effort to find a consensus between the various countries and stakeholders, as well as the members of the WA. For example, many European countries do not fully share U.S. concerns about certain countries such as Iran, and do not wish to resort to protectionist policies to contain China, even if the U.S. is Europe's

[1] This article builds on a policy-oriented publication by the authors on the topic: Brigitte Dekker and Maaike Okano-Heijmans, "The U.S.–China Trade-Tech Stand-Off, Clingendael Report," August 12, 2019, <https://www.clingendael.org/publication/us-china-trade-tech-stand>.

[2] Michael D. Beck and Scott A. Jones, "The Once and Future Multilateral Export Control Regimes: Innovate or Die," *Strategic Trade Review*, Vol. 5, Issue 8 (Winter/Spring 2019), pp. 55–76.

closest ally.

The existing multilateral regime hence needs to adjust if it is to keep up with the latest rapid developments in a changing geopolitical context and amid a great power rivalry. This article contributes to the discussion on the future of the MECR – specifically, the WA – by outlining the debates on the shift from physical to digital technologies, the (yet to be defined) norms and standards underpinning the discussions about reforming the WA, and possible other ways forward, complementing inter-governmental discussions in the WA. In doing so, the focus is on the political rather than the technical dimensions of the debate. It is argued that the top-down government-led approach through the MECRs alone no longer suffices and that new export control approaches that focus on principles and voluntary agreements are needed. Trusted communities are highlighted as a valuable instrument to engage relevant stakeholders, complementing governments' efforts in formal export control regimes.

This article begins with a discussion of the concept of emerging technologies, aiming to clarify the difference between today's emerging technologies and the dual-use technologies subject to the WA. The authors propose a conceptual shift from dual-use to omni-use and omnipresent technologies, in recognition of the fact that the now-emerging technologies are omnipresent in society, combined with the fact that a broad consensus on the potential (and "good") military and civilian uses of items is lacking. Next follows an analysis of proposed regulation in the United States, which is also pushing trade partners – including in the European Union (EU) – into action. This is illustrated by way of a case study of the Netherlands. Lastly, the article considers paths ahead, building on transnational global governance and epistemic communities' literature to discuss ways forward and propose the introduction of "trusted communities" as a viable complement to the WA, thereby upholding its relevance for the future.

Emerging Technologies: Omnipresent and Omni-Use

The existing export control regimes cover two categories: conventional military goods; and dual-use items, consisting of goods, software, and technology that can be used for both civilian and military applications. Technology, in export control regulations, is defined as "specific information which is required for the development, production, or use of a controlled item."[3] The export control regimes find their history in the establishment of the Coordinating Committee for Multilateral Export Controls (CoCom), which coordinated restrictions on the export of military items and technologies to the Soviet Communist bloc.

Today, four separate export control regimes constitute the MECRs: the Australia Group (AG), the Missile Technology Control Regime (MTCR), the Nuclear Suppliers Group (NSG), and the

[3] "List of Dual-Use Goods and Technologies and Munitions List," WA-LIST (16) 1 Corr. 1, Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, February 17, 2017; "Equipment, Software and Technology Annex," Missile Technology Control Regime, October 19, 2017.

successor of CoCom, the WA.[4] All four regimes are non-binding political arrangements, which support informal consultative mechanisms among their members. By promoting transparency and dialogue, these multilateral "soft-law" guidelines, which are translated into legally binding obligations or "hard law" at the national level, create responsibility for transfers and contribute to regional and international security and stability.[5]

To add clarity to the essence of the challenges facing the WA, two additional categories of technology that governments may wish to control are outlined in this article: critical infrastructure; and (the now-emerging) omni-use technologies. The critical infrastructure of a country consists of gas, water, and electrical infrastructure and is deemed critical for a country's sovereignty and daily functioning. Even though many companies that deliver critical infrastructure are privatized, governments have to protect these against hostile takeovers at all costs as these companies are vital for the national security as well as economic safety of a country. The critical infrastructure category of a country was, until now, defined quite limitedly, with only gas, water, and electricity at its core. However, as illustrated also by the global debate surrounding the adoption of Chinese 5G technology in critical government networks, the increasing importance of information and communication technologies (ICT) to secure the day-to-day activities of critical infrastructure is increasingly complicated and controversial.[6]

Emerging technologies are new, potentially disruptive technologies with elements that will continue to develop in the future to reach their full potential.[7] Moreover, the technical standards are not yet internationally agreed upon and the risks for national security and economic safety of any country are not yet identified.[8] Emerging technologies are not a new concept, but the technologies now developed pose a challenge to the WA in ways that previous emerging technologies did not. This article proposes the term "omni-use" for the emerging technologies now up for debate, in recognition of the fact that three key characteristics distinguish them from the emerging technologies for which the regimes' export control measures were originally designed.

