VOLUME 4 April 2023 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

ENTITY OF THE STATE: THE TRANSPARENCY OF RESTRICTING TELECOMMUNICATIONS FIRMS AS THREATS TO AMERICA'S NATIONAL SECURITY

Benjamin W. Cramer

INTRODUCTION 57
I. THE ENTITY LIST 58
II. TOWARDS THE COVERED LIST 65
III. POLITICAL AND NEWS FRAMING OF NATIONAL SECURITY THREATS 71
IV. VAGUENESS AND POOR TRANSPARENCY IN EXPORT/IMPORT POLICY 74
V. THE RAMIFICATIONS OF EXPORT/IMPORT RESTRICTIONS IN TELECOMMUNICATIONS 83
CONCLUSION 89

ENTITY OF THE STATE: THE TRANSPARENCY OF RESTRICTING TELECOMMUNICATIONS FIRMS AS THREATS TO AMERICA'S NATIONAL SECURITY

Benjamin W. Cramer[*]

INTRODUCTION

Telecommunications networks are now considered to be crucial for national security, and there is growing awareness of how foreign adversaries could target such networks for their own gain. In recent years, the American government has subjected the telecom sector to increasing restrictions on exports and imports, usually justified by concerns over threats to national security when equipment is bought from, or sold to, suspicious foreign firms. As this article will argue, such governmental restrictions are typically the outcome of non-transparent agency decision-making procedures, with ramifications for citizen oversight of government operations and the health of the American telecommunications network.

The U.S. Department of Commerce maintains a document called the Entity List for foreign firms that American manufacturers are not permitted to export products and services *to*. This type of restriction has been common since the 1990s, but in more recent years the restrictions have been applied in the other direction as well. In 2019, President Donald Trump issued an executive order banning Americans from buying supplies from foreign telecommunications firms that have been deemed threats to national security. This added the Federal Communications Commission to the process, as that commission now maintains a document called the Covered List for foreign firms that Americans are not permitted to import *from*.

Journalists, government watchdogs, and even America's allies suspect that these export/import restrictions are politically motivated and based on poorly defined threats to national security, which is itself a poorly defined term. This turns relatively straightforward economic regulatory processes into a political drama that may lead to short-term rhetorical victories but long-term damage to the American telecom marketplace.

[*] Associate Teaching Professor, Donald P. Bellisario College of Communications, Pennsylvania State University.

The next section of this article describes the history of national security-oriented export restrictions in telecommunications, and the following section does the same for more recent import restrictions. Section three of the article deviates temporarily from legal and policy research into an analysis of the framing strategies used by politicians and the media to mold American public opinion of international economic competition, and how these viewpoints have found their way into trade policy. The fourth section analyzes the effects of opaque government agency processes, combined with poorly defined justifications, on the ability of interested citizens and companies to determine why the export/import restrictions were enacted. This is followed by an examination of how non-transparent restrictions may negatively affect the American telecom marketplace. The article concludes with a discussion of why more transparency is needed during this process, with recommendations for better methods of addressing suspicious foreign companies that do not require banning them from the American market and disrupting the development and operation of networks for consumers at home.

I. THE ENTITY LIST

Modern regulations giving the federal government oversight of exports sold by American manufacturers date back to the Export Administration Act of 1979,[1] which was passed during a period of military tension with several countries,[2] and new awareness that potential enemies might become stronger with equipment sold knowingly or unknowingly by American firms. Congressional debates at the time often used the phrase "U.S. security,"[3] which gradually became the more familiar "national security" by the new millennium. Export controls are typically enforced on items destined for countries that have been subjected to sanctions by the U.S. government, items in certain high-risk categories like nuclear power equipment, and items in some other technological categories that the government has deemed to be of

---

[1] 50 U.S.C. app. §§ 2401–20 (1979).

[2] During this period, international opinions of the United States were still recovering after the end of the Vietnam War in 1975, while the Soviet Union's aggression toward Afghanistan near the end of the decade exacerbated Cold War tensions. The United States had its own political conflict with Iran during this period, culminating in the Iran Hostage Crisis. *See* Kenneth W. Abbott, *Linking Trade to Political Goals: Foreign Policy Export Controls in the 1970s and 1980s*, 65 MINN. L. REV. 739, 756-763, 798-822 (1981).

