BRILL
NIJHOFF

SECURITY AND HUMAN RIGHTS (2021) 1-24

SECURITY AND
HUMAN RIGHTS
brill.com/shrs

Trade and Emerging Technologies

A Comparative Analysis of the United States and the European Union Dual-Use Export Control Regulations

Cindy Whang
Assistant Professor, Department of Financial and Economic Law, Fu Jen Catholic University, New Taipei City, Taiwan
094573@mail.fju.edu.tw

Abstract

Export controls are domestic trade restrictions placed on technologies that have been determined to be important to the national security concerns of a country. In recent years, the policy purpose for maintaining export control regulations have shifted, and how these new export control regulations would interact with new emerging technologies is something that should be analyzed and considered. The passage of the United States (US) Export Control Reform Act (ECRA) of 2018 and the proposed regulatory changes for the European Union's (EU) Council Regulation (EC) No. 428/2009 have shifted the focus of dual-use export controls so that the national security goals of these controls have broadened to include economic security and human rights concerns. This paper argues that the infusion of geoeconomics into US national security considerations and the proposed expansion to include human rights considerations into EU export control regulations are made mutually exclusive of each other and were not made to expand the reach of export controls in a unifying way. Rather, the purpose and structural change to export control regulations serves to create more regulatory barriers on the trade of emerging technology industries that would not only impact the US and the EU, but also their international trading partners.

Keywords

dual-use export control – emerging technologies – national security – human rights – regulatory barriers

1 Introduction*

The economist Jeffrey D. Sachs has stated that "[t]echnological advances—especially in transport and communications—… have intensified our global-scale interdependency and awareness. As a result, politics too have gone from being very local to being global, never more so in our own time."[1] The observation made by Sachs highlights the interwoven relationship between technological advancement and global connectiveness that have in turn injected the issue of globalization into politics. However, an unstated element underlying his observation is the role that trade has played in creating such connections. Trade has strengthened global commercial relationships and helped spread technological advances through the interdependent structure of global technology supply chains. The promotion of international trade through the General Agreement on Tariffs and Trade (GATT) and the establishment of the World Trade Organization (WTO) in 1995 has lowered the average tariffs to 9% in 2018[2] and increased the trading value of world merchandise from 5.2 trillion USD in 1995 to 19 trillion USD in 2019.[3] Among the WTO Agreements, the Information Technology Agreement (ITA) has lowered the average tariff for information technology products that account for approximately 97 percent of global trade.[4] It is difficult, if not impossible, to discuss the innovation of technologies without considering the global impact that such technology development could bring to the world at large.

However, as countries have become more economically and technologically integrated with each other with robust international trade, the policy discussions surrounding technological innovations and trade have become a hot button issue for some states. Some of the technologically advanced countries such as the United States (US) are now faced with competition from countries

* The author wants to thank Taiwan's Ministry of Science and Technology for their grant (105-2410-H-030-011-) that funded the research contained in this paper.

1 Jeffrey D. Sachs, *The Ages of Globalization: Geography, Technology, and Institution*, Columbia University Press, 2020, p. 2.

2 See World Trade Organization, *Evolution of Trade under the WTO: Handy Statistics*, available at: https://www.wto.org/english/res_e/statis_e/trade_evolution_e/evolution_trade_wto_e.htm.

3 See World Trade Organization, *Evolution of Trade 1950–2019: Values, Billions USD*, available at: https://www.wto.org/english/res_e/statis_e/trade_evolution_e/world_trade_values.xlsx.

4 Computers, telecommunication equipment, semiconductors, semiconductor manufacturing and testing equipment, and their parts and accessories are all included in the products subject to ITA. World trade Organization, *Information Technology Agreement: An Explanation*, available at: https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm.

such as China that were the original destinations of these countries' outbound manufacturing investments. The advancement of technology is responsible for a part of the current trade tension between the US and China. In May of 2018, the US President Donald Trump accused China of unfair trade practices that included forced technology transfers and acquisition of sensitive technology from the US' enterprises that undermined American innovations and jobs.[5] These claims were made against the backdrop of China's internal industrial policy of "Made in China 2025" that emphasized China's domestic development of ten industries that would place some of these technologies in direct global competition with companies from the US.[6] As the trade tensions between the US and China rose, in August of 2018, Trump signed the Export Controls Reform Act of 2018 (ECRA) that re-established the US export control system, granting the US government legislative authority to control the export of dual-use goods and technology.[7]

The export control regime is a domestic trade mechanism used to control a country's outbound export of military-use and dual-use goods and technology based on national security concerns.[8] Since World War II, export control regimes have been used by nations, especially the US and countries in Europe, as a trade mechanism that would align with national security policies to restrict international proliferation and limit the development of military-use technology of hostile states. As international relationships have changed post-Cold War, the national security concerns that have guided export controls have also undergone policy changes that reflect the changing concerns of the countries.

This paper argues that emerging technologies have influenced export control regimes, and new policy concerns incorporated into export control regulations are influencing the trade of these emerging technologies. The paper first discusses the structure of dual-use export control regimes in the US and

5 The White House, *President Donald J. Trump is Confronting China's Unfair Trade Policies* (29 May 2018), available at: https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-confronting-chinas-unfair-trade-policies/.

6 The Notice on Issuing "Made in China 2025" listed ten industries targeted for development: (1) next generation of information technology; (2) automation and robotics; (3) aerospace equipment; (4) ocean engineering and high-tech ships; (5) advanced railway transportation equipment; (6) automobiles that rely on energy-saving or renewable energy sources; (7) power systems; (8) agriculture-use equipment; (9) advanced materials; and (10) biopharmaceutical and high-performance medical devices. Notice on Issuing "Made in China 2025" (State Council, Guo Fa [2015] No. 28, issued 8 May 2015), available at: http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

7 Export Control Reform Act of 2018, 50 U.S.C. §4801.

8 See Douglas E. McDaniel, *United States Technology Export Control: An Assessment, Praeger Security International* (1993), pp. 3–8.

the European Union (EU) in the context of their lists and allocation of export liability and how these liabilities have been impacted by emerging technologies such as cloud computing services. The paper then highlights how the traditional national security concerns of export controls for the US and the EU are evolving to include other policy considerations not included in the original context of export control. This change is specifically apparent in the recent changes made to the US ECRA and the proposed regulatory changes for EU Council Regulation (EC) No. 428/2009.[9] For the US, the statutory changes made to export control could be seen to reflect the concept of geoeconomics where economic considerations were being added into strategic policies and the infusion of national security concerns were being accounted for in economic policies.[10] For the EU, the proposed changes of Regulation 428/2009 included the consideration of human security that is a security concept meant to prevent the violation of human rights. As the export control regimes between the US and the EU started to incorporate different policy considerations, the global trade of emerging technologies could be facing different standards of government oversight from separate states in the future.