The first characteristic concerns the nature of the technologies, which has shifted from physical items to intangible "digital" technologies and technical know-how.[9] This shift is embedded in the fourth industrial revolution, characterized by "a fusion of technologies that is blurring the

[4] "A Resource on Strategic Trade Management and Export Controls: Overview of U.S. Export Control System," Government of the United States, Washington D.C., <https://2009-2017.state.gov/strategictrade/overview/index.htm>.

[5] Ibid.

[6] This article will not discuss this in further detail, focusing instead on the challenge of (now emerging) omni-use technologies.

[7] Kolja Brockmann, "Drafting, Implementing, and Complying with Export Controls: The Challenge Presented by Emerging Technologies," *Strategic Trade Review*, Vol. 4, Issue 6 (Spring/Summer 2018), p. 6.

[8] Ibid., p. 6. and Daniele Rotolo, Diana Hicks, and Ben R. Martin, "What is an Emerging Technology?," *Research Policy,* Vol. 44, Issue 10 (December 2015), p. 1831.

[9] Kolja Brockmann, "Drafting, Implementing, and Complying with Export Controls: The Challenge Presented by Emerging Technologies," *Strategic Trade Review*, Vol. 4, Issue 6 (Spring/Summer 2018), pp. 5–27.

lines between physical, digital, and biological spheres."[10] Technologies can now be transferred between countries without physically crossing national borders, thereby bypassing customs authorities that are normally tasked with dual-use export control. Second, the private sector, rather than the public sector, is in the lead in designing and developing omni-use technologies. This is a significant change from the post-1945 decades, when the state was vital in the process of technological innovation in defense, in what came to be called the "military-industrial complex." Back then, the state provided the critical financial resources required to take embryonic technologies and develop them at a speed unlikely to be matched by the civilian market. Now, the state mainly harvests and refines for defense purposes the technological developments spurred in the private sector, and increasingly more often in small and medium-sized enterprises (SMEs).[11] Moreover, these companies trade across borders and are at times unaware of the potential use of their technologies by specific end-users. This relates to the third key characteristic that distinguishes emerging technologies today from earlier times, namely the fact that the intangible technologies can be implemented in a broad range of civil and military applications, making them increasingly omnipresent in society. Subjecting specific items to export control thereby becomes increasingly difficult, as one particular item may consist of many elements and a variety of technologies.

Further adding to the challenge is the fact that omni-use technologies may not automatically fall into the realm of the WA, which focuses on dual-use items. Members do not agree on the possible implications for national security of emerging technologies because of diverging ethical norms and standards. Network intrusion software and surveillance technologies, for example, are considered by some governments as beneficial for public safety, while others emphasize privacy concerns. Hence, the diversity in potential application and integration at all levels in society renders newly emerging technologies omnipresent in society and thereby extremely difficult to control via the dual-use control lists of the WA. In addition to the omni-use technologies being used for new applications, these can also allow old items to be performed in a new way. This could lead to situations in which current policies do not offer sufficient guidance and discussions over which ethical understandings and societal conventions of existing regulations may be challenged.[12]

The WA has guidelines to implement export control regulations for intangible transfers of technology controls, but the regime's best practices document on implementing the intangible transfer of technology controls does not meet today's challenges.[13] This is illustrated by the debates on additive manufacturing, which encompasses all 3D printing and associated

[10] Klaus Schwab, "The Fourth Industrial Revolution: What it Means and How to Respond," *Foreign Affairs*, December 2015.

[11] James Manyika, William H. McRaven, and Adam Segal, *Innovation and National Security: Keeping Our Edge*, (Washington DC: Council on Foreign Relations, September 18, 2019), pp. 8–9 and 69–74.