[3] *See, e.g.*, S. REP. NO. 96-169 (1979) (concerning the Export Administration Act of that year).

strategic value.[4] In recent years, telecommunications equipment has been increasingly subjected to several types of export restrictions due to growing concerns about the industry's possible impacts on national security.[5]

The Export Administration Act instituted controls for both direct exports, in which an American company sells to a customer in a foreign nation, and "re-exports" in which that first foreign customer sells the item again to someone in a third country. Regulated product categories require an export license; American firms that mistakenly export controlled items without a license, or firms that violate an existing license, are typically charged a fine.[6] For most products, the Bureau of Industry and Security, a division of the Department of Commerce, exercises jurisdiction over exports and can require American firms to apply for licenses or outlaw certain exports altogether.[7] Current regulations require Commerce to consult with other government agencies per their areas of expertise.[8] For some items, licensing requirements and approvals from multiple agencies may be necessary.[9] As will be discussed herein, this results in many decisions by many agencies with their own procedures and definitions, which can lead to a shortage of transparency for interested citizens or companies trying to navigate through agency documents that readily announce final decisions but contain few useful references to prior decision-making processes.

The Export Administration Act eventually expired and was replaced by other statutes, and current export regulations are codified in Section 15 of the Code of Federal Regulations. That section mandates, and contains, the Entity List, which includes parties that American firms are not allowed to export *to*.[10] The Entity List was first published by the Department of Commerce in 1997 and has been regularly updated ever since.[11] While it was originally focused on preventing American products from winding up in the hands of enemies making weapons of mass

---

[4] *See* Michael T. Stewart, *U.S. Export Regulations: An Overview*, 241 N.J. LAW. 37, 37 (2006).
[5] 15 C.F.R. § 744.11(a)(2) (2022).
[6] *See* Stewart, *supra* note 4, at 37-38.
[7] *Id.* at 37.
[8] 15 C.F.R. § 730.4 (2022).
[9] *See* Stewart, *supra* note 4, at 39.
[10] 15 C.F.R. § 744.16 (2022). Note that export regulations are spread throughout various chapters of the Code of Federal Regulations, and are known collectively as Export Administration Regulations (EAR).
[11] Jeffery S. Allen, *Do Targeted Trade Sanctions Against Chinese Technology Companies Affect US Firms? Evidence from an Event Study*, 23 BUS. & POL. 330, 330-31 (2021).

destruction, it has since been expanded to encompass general foreign policy and national security interests that may be impacted by the export of American products.[12] Any American company wishing to do business with a foreign party that is on the Entity List must apply for a specific license from Commerce, and the Bureau of Industry and Security could reject the application.[13]

The Entity List identifies parties "reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States."[14] The regulations have no further definition of the phrase *reasonably believed*, nor by whom except entire Executive Branch agencies. Meanwhile, the phrase *national security* appears regularly throughout the regulations but with no definition beyond "activities that are contrary to the national security or foreign policy interests of the United States" and similar phrasing.[15] This oft-used but poorly defined term has resulted in many dubious and unaccountable export restrictions—and later, import restrictions—as will be discussed throughout this article.

As of 2023, companies headquartered in China or Russia are by far the most numerous on the Entity List, each with more than 300 listings.[16] A cursory review of those companies reveals many with some variation of "telecommunications" in their names. The lopsided representation from those two countries is largely due to longstanding suspicions of Chinese threats to American security interests, which have been festering for many years and were exacerbated during the Trump Administration. Meanwhile, American attitudes toward Vladimir Putin's regime in Russia have evolved from cooperative to frosty with Putin's gradually increasing militarism.[17] While the United States views several other nations and their companies as potential security risks, three particular telecommunications-oriented firms from China and Russia generated significant news coverage when they were banned from receiving exports from the United States.

---

[12] *See* Department of Commerce, Bureau of Industry and Security, *Entity List FAQs*, https://www.bis.doc.gov/index.php/cbc-faqs/faq/28#faq_282 (last visited Nov. 21, 2022).
[13] 15 C.F.R. § 744.16(a) (2022).
[14] 15 C.F.R. § 744.16 (2022).
[15] 15 C.F.R. § 744.11(b) (2022).
[16] 15 C.F.R. pt. 744 (Supp. 4 2022).
[17] *See* James Dobbins, Howard J. Shatz & Ali Wyne, *Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue*, RAND CORP. (Oct. 2018), at 2-8, https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE310/RAND_PE310.pdf.