2 Restricting the Trade of Dual-Use Technologies Based on National Security Concerns

The modern domestic export control regimes were established after World War II when the US and Western European nations formed the North Atlantic Treaty Organization (NATO), and the allies sought to use trade measures to help facilitate national security goals.[11] Because domestic export control regimes in the US and Western Europe were created under such a backdrop, the technologies subject to export controls included both military-use and dual-use goods and technologies. For defense articles and technical data that have clear military-use, these items and technologies are subject to strict export controls. For dual-use items that have both military and commercial application, the controls have been aimed at goods and technologies that have more military applications than those that have more widespread commercial applications. This would fulfill the national security concerns installed in the export control

9 Council Regulation 428/2009, 2009 O.J. (L 134) 1 (EC).

10 See Robert D. Blackwill and Jennifer M. Harris, War by Other Means 20–23 (2017). See also Anthea Roberts, Henrique Choer Moraes and Victor Gerguson, *Towards a Geoeconomic World Order* (16 May 2019), available at: https://ssrn.com/abstract=3389163 or http://dx.doi.org/10.2139/ssrn.3389163.

11 See Gregory W. Pedlow, *NATO Strategy Documents 1949–1969* (1999), p. 11.

regimes while not impinging on the economic interest of a country's technology industry.

The cohesiveness of an export control regime is established through the interwoven structure of international agreements and domestic export control regulations. Participating states of international agreements such as the Wassenaar Arrangement establish lists of dual-use items and technology.[12] Most countries adopt the dual-use export control lists passed by international export control agreements, but because international export control agreements are non-treaty instruments, the lists they create do not have a formally binding effect on the agreement's participating states.[13] As a result, countries maintain their autonomy in finalizing the technologies and methods they use to structure their own export control system.

There are two issues that are important to the constructs of a domestic export control regulation: the goods and technologies on export control lists and the determination of export liability for exporters. The establishment of the export control list determines whether goods or technologies are subject to a country's export control oversight, and the mechanism that exporters could use to determine whether or not they are in compliance with domestic export controls is decided by the allocation of export liabilities through export activities. In the following sections, the discussion on how emerging technologies would interact with and be influenced by domestic export control regulations will be presented through the perspective of these the dual-use export control lists and allocation of exporters liability.

3 National Security Concerns that Structured the Control of Technology in Trade

A main goal of export control was to prevent the proliferation of military-use weapons on the international market while simultaneously protecting a

12 The four international export control list setting agreements are the Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group, and Missile Technology Control Regime. See Wassenaar Arrangement, https://www.wassenaar.org/. See also Nuclear Suppliers Group, About the NSG, http://www.nuclearsuppliersgroup.org/en. See also, Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html. See also Missile Technology Control Regime, http://mtcr.info.

13 See Wassenaar Arrangement, About Us, https://www.wassenaar.org/about-us/. See also, Nuclear Suppliers Group, About the NSG, http://www.nuclearsuppliersgroup.org/en/about-nsg/history1. See also, Australia Group, The Origins of the Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/origins.html. See also, Missile Technology Control Regime, Frequently Asked Questions, http://mtcr.info/frequently-asked-questions-faqs/.

country's national security interests.[14] When a new technology emerges, national security concerns play into how the trade of these new technologies interact with the structure of the domestic export control regime's lists and the allocation of export control liability. If the new emerging technology has clear military-use applications, it would be included in the export control list that restrict the outbound trade and transmission of technology for defense purposes. For other types of emerging technologies used primarily for commercial-use, how they fit in an export control regime is dependent on how they would be used by their end-use or end-users. If the emerging technology might facilitate end-use or end-users to obtain technologies that would endanger the security of the exporting country, the emerging technology might be subject to export control.

Besides categorizing emerging technologies as a subject of control, the development of new technologies, especially those in the information technology, might create new conduits to facilitate the transmission of electronic data. The use of these new technology might create a pathway for end-use or end-users to obtain technologies that would endanger the security of the exporting country, and a separate issue on whether or not export liability should be allocated to the firms hosting these new technologies becomes a point of discussion.

The following section describes the main ways by which the export control regimes in the US and the EU were structured, and it also details how emerging technologies and other new technologies like the cloud computing services challenged the liability structure of the dual-use export control regime in these jurisdictions.

3.1 *U.S. Dual-Use Export Control Regulations prior to the ECRA*

Before the US passed the ECRA in 2018, the US dual-use export control regime was regulated through the Export Administrative Act of 1979 (EAA). When the EAA expired in 2001,[15] the dual-use export control continued to be operated under the authority given to the US president through the International Emergency Economic Powers Act (IEEPA).[16] The EAA authorized the US

14 See United States Department of State, *A Resource on Strategic Trade Management on Export Control, Overview of U.S. Export Control System*, available at: https://2009–2017.state.gov/strategictrade/overview/index.htm. See also European Commission, *Dual-use Trade Controls*, http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.

15 To provide for increased penalties for violations of the Export Administration Act of 1979, and for other purposes, Pub. L. No. 106–508, 114 Stat. p. 2360 (2000).

16 Continuation of Export Control Regulations, as amended, Exec. Order No. 13222, as amended by Exec. Order No. 136372, 3 C.F.R., 2001 Comp., p. 783 (2001).

Department of Commerce to pass the Export Administration Regulations (EAR) that regulated the export control of dual-use goods and technology.[17] The Bureau of Industry and Security (BIS) in the Department of Commerce was in charge of enforcing EAR regulations.