[12] Jean-Lou Chameau, William F. Ballhaus, and Herbert Lin, "ELS Framework for Emerging Technologies and National Security," in Jean-Lou Chameau, William F. Ballhaus and Herbert Lin, eds., *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues* (Washington, DC: National Academies Press, 2014), p. 116.

[13] Wassenaar Arrangement, "Best Practices for Implementing Intangible Transfer of Technology Controls," 2006, <https://www.wassenaar.org/app/uploads/2019/consolidated/ITT_Best_Practices_for_public_statement_2006.pdf>.

technologies such as scanning technologies. Additive manufacturing technology in itself does not pose a national security threat, but its capability to produce 3D printed objects based on a digitally transferable blueprint does, as this may include a wide range of items that are normally subject to strict customs control.[14] With the increased accessibility of 3D printers, and considering the technology's potential to reduce costs and the environmental footprint of exporting products, additive manufacturing will most likely become a central part in society and supply chains.[15]

Additive manufacturing is one of the fourteen categories of emerging technologies that are tentatively identified in ECRA for control. This shows that the categories – also including artificial intelligence (AI) and robotics – are extremely broad; in the case of additive manufacturing, encompassing every blueprint for 3D printing, even if actual items that need to be subjected to control are limited. The categories are thereby too focused on the manufacturing process rather than on the characteristics and end-use of the final product.

At Stake: Competitiveness, Norms, and Standards

The absence of technical norms and standards – and the growing norm gap between countries – underpinning the debates on economic competitiveness exacerbates the difficulties even more. The WA focuses on items and technologies that could have a civilian and military purpose, but the scope is limited as it does not cover control of software that is generally available to the public. This poses a challenge both for the items that already exist but are used for new applications because of recent software possibilities (e.g. a self-driving car), or new technologies where the possible security risks are not yet known. Besides, omni-use technologies are primarily intangible technologies (know-how, technical data, or software), which increases convergences between physical items and software flows and complicates regulations to control them.

Underpinning the rapid technological developments, definitional and normative debates concerning their omni-use and omnipresence complicate the decision-making process in the WA. Establishing whether technology is an omni-use technology, including its possible military purpose, is a challenge with the current 42 members of the WA. Every actor's opinion is informed by a combination of economic, ethical, legal, political, and strategic considerations – which are increasingly diverging globally. Therefore, the discussions about adding technologies to the list is not merely a discussion about whether or not an item has a military application, but also about which country can push its ideas and norms on the application of it. Even when an agreement is reached, a discussion about how controls should apply and what constitutes "good" and "proportional" regulation is on the table and will be politicized in the light of the discussion on standards. Innovative solutions are required to regulate the transfers of software and technical data underpinning the emerging technology items, considering the ease with which it can be developed and transmitted worldwide.

[14] Ibid., and Grant Christopher, "3D Printing: A Challenge to Nuclear Export Controls," *Strategic Trade Review,* Vol. 1, Issue 1 (Autumn 2015), p. 18.

[15] Mark Brannan, "Export Controls and 3D Print: Pizzas, Body Parts and Weapons," AEB, January 8, 2016, <https://www.aeb.com/uk-en/magazine/export-controls-and-3d-print.php>.

The U.S. Push for Action: Ally or Competitor of the EU?

Amid great power rivalry and the shift from a unipolar to a multipolar world, the U.S. pushed for action to counter Chinese ambitions in omni-use technology sectors. In line with the U.S.'s protectionist course of recent years, the U.S. government announced the Export Control Regulation Act (ECRA) in its National Defense Authorization Act for Fiscal Year 2019.[16] This is a U.S.-only "hard law" measure that includes fourteen categories of emerging technologies that could be subject to export control in the future.[17] These categories largely mirror the categories of Made in China 2025 (MIC2025) in which the Chinese government pronounced the aim to become independent from the West by 2025, and include primarily high-tech technologies such as semiconductors and artificial intelligence.[18] As the U.S. Congress did not define what constitutes emerging technologies, except for publishing the list of fourteen technology categories that may be emerging technologies and subject to ECRA in the future, the U.S. Commerce Department's Bureau of Industry and Security issued a request for comment.[19] Following a comment period in which more than 230 companies, business associations, academic institutions, and governments submitted feedback, the Commerce Department's Bureau of Industry and Security (BIS) is working towards ECRA's entry into force in 2020.