Huawei Technologies Ltd. of Shenzhen, China is the world's largest manufacturer of general telecommunications networking equipment and one of the largest producers of smartphones.[18] Huawei first attracted the attention of American lawmakers in 2012 due to suspicions of copying American intellectual property. By 2018, additional concerns arose about the company's close relationship with the Chinese government, which could lead to malicious surveillance of American consumers and government officials.[19] The U.S. Department of Justice also investigated Huawei during this period for reselling American networking equipment to Iran, thus violating U.S. sanctions on that country.[20] However, with the exception of a plea deal to resolve individual charges against Huawei executive Meng Wanzhou in 2019,[21] all of the investigations are still in progress at the time of this writing and the company has not yet been formally convicted of any violation of U.S. law. Regardless, the Department of Commerce placed the company on the Entity List in 2019.[22] The associated regulatory document cites those previous investigations to conclude that "there is reasonable cause to believe that Huawei . . . has been involved in activities determined to be contrary to the national security or foreign policy interests of the United States."[23] The most recent regulatory document on the matter describes the company as a "continuing threat to U.S. national security and U.S. foreign policy interests."[24] Note the nearly identical terminology.

Zhongxing Telecommunications Equipment Corp., commonly known as ZTE, is another telecommunications firm based in Shenzhen, China, that is best known for its inexpensive smartphones targeted at

---

[18] *See* Frank Chen, *Inside Huawei's Huge HQ Campus in Shenzhen*, ASIA TIMES (June 28, 2019), https://asiatimes.com/2019/06/inside-huaweis-huge-hq-campus-in-shenzhen/.

[19] *See* Grace Sullivan, *The Kaspersky, ZTE, and Huawei Sagas: Why the United States Is in Desperate Need of a Standardized Method for Banning Foreign Federal Contractors*, 49 PUB. CONT. L. J. 323, 334 (2020).

[20] *See* Steve Stecklow, *Newly Obtained Documents Show Huawei Role in Shipping Prohibited U.S. Gear to Iran*, REUTERS (Mar. 2, 2020, 9:11 AM), https://www.reuters.com/article/us-huawei-iran-sanctions-exclusive-idCAKBN20P1VA.

[21] *See* Eric Tucker & Jim Mustian, *Huawei Exec Resolves Criminal Charges in Deal with US*, ABC NEWS (Sept. 24, 2021, 2:24 PM), https://abcnews.go.com/Technology/wireStory/justice-dept-huawei-exec-poised-resolve-criminal-charges-80212658.

[22] *See* Additions to the Entities List, 84 Fed. Reg. 22,961, 22,961–62 (May 21, 2019); 15 C.F.R. pt. 744 (Supp. 4 2022).

[23] *Id.*

[24] *See* Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule), 85 Fed. Reg. 51,596 (Aug. 20, 2020) (to be codified at 15 C.F.R. pts 734, 744, 762).

consumers in developing countries, but is also an active player in 4G and 5G networking equipment.[25] ZTE has long been suspected of infringing on the patents of American telecommunications products, but the company first gained the notice of the export restriction regime in the mid-2010s when it re-exported American products to Iran and North Korea.[26] ZTE was added to the Entity List in 2016 with the usual obligatory reasoning: "for actions contrary to the national security and foreign policy interests of the United States".[27]

Kaspersky Lab is a cybersecurity firm headquartered in Moscow, Russia, which for a time had contracts with about 15% of U.S. government offices for antivirus software and other security services.[28] Starting in 2016, U.S. officials began to suspect that the company was closely tied to the regime of Vladimir Putin, mostly due to his longtime association with CEO Eugene Kaspersky, which in turn fed suspicions that Russia could use the company's software to spy on the U.S. government. In 2017, despite a lack of concrete evidence, the Department of Homeland Security ordered all government agencies to remove their Kaspersky software.[29] To date, Kaspersky Lab is not yet on the Department of Commerce's more expansive Entity List, though its products have been subjected to specific restrictions from the Federal Communications Commission.[30]