During his presidency, President Barack Obama was in the process of consolidating the US export control regime through the Export Control Reform Initiative that would focus the US export control regime on restricting the trade of defense articles and technologies while relaxing the control on dual-use goods and technology for commercial applications.[18] This would strengthen the export control on military-used goods and technologies that are viewed to have direct impact on the defense and national security of the US. The initiative would also decrease the overlap in administrative oversight of export control issues from the US State Department, Department of Defense, and Department of Commerce.

As the Export Control Reform Initiative sought to consolidate the export control lists and streamline the administrative process, a change in cyberspace technology brought about new issues for the enforcement of the export control regime. Under the EAR, the definition of an export is inclusive of the movement of items and transmission of controlled technology data beyond the US, and it is also inclusive of a release or transfer of technology to a foreign person inside the US.[19] Even when an export controlled item has left the US, it is still subject to the EAR if it is re-exported from a destination country to a third country.[20] When new technological advancements such as cloud computing services started to become prominent around 2010, new issues rose from trying to regulate the transmission of technology data through cloud computing services. Since the EAR regulates both the physical goods and technology data related to export restricted items, the allocation of export liability when the controlled technology was transmitted through cloud computing services needed to be addressed.

Under the EAR, the liability of export control is allocated to the exporter and defined as "[t]he person in the United States who has the authority of a principal party in interest to determine and control the sending of items out of the United States."[21] It is important to note that the EAR makes no distinction

17 Export Administration Regulations, 15 C.F.R. § 730.2, 730.9 (2020).

18 See White House, Executive Order: Export Control Reform, 8 March 2013, available at: https://obamawhitehouse.archives.gov/the-press-office/2013/03/08/executive-order-export-control-reform.

19 Export Administration Regulation, 15 C.F.R. §734.13(a)(1) and (2) (2020).

20 Export Administration Regulation, 15 C.F.R. §734.14 (2020).

21 Export Administration Regulation, 15 C.F.R. Part 772 (2020).

between exporters who are sending physical items and those sending intangible technologies. This made it possible for entities that are transmitting controlled technology data to be classified as exporters and subject to export liability. This also created a question for operators of commercially new technologies such as cloud computing services of the export control liabilities they might face for transmitting controlled technology through their services.

An Advisory Opinion was issued by BIS in 2009 in regard to the question of whether or not a cloud computing service transmitting controlled technology would be viewed as an exporter under the EAR.[22] Since the definition of cloud computing was still subject to debate at the time,[23] BIS's Advisory Opinion was given based on the facts provided by the inquirer that described cloud computing as a type of service that "stor[ed] data or r[an] pre-determined programs using data provided by the customer."[24] Based on that description, BIS stated that if cloud technology services transmitted a technology that was not subject to EAR control and was acting in a computational capacity for users of the service, cloud computing services were not "the principal party in interest" under the EAR's definition of exporter and were not liable under the EAR.[25] BIS stated that it was the users of cloud technology services that are in control of where and how data would be sent that should be considered to be the principal party in interest and subject to export control liability.[26]

However, the expanding types of activities that are being conducted on cloud computing services have allowed for the possibility that the cloud computing services might qualify as exporters under the EAR. In a 2014 Advisory Opinion issued by BIS, if a cloud technology service provider is a cloud storefront that sells software through its cloud services, the transmission of restricted technology from the cloud computing services to a remote location would render the cloud storefront to be a "principal party in interest" and considered as an exporter in the determination of export control liabilities.[27]

22 See Department of Commerce, Bureau of Industry and Security, *Advisory Opinion: Application of EAR to Grid and Cloud Computing Services* (13 January 2009), available at: https://www.bis.doc.gov/index.php/documents/advisory-opinions/527-application-of-ear-to-grid-and-cloud-computing-services/file.

23 It would not be until 2011 when the National Institute of Standards and Technology in the U.S. Department of Commerce would give its definition of cloud computing. See Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing Services*, available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

24 See Department of Commerce, *supra* note 22.

25 Ibid.

26 Ibid.

27 See Department of Commerce, Bureau of Industry and Security, *Advisory Opinion on Cloud-based Storefronts* (*Nov. 13, 2014*), available at: https://www.bis.doc.gov/index.php/forms-documents/advisory-opinions/1098-cloud-based-storefronts/file

In 2016, in order to consolidate the definitions used in various US export control regulations and clarify the liability of dual-use technology that is being transmitted through cloud technology services, BIS issued new rules revising the definitions under the EAR.[28] With the 2016 EAR revision, the definitions for the exceptions to exports[29] and the exception to release[30] were of particular importance as it sought to answer questions related to the movement of dual-use technology on cloud technology services.

The exception to export definition was amended to resolve challenges related to the transmission of technology on cloud technology services over its possible extraterritorial issues.[31] The addendum to EAR §734.18 determined that the sending, taking, or storing technology or software in the following two circumstances will not be considered to be exports.[32] First, if re-exports or transfers of technology and software are using "end-to-end" encryption, those kinds of transmissions would not be considered to be exports.[33] Second, when the transmission of technology and software has been secured using cryptographic modules that are in compliance with US Federal Information Processing Standards Publication 140–2 or its successors, and this type of transmission is supplemented by "software" implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current US National Institute for Standards and Technology publications or other equally or more effective cryptographic means, then the transmission will also not be considered to be an export.[34] The transmission of export controlled technology and software that are not intentionally stored but have temporarily resided on the database in the Russian Federation or US arms embargoed countries listed in the EAR will not be considered as exports either.[35] BIS had made the determination that dual-use technology temporarily stored on data servers in countries on the EAR's embargoed list would not be viewed as an export of these dual-use technologies to those data servers.

28 Revisions to Definitions in the Export Administrative Regulations, 81 Fed. Reg. p. 35586 (Jun. 3, 2016).
29 Ibid., pp. 35593–35594.
30 Ibid., pp. 35592–35593.
31 Ibid., pp. 35593–35594.
32 Ibid.
33 Export Administration Regulation 15 C.F.R. §734.18(5)(ii)(2020).
34 Export Administration Regulation 15 C.F.R. §734.18(5)(iii)(2020).
35 Revisions to Definitions in the Export Administrative Regulations, 81 Fed. Reg. pp. 35593–35594 (Jun. 3, 2016).