The contest for leadership in the development of emerging technologies and the writing of norms and standards for their use is a key explanatory factor for the U.S. government's push for new legislation. There is a vast grey area, however, where Washington's actions may be informed by national security concerns and ethical considerations – such as balancing the rights of the individual with the collective, or the right to privacy – or by a desire to curb China's rise as a technological power. Network intrusion software and surveillance technologies, for example, have become new areas of concern. The U.S. regards China as a revisionist power that actively seeks to challenge the power, influence, and interests of the U.S. by eroding its prosperity and security.[20] This is mainly translated into concerns over Chinese forced technology transfer and intellectual property (IP) theft, which are exacerbated by China's far-reaching technology drive, as outlined in MIC2025. With this program, the Chinese government acts on its ambition

[14] "H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019," 115th Congress of the United States of America, Washington D.C., August 13, 2018.

[17] A second key part of the National Defense Authorization Act (NDAA) is the Foreign Investment Risk Review Modernization Act (FIRRMA). Although ECRA and FIRRMA – i.e. export control and investment review – are closely intertwined, the focus in this article is on export controls governed under ECRA: H.R. 5515, National Defense Authorization Act for Fiscal Year 2019. See Ibid.

[18] The full list comprises the following categories: biotechnology; artificial intelligence (AI) and machine learning technology; position, navigation and timing (PNT) technology; microprocessor technology; advanced computing technology; data analytics technology; quantum information and sensing technology; logistics technology; additive manufacturing; robotics; brain-computer interfaces; hypersonics; advanced materials; advanced surveillance technologies.

[19] Stephen Ezell and Caleb Foote, "How Stringent Export Controls on Emerging Technologies Would Harm the U.S. Economy," Innovation Technology & Information Foundation, May 2019, <https://itif.org/publications/2019/05/20/how-stringent-export-controls-emerging-technologies-would-harm-us-economy>.

[20] "United States' 2017 National Security Strategy (NSS)," Government of the United States, Washington D.C., December 2017.

to be a global manufacturing, cyber, and science and technology innovation superpower. This unprecedented industrial policy triggered considerable criticism and concern in Western countries, prompting the Chinese government to stop referencing the plan, albeit not giving up on its economic and strategic goals.[21]

Although ECRA primarily constitutes a hard-law protectionist move by the U.S. government, the regulations that will follow from this procedure will have far-reaching implications for daily operations of global companies, as the regulations will also be applicable to every technology consisting of more than 25 percent U.S. material, because of the extraterritorial jurisdiction of U.S. law. This extraterritorial jurisdiction, despite being controversial in international law, allows U.S. companies and the government to block re-exports of products consisting of more than 25 percent U.S. material to countries on the U.S. Entity List – the export blacklist of the U.S. – and is enshrined in the U.S. export administration regulations (EAR).[22,23] When the U.S. withdrew from the Joint Comprehensive Plan of Action (JCPOA), better known as the "Iran Nuclear Deal," the EU immediately took action against this extraterritorial jurisdiction. The U.S. would re-impose sanctions on Iran, thereby blocking any export from EU capitals to Iran through its extraterritorial jurisdiction. The European Commission included an annex on the EU Blocking Statute to mitigate the effects of the re-imposed extraterritorial U.S. sanctions to nullify the effect in the EU of any foreign court ruling based on the foreign laws listed in its annex and to allow EU operators to recover in court any damages caused by the extraterritorial application of the specified foreign laws. This may also apply to the controls pushed for by the U.S. in the field of export controls on emerging technologies. Reforming the WA becomes a challenge because of this, exacerbated by the increased gap in norms between the members.

Therefore, the forthcoming ECRA regulations will not solely be a business decision, but also a political dilemma for the EU: either to follow the U.S. or to push for the protection of EU-based companies against the extraterritorial jurisdiction of the U.S. Moreover, because the regulations will significantly affect respective EU Member States, the ministries responsible for executing export control regulations oftentimes lack the capacity to deal with a sudden increase of export license requests.

Case Study: The Netherlands

The case of the Netherlands is useful to gain a better understanding of the challenges involved with updating regulations that prohibit the unlicensed export of certain new, omni-use technologies to specific end-users. The Netherlands has a strong position in specific niche markets for the high-technology sector – specifically semi-conductors, photonics, and quantum

[21] Max J. Zenglein and Anna Holzmann, "Evolving Made in China 2025: China's Industrial Policy in the Quest for Global Tech Leadership," Mercator Institute for China Studies, Papers on China, No. 8 (July 2019).