The most recent high-profile international firm to be added to the Entity List, this time by the Biden administration, is NSO Group of Israel,[31] which journalists exposed in 2021 for selling its smartphone surveillance technology to governments around the world, including

---

[25] *See* Rachel Layne, *3 Things to Know About ZTE and Huawei*, CBS NEWS (June 7, 2018, 3:49 PM), https://www.cbsnews.com/news/3-things-to-know-about-zte-and-huawei/.
[26] *See* Sullivan, *supra* note 19, at 331.
[27] *See* Additions to the Entity List, 81 Fed. Reg. 12,004 (Mar. 8, 2016) (to be codified at 15 C.F.R. pt. 744).
[28] *See* Dustin Volz, *About 15 Percent of U.S. Agencies Found Kaspersky Lab Software: Official*, REUTERS (Nov. 14, 2017, 11:25 AM), https://www.reuters.com/article/us-usa-cyber-kaspersky-congress-idUKKBN1DE28P.
[29] *See* Sullivan, *supra* note 19, at 337–38.
[30] *See* Dan Goodin, *FCC Puts Kaspersky on Security Threat List, Says It Poses 'Unacceptable Risk'*, ARSTECHNICA (Mar. 25, 2022, 8:38 PM), https://arstechnica.com/information-technology/2022/03/fcc-puts-kaspersky-on-security-threat-list-says-it-poses-unacceptable-risk/.
[31] *See Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities,* U.S DEP'T OF COM. (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

several dictatorships.[32] Following the largely enemy-based use of the Entity List by the Trump administration, the restriction of NSO Group by the Biden Administration was the first prominent use of this export control technique against a company residing in a staunch-allied nation after the Trump era.[33]

For any company on the Entity List, placement is decided by an "End-User Review Committee" chaired by a representative from the Department of Commerce and including representatives from the Departments of State, Energy, Defense, and (when relevant) Treasury.[34] The regulations contain few details on how this committee should reach its decision to add a company to the Entity List, except that decisions must be unanimous and that the resulting documents must properly cite that same category of regulations.[35] There is no requirement to cite decision-making documents by the Department of Commerce or other agencies that may have investigated the foreign firm. A listed company can request removal from the End-User Review Committee,[36] but the delisting process is described with the same lack of detail as the listing process.[37]

The ultimate result is a regulatory document from the Department of Commerce stating that the End-User Review Committee decided that a foreign firm was a threat to national security due to suspicious activities, or preliminary investigations of such by other agencies, that may or may not have come to fruition, and typically without citations to investigative or decision-making documents. For example, in 2018, a company from the British Virgin Islands called Evans Meridians Ltd. was added to the Entity List. The regulatory document stated that the committee had decided that the firm tried to re-export American equipment to Iran in violation of U.S. sanctions, but provided no citations to any documents that informed this decision.[38] As another example, in 2021, a company called Gensis Engineering from Turkey was

---

[32] *See* Drew Harwell et al., *Biden Administration Blacklists NSO Group over Pegasus Spyware*, WASH. POST (Nov. 3, 2021, 2:30 PM), https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/.

[33] *See* David E. Sanger et al., *U.S. Blacklists Israeli Firm NSO Group over Spyware*, N.Y. TIMES (Nov. 3, 2021), https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html.

[34] 15 C.F.R. § 744.16(d) (2022).

[35] 15 C.F.R. pt. 744 (Supp. 5 2020).

[36] 15 C.F.R. § 744.16(e) (2022).

[37] 15 C.F.R. pt. 744 (Supp. 5 2020).

[38] *See* Addition of Certain Entities to the Entity List, Revision of Entries on the Entity List and Removal of Certain Entities from the Entity List, 83 Fed. Reg. 44821, 44822 (Sept. 4, 2018); 15 C.F.R. pt. 744 (Supp. 4 2022).

added to the Entity List, with the regulatory document lumping that company in with more than a dozen others under suspicion for trafficking American equipment to Iran. That document states only that the committee "determined" that the company was involved in "activities that are contrary to the national security and/or foreign policy interests of the United States"—the exact same phrase that appears in the governing regulations—and once again with no citations to actual investigative documents.[39]