Besides revising the exception to export definition, the definition of the exception to release was also amended.[36] Under the EAR, contact with controlled technology is considered a release of technology that would trigger export control liability, and this is usually described the situation where a controlled technology is made available to a foreign person inside the US.[37] Under the revised rules of the EAR, a release of technology must provide knowledge of the export controlled technology or software to the foreign person and not just present the possibility that they would be exposed to the export-controlled technology.[38] This means that for an action to qualify as release under the EAR, it must be apparent that the foreign person with access to export controlled technology and software be able to gain information of the export-controlled technology. A foreign person that simply has the potential or theoretical access to the export-controlled technology or software would not be viewed as having technology released to them under the EAR.[39]

Both of these amendments made to the EAR in 2016 moved to create a feasible export control liability for regulating technology and software on cloud technology services. These amendments sought to balance the cohesiveness of the technical realties of cloud computing services as an emerging technology while trying to maintain the national security concerns of export controls. The EAR amendments reflected how the regulations dealt with commercially emerging technologies and the challenges of this new technology on the structure of export liability under the US' export control framework.

3.2 *EU Dual-Use Export Control Regulations*

The EU's dual-use export control as of July 2020 is found in Regulation 428/2009[40] and provides EU member states with the regulatory principles of exporting dual-use items and technology outside of EU member states and transferring them between EU member states.[41] The Regulation does not establish a centralized export control regime for the EU but rather creates a common list of dual-use items, destinations and guidelines for the member states.[42] Although the EU has an export authorization called the Community

36 Ibid., pp. 35592–35593.
37 Export Administration Regulation 15 C.F.R. §734.15(2020).
38 Ibid.
39 Revisions to Definitions in the Export Administrative Regulations, 81 Fed. Reg. pp. 35592–35593 (Jun. 3, 2016).
40 Council Regulation 428/2009, 2009 O.J. (L 134) 1 (EC).
41 See Quentin Michel, The European Union Export Control Regime: Comment of the Legislation: Article-by-Article (2011), p. 22.
42 Council Regulation 428/2009, 2009 O.J. (L 134) 1 (EC).

General Export Authorization (CGEA) that is issued on the EU level, the CGEA is still subject to national registration and reporting requirements determined by member states of the EU.[43] Member States retain their own authority to structure their own export control regimes and issue their own export licenses.

The amendments made to the EU's dual-use export control regulations from Council Regulation (EC) No 3381/94[44] to Council Regulation (EC) No 1334/2000[45] showcased how advances in new technology created the need to expand the definitions of exports and exporters to establish a more suitable liability framework for export control regulations. Regulation 3381/94 and Regulation 1334/2000 are similar in that both regulations noted that member states retain the right to carry out controls on transfers of certain dual-use items within the EU in order to safeguard public policy or public security, but the subject of export control had evolved between the two regulations.[46] Whereas Regulation 3381/94 focused on the movement of dual-use goods,[47] Regulation 1334/2000 expanded the scope of export controls to be also inclusive of dual-use software and technology. As a result of including software and technology into the items subject to export control, the definition of export activities expanded under Regulation 1334/2000 to include "[the] transmi[ssion of] software or technology by electronic media, fax or telephone to a destination outside the Community."[48] The entities subject to dual-use export control are no longer limited to goods, but also intangible technologies, thus creating the need to redefine export activities.

When Regulation 428/2009 replaced Regulation 1334/2000, human rights concerns were added to Regulation 428/2009 as a policy goal, and member states could impose additional export control due to human rights concerns to the list of dual-use goods and technology found in Annex I of Regulation 428/2009.[49] While this did not change the structure of Regulation 428/2009

43 See Michel, *supra* note 41, p. 51.

44 Council Regulation 3381/94, 1994 O.J. (L 367) 1 (EC).

45 Council Regulation 1334/2000, 2000 O.J. (L 159) 1 (EC).

46 The concept of public security has been defined by the European Court of Justice to include a "Member State's internal security and its external security" and "the exportation of goods capable of being used for military purposes to a country at war with another country may affect the public security of a Member State." Ground 28 of Case C-70/94 of 17 October 1995. – Fritz Werner Industrie-Ausrüstungen GmbH v Federal Republic of Germany. Council Regulation 3381/94, 1994 O.J. (L 367) 1 (EC). Council Regulation 1334/2000, 2000 O.J. (L 159) 1 (EC).

47 Council Regulation 3381/94, art. 1, 1994 O.J. (L 367) 1 (EC).

48 Council Regulation 1334/2000, art. 2(c), 2000 O.J. (L 159) 1 (EC).

49 Council Regulation 428/2009, art. 8, 2009 O.J. (L 134) 1, 1 (EC).

from its preceding regulations, the added policy concern refocused the policy goals of export controls in the EU.

Regulation 428/2009 defined export as being inclusive of three different types of activities. The first type of activity is the outbound movement of goods originating from the EU that leaves the territory of the EU.[50] The second type of activity is the re-export of goods that originated from outside of the EU that are not simply in transit through the EU and could be subject to additional policy measures for re-exportation.[51] The third type of activity is the transmission of technology or software through electronic media to a destination outside of the EU that includes making such technology and software available to legal and natural persons outside of the EU through methods such as oral transmission over the telephone.[52] Although making technology available to legal and natural people outside of the EU is considered to be a type of export, the Regulation does not view the cross-border movement of a person to be a transmission of technology.[53]

The allocation of exporter liability in the Regulation is imposed on the exporter, and the natural or legal person or partnership that could be determined as an exporter are separated into two categories. The first category of exporters are those in contract with the consignee in a third country that make an export declaration that has the power to determine where to send items out of the EU or those without an export contract but still have the power to determine where to send items out of the EU.[54] The second category of exporters are those that have transmitted or made software or technology available by electronic media.[55] The category of exporters is divided based the items they export. While the liability of a dual-use exporter of physical items could be determined by the structure of a contractual relationship, that requirement is not a factor for an exporter of software or technology. Any provider or transmitter of a software or technology export that is aware that they are electronically allowing people outside of the EU to obtain the technology would be liable as an exporter. Under this definition, it is possible that a service provider or cloud computing service that has made software available to people outside of the EU is liable to export control under the EU. This would impose a heightened export liability for internet and cloud computing service providers for the transmission of intangible property.