[22] The EU has adopted the EU blocking statute to challenge the extraterritorial jurisdiction of the U.S. and protect EU-based companies. However, EU-based companies often adhere to the U.S. jurisdiction as the losses suffered are greater than the EU fines.

[23] "Export Administration Regulations," Bureau of Industry and Security, Washington DC, November 13, 2019.

technology – with value-chains closely intertwined with the U.S. and Chinese markets. The concerns of numerous Dutch stakeholders about the near and long-term implications of the use and control of emerging technologies – especially by the Chinese government – are similar to those of the U.S. government, and the Netherlands Ministry of Economy and Climate has identified key technologies, published in a list corresponding with the categories identified by the U.S. government.[24]

Considering the breadth and depth of transatlantic and U.S.–Netherlands political, economic, and military ties, the Netherlands might be expected to follow the U.S. in its regulations. This seems, however, not to be the case; diverging understandings of economic and national security of the Netherlands and the U.S. hinder fruitful cooperation. The explicitly China-focused approach of the U.S., in comparison to the economy-focused Dutch vision, complicates cooperation even more.

Historically, whereas economic security is considered part of national security in the U.S., economic security and national security have been separated institutionally and practically in the Netherlands, as in most other EU Member States. More recently, however, the overlap between economic security and national security is increasingly discernible in both the U.S. and the Netherlands. In the Netherlands, economic security refers to an efficient economy that is protected from threats that have the potential to disturb its functioning. To the Dutch government, achieving economic security is a core strategic interest, as its businesses are extensively integrated into global value-chains. Upholding national security interests solely relates to protecting vital Dutch interests and critical infrastructure against a divergent range of threats, such as terrorist threats or floods, that could have a disruptive effect on Dutch society.

In the U.S., relations between the government and businesses are stronger, as the private sector has successfully linked IP protection to innovation, innovation to global competitiveness, and global competitiveness to national security. This has resulted in a historically strong convergence between economic and national security. Concerns about weakening U.S. supremacy in high-technology and IP-sensitive industries are therefore also a national security issue for the respective responsible departments in the U.S. Department of Defense, the U.S. intelligence community, and U.S. industries.

The ethical considerations of today's debates have caused a shift in both the Dutch and the U.S. approach. The dividing line that has been apparent in the Netherlands between economic and national security is slowly vanishing, as reflected in the gradual convergence of the two concepts in the National Security Strategies of 2007 and 2013.[25] In the U.S., the high-tech industry is now increasingly pushing for the opposite: a stricter distinction between economic and national security issues. While agreeing with the need to implement export control

[24] "Quantitative Analysis of Dutch Research and Innovation in Key Technologies: A Report for the Ministry of Economic Affairs and Climate Change," Directorate-General for Enterprise and Innovation, Innovation and Knowledge Department, Government of the Netherlands, *Elsevier,* June 1, 2018, <https://www.government.nl/documents/reports/2018/06/01/quantitative-analysis-of-dutch-research-and-innovation-in-key-technologies>.

[25] "International Security Strategy: A Secure Netherlands in a Secure World," Government of the Netherlands, The Hague, June 21, 2013.

regulations to maintain technological superiority, industry voiced severe concerns about the proposed broadening of export control regulations in the first call for comments on the announced categories of emerging technologies in ECRA.[26]

Although small in size, the Netherlands is a global leader in various high-tech sectors, making it an important bilateral partner for the U.S. In recognition of this, the U.S. and the Netherlands have engaged in bilateral consultations and regulatory coordination, especially in response to the U.S.'s export control reform proposals.

In the field of export control, however, bilateral arrangements are no substitute for an effective regime of a third (that is, non-EU) country with one EU Member State, such as the Netherlands. Even though a bilateral agreement will potentially promote U.S.–Dutch business cooperation, an effective multilateral export control regime must involve all member states that encompass the Schengen Area as a whole. After all, foreign companies exporting from one specific EU Member State can engage in so-called "license shopping" – that is, using the free flow of goods, persons, and services within Schengen to export technologies that are subject to export regulations to another Schengen country that has not yet adopted such export control regulations. In this way, Member States can be used as a third intermediary country, thereby bypassing the strict export control regulations of specific Schengen countries.