Furthermore, the Entity List includes a column titled *License review policy* which contains the phrase "presumption of denial" for most of the companies listed.[40] This means that if any American company wants to apply for a license to export goods to such a foreign company, the Department of Commerce has already declared that the license will likely be denied. How this decision was made, and what types of extenuating circumstances could possibly override it, are usually absent from the regulatory documents. For example, in 2020, a company called Multi Technology Integration Group from Bulgaria was added to the Entity List with a "presumption of denial" for any future export licensing requests. The regulatory document states that this company is a suspected front for operators who smuggle American products into Russia.[41] Like in the examples above, no citations are given to any outside documents in which this determination was made. Moreover, no cited evidence is given to support the "presumption of denial," but in fairness, the presumption for the Bulgarian firm is limited to specific technological categories of "sensitive electronic components" of interest to Russia.[42]

With thousands of relevant documents, finding comprehensive or qualitatively significant patterns of citations is beyond the scope of the present article, but the author has determined that these examples, plus others described herein, are indicative of the transparency of Entity List decisions by the End-User Review Committee at the Department of Commerce, or the lack thereof.

The export-only restrictions described in this section, which, in short, tell an American company who it cannot export its products *to*, have been standard practice since the late 1970s. In the 2010s, political

---

[39] *See* Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List, 86 Fed. Reg. 71557 (Dec. 17, 2021); 15 C.F.R. pt. 744 (Supp. 4 2022).
[40] *See* 15 C.F.R. pt. 744 (Supp. 4 2022).
[41] *See* Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. 83416 (Dec. 18, 2020); 15 C.F.R. pt. 744 (Supp. 4 2022).
[42] Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. at 83417.

motivations and non-transparent suspicions of threats to national security expanded this regime to imports as well. Now American companies have additional rules for importing raw materials or components *from* certain targeted entities.

II. TOWARDS THE COVERED LIST

In the 2010s, it became increasingly common for the U.S. government not just to restrict exports to foreign business partners, but to enact controls in the other direction as well. Federal government agencies are now often restricted from contracting with foreign firms that reside in nations that America has deemed hostile to national security, especially China and Russia, for purposes of *importing* products and services. For example, in addition to the aforementioned export restrictions, in 2017 and 2018, U.S. government agencies were banned from entering into contracts with Kaspersky, Huawei, and ZTE.[43] All three have also had their products banned by the Federal Communications Commission (FCC) from any network development efforts that receive agency funds.[44]

Until 2019, these import restrictions were usually accomplished via annual defense budget authorization bills, which in turn often featured a specific focus on telecommunications equipment.[45] Starting in 2019, President Donald Trump adopted a strategy of restricting imports via executive orders and executive branch regulations, and this kicked off several new legislative efforts to address procedural gaps. Telecommunications equipment received particular attention during these developments. Such import restrictions have become increasingly popular, reflecting current political tensions and typically citing threats to national security, but they tend to be written with vague and expansive language that makes their effectiveness difficult to assess.[46]

On May 15, 2019, President Trump issued Executive Order No. 13873, which barred American telecom service providers from importing equipment from any foreign company that has been deemed a national

---

[43] *See* Sullivan, *supra* note 19, at 325.
[44] *See* Goodin, *supra* note 30. The FCC restrictions will be discussed at *infra* notes 168-173 and accompanying text. Note: While export/import controls are under the jurisdiction of the Department of Commerce, the FCC has authority over publicly-funded telecom development projects within the United States.
[45] *See, e.g.*, John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917-18 (2018). This statute specifically targeted ZTE and Huawei in § 889(f)(3).
[46] *See* Sullivan, *supra* note 19, at 324.

security risk.[47] Carrying the telecom-specific title, *Securing the Information and Communications Technology and Services Supply Chain*, the executive order uses very broad language, encompassing:

> services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries [that] augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.[48]

The executive order's language is particularly expansive and vague, beyond obvious hyperbole like "catastrophic" and "extraordinary." Elsewhere in the order, authority over the matters discussed is given to the Secretary of Commerce, but in conjunction with a bewildering plethora of other officials including the Secretaries of Treasury, State, Homeland Security, and Defense; plus the Attorney General, the U.S. Trade Representative, the Director of National Intelligence, the Chair of the Federal Communications Commission, and additional officials with expertise as needed.[49] In a reflection of current technological trends and political controversies, "information and communications technology or services" are mentioned specifically as crucial factors for "critical infrastructure" and the "digital economy."[50] The Department of Homeland Security received a specific command to continuously watch for hardware and software that could compromise such networks,[51] with a citation to an earlier executive order by President Barack Obama, which addressed the cybersecurity of critical infrastructure.[52] "Critical infrastructure" entered governmental parlance after the terrorist attacks on September 11, 2001; the term has been used in many statutes for systems in which disruption by enemies could cause