50 Council Regulation 428/2009, art. 2(2)(i), 2009 O.J. (L 134) 1, 1.
51 Council Regulation 428/2009, art. 2(2)(ii), 2009 O.J. (L 134) 1, 1 (EC).
52 Council Regulation 428/2009, art. 2(2)(iii), 2009 O.J. (L 134) 1, 1 (EC).
53 Council Regulation 428/2009, art. 7, 2009 O.J. (L 134) 1, 1 (EC).
54 Council Regulation 428/2009, art. 2(3)(i), 2009 O.J. (L 134) 1, 1 (EC).
55 Council Regulation 428/2009, art. 2(3)(ii), 2009 O.J. (L 134) 1, 1 (EC).

3.3 *Comparison between U.S. and EU Dual-Use Export Control Regulations before 2018*

The US and the EU dual-use export control regulations were both established with national security concerns as a core focus and allocated the liability of exporting goods and technology to domestic exporters. Prior to the passage of ECRA in 2018, the dual-use export control lists in the US and the EU were aligned with lists established by international export control agreements to create a united front to prevent proliferation of military-use technologies.[56] The primary difference between the US and the EU dual-use export controls exist in the allocation of export liability, and this difference is particularly noticeable as emerging technologies have played a role in changing the structure of export control for intangible technology.

The control of intangible technology was not the norm in international trade. International trade agreements such as the GATT have traditionally been focused on the trade in physical goods and not on the cross-border movement of knowledge or intangible technology. The US export control has been the exception to this as it has been inclusive of regulating intangible technology in its regulations. As was discussed in the previous section, the EU dual-use export control regulations did not include software and technology as entities for export control in its dual-use export control regulations until Regulation 1334/2000. The original framework of export controls held a person liable to export controls if they have knowledge and control over the final destination of the goods that are being transported from one jurisdiction to another. Without changing the original regulatory structures of export controls, the use of new technology expands the venues for export activities and potentially shifts the export control liabilities imposed under US and EU regulations so that the two jurisdictions would arrive at different conclusions for similar export activities.

The development of new technologies created new venues and methods for export activities to be subject to the control of US and the EU export control regulations. These new technologies have provided ways for intangible technology to be transmitted without being attached to physical goods, and regulations specifically drafted for the purpose of containing intangible technology became more important in discussing the changes made under export control regulations. The US had consistently included the export control of knowledge and intangible technology into its export controls, and the challenge for the US when faced with these new technologies was the implementation of control

56 Cindy Whang, *Undermining the Consensus-Building and List-Based Standards in Export Controls: What the US Export Controls Act Means to the Global Export Control Regime*, 22 Journal of International Economic Law, pp. 583–585 (2019).

on these new technologies that could influence the compliance structure of dual-use export controls. The challenge was the balance of national security interests against commercial interests when trying to enforce export activities on the new technologies. For the EU, the development of these new technology facilitated the inclusion of software and technology as subject matters added to dual-use export control regulations. What might seem to be an expansion to the scope of export-controlled entities actually reflected the advances of new technology and its impact on EU's export control regulations.

The determination of liability was also different between the US and the EU, and this difference could potentially become more nuanced through the development of new technology. To begin with, the determination of export liability for electronic transmission under the US EAR required that the exporter be the principal party in interest. The Advisory Opinion given by BIS had made it clear that passively making technology available for transmission without deriving direct financial gain from the transmission would not automatically qualify the provider of the electronic transmission to be an exporter.[57] This is different from the EU's definition of exporter in Regulation 428/2009 where the there is no requirement of a person to obtain financial gain to be viewed as an exporter as long as transmission or availability of technology was made to a party outside of the EU. However, since the US has historically been focused on the control of technology and knowledge in its intangible form, the jurisdictional reach of the US export control is also more far-reaching. Under the US dual-use export control, an export-controlled technology that is released to foreign persons inside the US is also subject to export control, and re-exports of export-controlled goods and technology beyond the borders of the US are all subject to the export control of the US. This is different from the export activity stated through EU Regulation 428/2009 where export activities specifically refer to the transmission of technology out of the EU, and the movement of people that cross borders does not count as falling under the purview of Regulation 428/2009.[58]

As a result, the arms of the US dual-use export control seem to reach further extraterritorially, while there seems to be a higher probability for the EU's dual-use export control to impose more liability on internet or cloud service providers. For both the US and the EU, even when faced with the regulatory changes made with the ever-evolving technology changes, the structure and content of export control have not shifted too much. However, with the amendments made to the US export control regime after ECRA and the amendments

57 See *supra* note 22.

58 Council Regulation 428/2009, art. 7, 2009 O.J. (L 134) 1, 1 (EC).

proposed for Regulation 428/2009, there are substantial changes in store for both of these export control regimes, as will be discussed in the following sections.

4 The Diverging Paths: Geoeconomics and Human Security Concerns of Dual-Use Export Control

Advances in technology have created the need to amend the US and the EU dual-use export control regulations to protect the national security concerns of these countries. However, even with the amendments, the policy focus of dual-use export controls has never strayed far from the fundamental policy rooted in protecting the national security of the export controlling country. The changes made to the US dual-use export control regulations in ECRA and the proposed amendments made to Regulation 428/2009 signaled a significant shift in the policy focus of dual-use export controls. For the US, the trade conflict with China and the need to maintain technological leadership changed the purpose of dual-use export control policies to include economic policy considerations. For the EU, the consideration of protecting cybersecurity and human rights through the regulation of dual-use export controls aligned with the EU's overall security policy. The ECRA and proposed amendments for Regulation 428/2009 have both expanded the policy scope of their regulations to incorporate different policy concerns, and the variance of economic or human rights consideration for domestic dual-use export controls could potentially increase the administrative measures in different jurisdictions as it relates to the trade of technology.