Revising the EU's export control regime is a significant challenge, however, as Member States have divergent views and relationships with the U.S. and China, and not every Member State will be involved directly with stricter export control regulations, since only a few have a high-technology sector. Discussions towards this end – that is, a recast of EU regulations dating back to 2009 – had been ongoing before the publication of ECRA, but have yet to be concluded. Clearly, however, a coherent EU policy with stricter punishments would be a stronger stance against the extraterritorial jurisdiction of the U.S. Moreover, the EU could be a respective powerful force for regime change and increase the win-set of the Netherlands in negotiations with the U.S.

Voluntary Measures Complementing the WA: Trusted Communities

The international debate to define emerging technologies – here referred to as omni-use – is slowly moving forward, and establishing norms and standards is a growing challenge in the context of great power rivalry. At the same time, technological developments and unilateral action by some states are moving faster than in the past. Clearly, these two trends complicate discussions within the WA, as not all members agree to – or even on the need for – multilateral guidelines on specific issues, on which they have yet to develop a clear position of their own. At the same time, the semi-annual meetings and sometimes highly politicized discussions within the WA further complicate any fast decision-making process at the multilateral level.

A more innovative approach complementing the WA process is therefore needed to push

[26] "Review of Controls for Certain Emerging Technologies," Bureau of Industry and Security, Department of Commerce, Washington, DC, October 11, 2018.

the debate on emerging technologies forward. Turning to voluntary instruments seems promising, refocusing from a rules-based to a principles-based approach. As a first step, so-called "trusted communities" can create valuable partnerships between a range of stakeholders based on shared principles. These communities may include government officials, businesses, lawyers, and researchers, domestically or across countries. Through regular meetings between a fixed membership group, trusted communities contribute to information-sharing and best practice exchange in an informal, closed environment. Ultimately, trusted communities serve as a confidence-building and knowledge-sharing instrument that benefits all stakeholders, enhancing understanding and cooperation between government and businesses, and discussions on technological developments and future regulation.

Transnational Global Governance in Flux

Trusted communities can be positioned in the broader transnational global governance literature, which proposes that non-state actors are influential players in the policy-making process.[27] Epistemic communities are the most well-known subset of this, defined as a grouping of scientists linked by their professional ties and ideas in their specific area of expertise.[28] Bound together by their knowledge, the added value of epistemic communities – even with a small membership – lies in their strong internal cohesion. Particularly at times of uncertainty, governments and politicians tend to ask for new ideas and innovative proposals. The extent to which such communities interact with government officials fluctuates, and their influence on the policy-making process hence also varies – between groups and over time. While epistemic communities commonly arise without any government or official influence, governments play an increasingly catalytic role in gathering experts. Otherwise similar to traditionally evolved epistemic communities, these groups are positioned within government structures, as independent agencies.[29] Epistemic communities evolving without government interference have been particularly successful in the environmental field where debates tend to be highly politicized and technical. For its part, the European Commission has been instrumental in the creation of various "high-level groups of wise persons" to provide it with advice – for example, on the European financial architecture for development.[30]

Next to epistemic communities, which are mostly based on shared scientific knowledge, the transnational global governance literature introduces transnational advocacy networks and communities of practice.[31] Transnational advocacy networks consist of non-governmental organizations such as human rights groups or nonproliferation movements that share values and ideals. Communities of practice are made up of various stakeholders – either groups or

[27] Mai'a K and Davis Cross, "Re-thinking Epistemic Communities Twenty Years Later," *Review of International Studies*, Vol. 38, No. 1 (January 2013), pp. 137–160.

[28] Peter M. Haas, "Introduction: Epistemic Communities and International Policy Coordination," *International Organizations*, Vol. 46, Issue 1 (Winter, 1992), pp. 1-35.

[29] Ibid.

[30] "European Financial Architecture for Development: Council Sets Up a High-Level Group of Wise Persons," European Council, Brussels, April 9, 2019.

[31] Margret E. Keck and Kathryn Sikkink, "Transnational Advocacy Networks in International and Regional Politics," *International Social Science Journal*, Vol. 68, No. 227-228 (1999), pp. 89–101.

individuals – that are tied together by a specific topic and their desire to share information, best practices, and experiences to develop on a professional level.[32] These communities differ from epistemic communities, which are bound together by their knowledge, while transnational advocacy networks are united in their ideals, and communities of practice by their wish to share information.