---

[47] *See* Exec. Order No. 13873, 84 Fed. Reg. 22,689 (May 15, 2019) (codified at 3 C.F.R. 13873).
[48] *Id.* The word "persons" in this excerpt reflects the traditional use of that word in export/import regulations, in which it serves as a catch-all term for individuals, companies, and organizations.
[49] *Id.* at 22689-90.
[50] *Id.* at 22690.
[51] *Id.* at 22691.
[52] *See* Exec. Order No. 13636, 3 C.F.R. 13636 (2014).

major hardships for the United States. "Critical infrastructure" tends to be vaguely defined in the law, and is often mixed up with the equally vague term "national security."[53]

While the executive order focuses on American persons or companies that do business directly with telecom firms that have been deemed hostile in themselves or are housed in hostile nations, its language (particularly pertaining to re-exports) is expansive enough to encompass economic transactions that take place outside of the United States as well.[54] The order also uses very broad language for its targeted products:

> [A]ny hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display.[55]

This broad categorization can sweep up practically all computerized telecommunications networking components that can process data, and the services that keep those components connected.[56]

The executive order invoked the International Emergency Economic Powers Act[57] and the National Emergencies Act.[58] Those two statutes allow such declarations from the President in the event of "unusual and extraordinary threats," with the former statute adding particular procedures for export/import transactions with hostile adversaries. These two statutes allow the President to unilaterally declare an emergency, and Congress only needs to be informed after the declaration has been made.[59] The term "emergency" can be used at will

---

[53] *See* Benjamin W. Cramer, *Envirodemic: Unconstitutional Restrictions on Environmental Protests from the Attacks of 2001 to the Struggles of 2020*, 14 L.J. SOC. JUST. 79, 81 (2021).
[54] *See* Caroline Elyse Burks, *The Case for Presumptions of Evil: How the E.O. 13873 'Trump' Card Could Secure American Networks from Third-Party Code Threats*, 11 AM. U. NAT'L. SEC. L. BRIEF 95, 99-100 (2021).
[55] 84 Fed. Reg. 22,689, 22,691.
[56] *See* Burks, *supra* note 54, at 100. Illustrating the executive order's expansive language, the Department of Commerce later published a list of industry sectors that can be included in the regulations, consisting of twelve types of telecom service providers, seven types of Internet service providers, and six types of equipment manufacturers. *See Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 65316, 65318-19 (Nov. 27, 2019).
[57] 50 U.S.C. § 1701 *et seq*. (1977).
[58] 50 U.S.C. § 1601 *et seq*. (1976).
[59] 50 U.S.C. § 1621 (1976); 50 U.S.C. § 1701 (1977).

too, and Trump's justification for the apparent emergency in 2019 is tough to decipher.[60] Trump opined that some telecommunications-related imports and exports constituted a "national emergency" because:

> additional steps are required to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States. In light of these findings, I hereby declare a national emergency with respect to this threat.[61]

The executive order did not list any specific foreign companies or what made them national security risks, and it also did not mention the Entity List in particular. However, it did instruct the Department of Commerce to draft enforcement rules[62] and to determine which companies and countries constitute national security threats.[63] Commerce, in consultation with various other knowledgeable agencies, was instructed to investigate any:

> undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States.[64]

Since Trump's executive order concerned both imports and exports, later that week Commerce added Huawei to the export-specific Entity List, as described above.[65] The timing was not a coincidence, as the department endeavored to fulfill Trump's goals. Secretary of Commerce Wilbur Ross made a public statement about his department's efforts to help the President tackle national security threats, but as is