4.1 *Geoeconomics: The US Export Control Reform Act of 2018*

When the US passed ECRA in 2018, one of ECRA's national security policy goals stated that, "…the United States [needs to] maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation. Such leadership requires that United States persons are competitive in global markets."[59] ECRA included controlling the export of emerging and foundational technologies in its statute, and ECRA discussed the establishment of the foundational and emerging technology export control list as a national security concern of the US.[60] However,

59 Export Control Reform Act of 2018, 50 U.S.C. §4811(3).

60 Export Control Reform Act of 2018, 50 U.S.C. §4817(1).

ECRA never clearly defined the parameters and elements of how emerging and foundational technologies would be identified, and the context of the national security need mentioned in ECRA was slightly different from the traditional military-oriented national security concerns. ECRA's national security concern has expanded to include economic considerations as it discussed the need for the US to maintain its global leadership role in the science and manufacturing sectors in order to maintain their competitiveness in international markets.

The expanded policy changes made to the US dual-use export control regulations could best be described through the concept of geoeconomics. Geoeconomics has been described by Robert Blackwill and Jennifer Harris as "[t]he use of economic instruments to promote and defend national interest, and to produce beneficial geopolitical results; and the effects of other nations' economic actions on a country's geopolitical goals."[61] Anthea Roberts, Henrique Choer Moraes and Victor Ferguson further explored the concept of geoeconomics by anchoring a country's use of economic instruments and economic actions to those of a country's economic policies, stating that geoeconomics meant an increase in the "securitization of economic policy and economization of strategic policy" in a country's policy-making process.[62] For the US, passing ECRA was a good example of geoeconomics where economic considerations were being added into strategic policies, and national security concerns have become interwoven with economic policy concerns. As a result, the dual-use export control of the US was no longer rooted only in national security concerns, but the reach of security considerations was expanded to include using dual-use export controls to maintain global technological leadership.

4.1.1 Emerging and Foundational Technologies

In November of 2018, as a result of ECRA calling for the identification and establishment of the emerging and foundational technologies list, BIS posted in the Federal Register a Department of Commerce Advanced Notice of Proposed Rule Making related to the Review of Controls for certain Emerging Technologies (the Notice).[63] The Notice proposed rulemaking for the review of controls for emerging technologies.[64] BIS stated that the emerging technologies and foundational technologies would be proposed as two separate lists, and the Notice was for establishing the category of emerging technologies. Fourteen types of emerging technologies were proposed to be export controlled in the Notice:

61 See Blackwill and Harris, *supra* note 10.

62 See Roberts, Choer Moraes, and Gerguson, *supra* note 10.

63 Review of Controls for Certain Technologies, 82 Fed. Reg. 58201 (Nov. 19, 2018).

64 Ibid.

biotechnology, artificial intelligence, navigation technology, micro-processing technology, advanced computing technology, data analytics technology, quantum information and sensing technology, logistics technology, additive manufacturing such as 3D printing, robotics, brain-computer interfaces, hypersonics, advanced materials, and advanced surveillance technologies.[65]

The comments submitted in response to the Notice were not supportive of listing the fourteen technologies as emerging technologies. The commenters had three concerns regarding the emerging technologies list. The main concern had to do with the lack of clarification of the definition of emerging technology. ECFA did not include the criteria of determining how emerging technologies would be identified, and commenters sought to define the elements needed to be construed as an emerging technology.[66] Included in the question of trying to define the parameter of emerging technology was a preference for the technologies to be closely aligned with military-use technology. Another concern raised was that the scope of emerging technology in the Notice was too broad. Commenters noted that some of the technologies included in the lists, such as artificial intelligence, were already in wide use in commercial applications. According to these commentators, imposing export controls on these technologies would hinder both the commercial trade and interdisciplinary technological developments involving these technologies.[67] The last concern that commenters had was the unilateral application of export controls. Because the category of emerging technologies was specifically created in ECRA and not identified in international export control agreements, this category of technology is controlled unilaterally. There was a desire for

65 Ibid., p. 58202.

66 The American Bar Association Section of International Law proposed a definition of emerging technology that reflected the proposals of other commenters. The definition of emerging technologies should be specific non-mature technologies that include the following elements: 1. important for the United States in maintaining a qualitative military or intelligence advantage or for U.S. national security; 2. not widely available or traded within the global marketplace; 3. not available in US embargoed countries including arms embargoed countries; 4. not possessing significant commercial value to US persons who have invested in making the finished items and technology generally available commercially; and 5. cannot be controlled or monitored through other methods." See American Bar Association Section of International Law, *ABA SIL Comments on Emerging Technologies ANPRM* (10 January 2019), available at: https://www.regulations.gov/document?D=BIS-2018-0024-0157.

67 See Harvard University, *Comments on Advanced Notice of Proposed Rulemaking Regarding Review of Controls for Certain Emerging Technologies* (22 February 2019), https://www.regulations.gov/document?D=BIS-2018-0024-0180. See also EGADD, RIN 0694–AH61: Review of Controls for Certain Emerging Technologies (31 May 2019), available at: https://www.regulations.gov/document?D=BIS-2018-0024-0234.

there to be more multilateral cooperation with other countries instead of the unilateral application of the export controls on emerging technology by the US.[68] As of July 2020, BIS has not announced the finalized list of emerging and foundational technologies, and the emerging technologies list has not been implemented under ECFA.

4.1.2 Other EAR Measures

Although the emerging and foundational technologies list has not been finalized as of July 2020, this has not deterred the US government from using other export control measures in the EAR to target specific industries under the claim of protecting national security. This was especially the case for the export control measures that have been levied on the Chinese enterprise, Huawei Technology Co. (Huawei). On 15 May 2019, Trump signed the "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" that identified information and communications technology as a vulnerable US industry that needed to be protected.[69] On the same day, the US Department of Commerce added the world's largest telecommunications firm Huawei to the EAR's Entity List.[70] The EAR's Entity List contains the names of foreign persons that are reasonably believed to be involved, or to pose a significant risk of being or becoming involved in activities contrary to the national security to foreign policy interests of the US.[71] By adding Huawei to EAR's Entity List, the US has subjected the export activities of Huawei to increased administrative restrictions and scrutiny.