More recently, and particularly relevant to the field of export control, a rise of privatization of transnational governance is being observed. Key in this trend is a growing need – and willingness – for engagement between government and private-sector representatives. State actors have less access to necessary technological know-how, complicating efforts to regulate increasingly global challenges, while businesses are more inclined to abide by self-imposed rules of standards, voluntarily setting a precedent for other companies. Motorola Corporation, for example, has effectively contributed to setting telecommunications standards through its chairmanship of the International Telecommunication Union.[33] Critics argue that this might trigger a shift to states being merely rule-takers rather than rule-makers, and undermine equity among states.[34] Others argue that only private sector firms will have the capacity for research, technology, and development to address and tackle global challenges in the 21st century.[35]

Beyond Epistemic Communities: Trusted Communities

The narrow definition of epistemic communities has been subject to substantial criticism in the academic field. In particular, the inclusion of scientists solely in one specific field seems to hamper constructive multidisciplinary solutions, recognizing new trends and successful translation of knowledge into power.[36] Therefore, the execution of epistemic communities could be extended beyond the current narrowly defined definition. The inclusion of a multidisciplinary team, consisting of businesses, lawyers, government officials, and researchers could lead to discussions among a diverse range of experts and result in widely shared consensus.[37] The inclusion of government officials would prevent governments from becoming merely rule-takers, and statements deriving from the trusted community can be perceived as more

[32] Emanuel Adler and Vincent Pouliot, “International Practices,” *International Theory*, Vol. 3, No. 1 (2011), p. 136.

[33] John Braithwaite and Peter Drahos, *Global Business Regulation* (Cambridge: Cambridge University Press, 2000), p. 4.

[34] Peter Utting, “Codes in Context: TNC Regulations in an Era of Dialogues and Partnerships,” Briefing 26, The Corner House, February 2002.

[35] S. Tesner, *The United Nations and Business: A Partnership Recovered* (New York, NY: St Martin’s Press, 2000), p. 150, quoted in P. Utting, “UN–Business Partnerships: Whose Agenda Counts?,” paper presented at “Partnerships for Development or Privatization of the Multilateral System?,” seminar organized by the North–South Coalition, Oslo, Norway, December 8, 2000 (abridged version published in *UNRISD News* 23, Autumn/Winter 2000, pp. 1–4).

[36] Mai’a K. and Davis Cross, “Re-thinking Epistemic Communities Twenty Years Later,” *Review of International Studies*, Vol. 38, Issue 01 (January 2013), pp. 137-160.

[37] William J. Drake and Kalypso Nicolaïdis, “Ideas, Interests, and Institutionalization: ‘Trade in Services’ and the Uruguay Round,” cited in: Mai’a K. and Davis Cross, “Re-thinking Epistemic Communities Twenty Years Later,” *Review of International Studies*, Vol. 38, No. 1 (January 2013), pp. 137–160.

legitimate as they would be based on consensus among experts across the field.[38] Although more uncommon in Europe, consultative bodies that bring together a diversity of stakeholders, including business, are not a new phenomenon. In Japan, for example, deliberation councils (s*hingikai*) have long served as lines for communication between groups – mainly government officials, business representatives, and experts – that operate in distinct but, in reality, linked environments.

Trusted communities offer government officials direct access to academic and private-sector expertise on the global value-chains, the latest technological developments, and the economic context wherein policymakers have to make decisions that also impact domestic businesses. By consulting with the relevant industries, more accurate policies can be implemented, while simultaneously possible gaps in the current policies can be monitored. The influence businesses gain in the decision-making process may be of great value as not only they but also the government are in uncharted territory with regards to emerging technologies in the changing geopolitical context. The consultative sessions with all parties may also be an incentive for companies to increase their due diligence concerning international cooperation. By discussing which regulations are necessary or not to safeguard global trade, self-regulation and responsibility of companies may increase.

Consultative trusted communities can present an opportunity also for SMEs that are often unaware of possible global tensions and the repercussions of export to specific parties – either for the end-use or end-user. A regular dialogue between representatives of SMEs, start-ups, multinational companies, government officials, and academia active in the field of emerging technologies can contribute to information- and best practices sharing among them. Discussing regulations focused on the SMEs could balance a number of concerns that these parties may have concerning export control regulations, the end-use of their technology and broader geopolitical discussions. At the same time, trusted communities are a tool of "preventive diplomacy" whereby governments can sensitize enterprises operating in the field to a variety of evolving export control concerns.