Consequently, in 2020, the US made three other amendments to the EAR that directly or indirectly controlled the trade of technology with China and Huawei for the purpose of promoting the national security and foreign policy

68 See American Association for the Advancement of Science, *Comment on FR Doc # 2018–25221* (22 February 2019), available at: https://www.regulations.gov/document?D=BIS-2018-0024-0174. See also Association of University Export Control Officers, *AUECO BIS – Full Response – ANPRM – Emerging Technology – Final – Executed* (*01-08-2019*) (14 February 2019), available at: https://www.regulations.gov/document?D=BIS-2018-0024-0085.

69 See The White House, Executive Order on Securing the Information and Communications Technology and Services Supply Chain (15 May 2019), available at: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

70 See United States Department of Commerce, *Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List* (15 May 2019), available at: https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd.

71 Export Administration Regulation 15 C.F.R. §744.16 (2020).

interests of the US. The first amendment was made to expand the military end use and military end-user controls specifically for items such as semiconductor equipment, sensors and other technologies that are being exported to China, Russia, and Venezuela.[72] The inclusion of military end-users into the regulations instead of only controlling the end use was an expansion of individuals that might create export liability for exporters. The second amendment BIS made was the Elimination of License Exception Civil End-User (CIV).[73] The civil end-user exception authorized the exports, reexports, and transfers of certain national security controlled items without prior review by BIS when the exception's criteria were met, and the export was directed at civil end users or civil end uses in the Country Group D:1, the countries listed in the EAR for national security reasons.[74] The rationale for removing this exception was to protect the national security controlled items from the countries listed in the Group D:1 because the technology developments between civilian and military technology were becoming more integrated.[75] The third EAR amendment was amending General Prohibition Three, also known as the foreign-produced direct product rule.[76] The amendment applied new controls to foreign-produced items if these items consisted of US export controlled "technology" or "software" and when there was knowledge that the foreign-produced item was destined for those on the Entity List under Supplement No. 4 to Part 744.[77] The amendment to this rule specifically applies to Huawei and its non-U.S. Affiliates as entities.

The results of the 2020 EAR amendments were that the heavy burdens of export control liabilities were placed on entities that engaged in technology trade with the US under the guise of national security concerns. This liability is specifically imposed on countries such as China, and companies such as Huawei, that the US see as being a threat to the US' global technological leadership. The amendments made to the EAR also sought to impose US export control on foreign-produced items, highlighting the questionable extraterritorial

72 Expansion of Export, Reexport, and Transfer (In-Country) Controls for Military End User or Military End Users in the People's Republic of China, Russia, or Venezuela; Correction, 85 Fed. Reg. p. 34306 (3 June 2020).

73 Elimination of License Exception Civil End Users (CIV), 85 Fed. Reg. p. 23470 (28 April 2020).

74 Export Administration Regulation 15 C.F.R. § 740.5 (2016).

75 Elimination of License Exception Civil End Users (CIV), 85 Fed. Reg. p. 23471 (28 April 2020).

76 Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, 85 Fed. Reg. p. 29849 (19 May 2020).

77 Ibid., p. 29850.

reach that the US gave its export control regulations. The EAR amendments reflected the US' expansive use of dual-use export control regimes to achieve their economic and national security goals.

4.2 *Human Security Concerns: The Proposed Regulatory Changes for EU Regulation (EC) No. 428/2009*

After the EU's dual-use export control Regulation 428/2009 had passed, the European Commission presented reports and reviews of Regulation 428/2009 in 2013 and 2014 in order to assess the evolving security and technology advances that would challenge the EU's dual-use export control regime.[78] In 2015, The European Commission made an impact statement and proposal to Regulation 428/2009 that listed specific policy objectives for export control policy review that included adjusting the EU export controls to reflect security risks and technological developments, prevent the export of cyber-surveillance technology that could be misused to violate human rights, and reduce the administrative burden associated with controls by creating effective and consistent application of controls in the EU.[79] Through the policy review, five options and impact assessments were made for changing the EU's dual-use export control regulations,[80] and a preferred option of combining the options of adjusting the EU regulatory framework

78 See European Commission, *Report from the Commission to the Council and the European Parliament on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items* (Oct. 16, 2013), available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0710:FIN:EN:PDF. See also European Commission, *Communication from the Commission to the Council and the European Parliament, The Review of export control policy: ensuring security and competitiveness in a changing world* (24 April 2014), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0244&from=EN.

79 See European Commission, *Commission Staff Working Document Impact Assessment, Report on the EU Export Control Policy Review Accompanying the document 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* 20–21 (28 September 2016), available at: https://trade.ec.europa.eu/doclib/docs/2016/october/tradoc_155008.pdf.

80 Policy option no. 1 was the baseline scenario where no policy change was implemented. Policy option No. 2 was called "Implementation and Enforcement Support" that consisted of using soft law and non-regulatory actions to develop a EU system. Policy option No. 3 was called "EU System Upgrade" that would make adjustments to the EU regulatory framework. Policy option No. 4 was called "EU System Modernization" that would introduce a new human security dimension to EU's export control system and resolve the insufficient control of cyber-surveillance technologies. Policy option No. 5 was called "EU System Overhaul" that would create a full centralization of controls at EU level. Ibid., pp. 21–27.

and policy focus on cyber-surveillance technologies and human rights was made.[81] This option was consistent with the EU's structure of rights-based approach that sought to prevent the proliferation of the weapons of mass destruction and decrease the threat of terrorism in improving human rights around the world.[82] The concept of improving human rights as a policy goal was introduced as a "human security" element that was added to the proposal to amending the EU's dual-use export control regime.[83]

4.2.1 The Catch-all Control for Violation of Human Rights

The concept of "human security" was proposed during the process of reviewing Regulation 428/2009 that would prevent the misuse of digital surveillance and an intrusive system that would result in human rights violations.[84] In the proposed amendments made in 2016, the protection of human rights have evolved into creating a "catch-all control" that could be applied to non-listed dual-use items when there is the risk of terrorism and violation of human rights in an item's end use.[85] The establishment of a catch-all provision meant that for dual-use goods and technology not classified on the EU dual-use export control lists, these items would be subject to EU export control if it is known that the items could be used for committing terrorism and/or human rights violations.[86]

The feedback given by EU industries and member states in response to adding the concept of "human security" to the EU's dual-use export control regime were mixed.[87] The feedback acknowledged that implementing a catch-all control for dual-use items might have a positive impact on promoting global human rights.[88] However, the industries were concerned with how the catch-all controls would be implemented and the potential negative impact it would

81 See European Commission, *supra* note 77, p. 5.

82 See Machiko Kanetake, *The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches*, 4 Bus. and Human Rights J, 155, 157 (2019).

83 See Beatrix Immenkamp, *Briefing: EU Legislation in progress: Review of Dual-Use Export Controls,* European Parliamentary Research Service (Nov. 2019), https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

84 See European Commission, *supra* note 77, pp. 23–24.

85 See European Commission, *supra* note 77, pp. 12–13.

86 Ibid.

87 See Bundesverband der Deutschen Industrie e.V., *EU Dual-Use Reform: EC Proposed Regulation COM* (2016). See also DigitalEurope, *European Commission Proposed Recast of the European Export Control Regime* (24 February 2017).

88 See European Commission, Final report: Data and Information Collection for EU Dual-Use Export Control Policy Review 220–221 (2015).

have on the EU's industries.[89] One of the concerns was that applying a catch-all control for dual-use goods and technology would change the structure of the EU's export control regime because the export control list contained in Annex I would not be the defining EU export control list.[90] The establishment of a catch-all control creates a category of unspecified technologies under the EU's dual-use export control regulations that would not be predetermined based on the characteristics of the technology, but rather on the end use of the technology. The catch-all control creates an open-ended export control list that imposes liability for the exporters based on the way the exported item was used. Another concern was the unilateral nature of EU's catch-all control that would cause EU's dual-use export control lists to differ from the international dual-use list agreed upon through various international export control agreements.[91] The cost associated with maintaining export control compliance might place EU industries at a competitive disadvantage because there would be increased need for administrative oversight and cost related to dual-use export control compliance.[92]

As of July 2020, the proposed amendments to the EU's dual-use export controls have not been adopted, so whether or not the catch-all control related to human security would be integrated into the EU's dual-use export control regime remains undecided. However, the proposition of adding a catch-all control to protect human security could change the structure of the export control lists so that export control lists could potentially become more open-ended and susceptible to the policy considerations of export controlling countries.

4.3 *The Changing Landscape of Dual-Use Export Controls*

ECRA and the proposal made to Regulation 428/2009 reflected a policy change to the dual-use export control regime as the policy purposes have expanded to include other considerations in addition to national security concerns. The inclusion of economic policy concerns and human security concerns have created structural differences for the US and the EU dual-use export control regimes in the construct of export control lists and the control of end use and

89 See Bundesverband der Deutschen Industrie e.V., *supra* note 87, p. 9. See also DigitalEurope, *supra* note 87,pp. 3–5.

90 See Bundesverband der Deutschen Industrie e.V., *supra* note 87, pp. 6–9. See also DigitalEurope, *supra* note 87, p. 3.

91 See DigitalEurope, *supra* note 85, pp. 3–5.

92 See Bundesverband der Deutschen Industrie e.V., *supra* note 87, pp. 6–9. See also DigitalEurope, *supra* note 87, pp. 3–5.

end-users to export control liability. This change will drastically change the functions of dual-use export control regulations in their own countries and create great divergence in the actual implementation of dual-use export control regimes around the world.

Because the export control lists are no longer determined through the evaluation of their relationship with military-use technology, the evolving export control regulations create additional administrative costs and legal uncertainties for the technology companies involved in the trading of technologies. For ECRA, the dual-use export control list was expanded to include new sets of lists of emerging and foundational technologies that seemed to be more inclusive of technologies not purely meant for military-use. The EU's 2016 proposed framework could potentially sideline the use of the export control lists as the main guide for determining the goods and technologies subject to export control. Since the US has decided to unilaterally add technologies not adopted by multilateral agreements to its dual-use export control lists and also mandate its export control liability be imposed on foreign produced US technology and software, there is a question of the legality of the jurisdictional reach of the US export control regulations.

As the line between military-use technology and civilian technology continues to blur, what would constitute as emerging technology or technologies subject to export control might be different under different jurisdictional export controls. A potential consequence might be a restructuring of the global technology supply chains and the investment of manufacturing facilities in countries with large internal markets that have strict export control. For example, the Taiwan Semiconductor Manufacturing Co. (TSMC), the world's largest semiconductor foundry holding 52% of the market share in the international foundry segment,[93] announced that it was planning to invest in building a manufacturing facility in the US.[94] Since TSMC is a supplier of semiconductor chips to many hi-tech corporations in the US, TSMC's investment within the US would decrease the need for export control considerations that it otherwise might need to resolve as a corporation with a manufacturing plant located in Taiwan.

93 See TSMC, TSMC Annual Report 2019 (I) 4, available at: https://www.tsmc.com/download/ir/annualReports/2019/english/pdf/e_all.pdf.

94 See TSMC, *TSMC Announces Intention to Build and Operate an Advanced Semiconductor Fab in the United States* (15 May 2020), available at: https://www.tsmc.com/uploadfile/pr/newspdf/THGOANPGTH/NEWS_FILE_EN.pdf.

5 Conclusion

Dual-use technology export control was a trade measure established to secure national security and contain the international proliferation of weapons. As the US and the EU start to differ in their policy goals for dual-use export control, changes are being made to the export control lists and the structure of export liability so that there would be noticeable differences found in the two different export control regimes. As military-use technology and civilian-use technology become less discernable from each other, the control of emerging technologies becomes harder to be defined under the conflicting policy goals that are presented by the US and the EU. What might be true is that the changing national security focus for the dual-use export control regimes will create challenges in the trade of emerging technologies.