The U.S. government has been a frontrunner on such trusted communities, having initiated so-called "communities of caution" that aim to share information on tech-transfer threats.[39] The inclusion of both state and non-state actors in one consultative trusted community has so far, however, been controversial in Europe. A close relationship between the government and industry is historically related to increased industry influence in politics, a practice fueling resistance in most European states. While the strict division of business and politics was long proven successful, with the new geopolitical tensions and the rise of emerging technologies, government and industry are experiencing – albeit to varying degrees – similar challenges globally. The establishment of trusted communities as a consultative organ consisting of government officials, business representatives, and academia, could thus be an answer to the increased overlap between the domains.

[38] Eleni Tsingou, "Transnational Policy Communities and Financial Governance: The Role of Private Actors in Derivatives Regulation," Center for the Study of Globalization and Regionalization Working Paper 111, 2003, p. 8.

[39] "Coalitions of Caution: Building a Global Coalition Against Chinese Technology-Transfer Threats," U.S. Department of State, Washington DC, September 13, 2018.

Regular gatherings help to build trust among members, which is required for a frank discussion on the necessities to define or redefine an export control regime, including the ethical considerations and normative debates that fit our increasingly globalized world. Non-state actors, including from industry and academia, have to engage voluntarily in global governance. Previously, voluntarily abiding by the norms set by a transnational network was considered a limitation, but as trusted communities also include state actors, the benefits of direct influence in the policy-making process and standard-setting could outweigh this. One condition for this is the scope of the trusted community, as it has to be both sector-specific, but also needs to include like-minded states, companies, and academia. When multiple domestic trusted communities start to discuss their ideas, competition in thoughts can commence, which eventually enhances the international debate on emerging technologies and export control.

Conclusions

In today's rapidly changing and increasingly polarized world, technological developments improve lives globally, but also present new national security risks. Harnessing the current wave of technological development and mitigating its potential threats are vital for gaining an economic and military advantage over potential global rivals in the future. For a long time, the U.S. has led the race for technological supremacy, but the now emerging omni-use technologies pose new challenges next to the vast opportunities they offer. To maintain its technological supremacy and standard-setting ability in the 21st century, the U.S. is pushing – once again – for new export control mechanisms to coordinate restrictions on the export of certain items to specific end-users, uses, and destinations of concerns.

Washington's protectionist and mercantilist considerations are perceived by many other governments – including that of the Netherlands – as problematic, even if its ethical concerns are more widely shared between developed countries. Add to this the deeper economic interdependence stemming from the global technological value-chains and it is clear that the challenge today is vastly greater than in the years following the Second World War when the first MECR was created.

The WA would be the natural regime to turn to, but the intangible nature of the technologies, the fact that today the private sector – rather than the public sector – plays the lead role in the development of emerging technologies, and the lack of consensus in identifying which actors present a proliferation threat and which items have omni-use potential in today's society complicate this avenue. This article argues that the discussion needs to move beyond existing debates on the inclusion of emerging technologies in dual-use lists. Shifting the debate to the omni-use and omnipresence of emerging technologies is a valuable step towards acknowledging the particularities of today's emerging technologies.

In addition, trusted communities that bring together government officials, business representatives, and experts with a stake in specific high-tech sectors appear to be an innovative way forward. These groups may be a means to support the multilateral export control regime and to push for norms and standards, while simultaneously not excluding upfront other vital players within the global value-chain.

In the future, trusted communities could either transform into a consultative body within an existing framework – such as the WA – or on the national level merge into government structures. Either way, trusted communities provide room to discuss ethical, legal, and societal dimensions of emerging omni-use technologies. They help to ensure that governments keep up with rapid technological developments – thereby contributing to more appropriate policy responses and regulation – and are at the same time a tool of "preventive diplomacy" whereby governments can sensitize relevant SMEs to a variety of concerns in export control with regard to end-users, uses, or destinations of concern. As a voluntary confidence-building measure involving a range of stakeholders rather than only government officials, trusted communities are thereby an important addition to hard regulation and soft law measures that have so far characterized the MECRs.