---

[60] *See* David W. Opderbeck, *Huawei, Internet Governance, and IEEPA Reform*, 47 OHIO N.U. L. REV. 165, 173-74 (2021). *See also* 50 U.S.C. § 1701 (1977); 50 U.S.C. § 1702(a) (2001).
[61] Exec. Order No. 13873, 84 Fed. Reg. 22,689 (May 15, 2019) (codified at 3 C.F.R. 13873).
[62] *See* Kendra Chamberlain, *Trump to Ban U.S. Carriers from Using Network Gear Posing Security Risk*, FIERCE WIRELESS (May 15, 2019, 10:33 AM), https://www.fiercewireless.com/tech/trump-to-direct-us-carriers-to-ban-network-gear-pose-security-risk-reuters.
[63] 84 Fed. Reg. 22,689, 22,689-22,690.
[64] *Id.* at 22,690.
[65] *See* Additions to the Entities List, 84 Fed. Reg. 22,961, 22,961–62 (May 21, 2019); 15 C.F.R. pt. 744 (Supp. 4 2022).

common in his agency's Entity List documentation, Ross avoided details on the nature of those threats.[66]

The day before Trump left office, the Department of Commerce issued a rule to extend the 2019 executive order into the incoming Biden Administration, and for the Department's new leaders to continue collecting public comments on how to protect national security interests from threats posed by adversarial foreign telecom firms.[67]

Meanwhile, since the Entity List is focused on exports, new legislation was needed to tackle the aspects of Trump's executive order that concerned imports from the same suspicious foreign companies. The first legislative action concerned the use of federal money to buy equipment *from* suspicious foreign companies, and the apparent importance of telecommunications networks during such processes received specific attention from Congress. The Secure and Trusted Communications Networks Act, passed in March 2020, prohibits the use of telecom subsidies (which are managed by the Federal Communications Commission) to purchase networking equipment that presents a national security risk.[68] The statute did not define "national security" or the types of risks it faces from unsecure telecommunications equipment. The FCC was instructed to figure this out in consultation with yet another bewildering plethora of agencies: the Department of Homeland Security, the Department of Defense, the Director of National Intelligence, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI).[69] Neither the NSA nor the FBI had been suggested for their expertise on this topic in President Trump's executive order the previous year.

The Secure and Trusted Communications Networks Act mandated the creation of another list of suspicious foreign telecom-oriented companies, this time called the Covered List, to enable import controls and to be managed by the FCC, in a fashion similar to Commerce's ongoing management of the multi-industry and export-specific Entity List.[70] The FCC also found itself with new authority to decide that

---

[66] *See* Kendra Chamberlain, *Commerce Dept. Bans Huawei, 70 Affiliates from Sourcing U.S. Components*, FIERCE WIRELESS (May 16, 2019) [hereinafter Commerce Dept. Bans Huawei], https://www.fiercewireless.com/5g/commerce-dept-adds-huawei-and-70-affiliates-to-telecom-ban-list.

[67] *See* Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (Jan. 19, 2021).

[68] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, § 3(a), 134 Stat. 158, (2020).

[69] *Id.* at § 9(2).

[70] *See* Federal Communications Commission, Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization

something is a threat to national security.[71] Huawei and ZTE were among the first companies to be placed on the Covered List, with the commission's Public Safety and Homeland Security Bureau determining, per its new authority under the Secure and Trusted Communications Networks Act, that those companies were indeed threats to national security.[72] Given recent political controversies, that may have been a straightforward decision, regardless of the lack of a comprehensive definition of "national security". But, things were not so easy when it came to less newsworthy firms. More than a year after the Secure and Trusted Communications Networks Act was passed, the FCC issued a call for public comments as it attempted to put together the Covered List and procedures for maintaining it into the future.[73] Kaspersky Lab, which, as discussed above, is not yet on the Department of Commerce's export-only Entity List,[74] was added to the FCC's import-oriented Covered List in March 2022.[75]

The 2019 Secure and Trusted Communications Networks Act had a flaw in that it only applied to the use of federal subsidies for the purchase of items to be imported from suspicious foreign firms.[76] Another statute applying to purchases by private American companies, known as the Secure Equipment Act, was passed in October 2021 to close this loophole.[77] This statute also prohibited the FCC from allowing case-by-case exceptions (e.g., emergency network repairs in remote areas) to the restrictions mandated by a foreign firm's placement on the Entity List or Covered List, which it had been able to do thanks to another loophole in the 2019 statute.[78] Now, American firms were prohibited from both

---

Program, ET Docket No. 21-232/21-233, FCC 21-73 (June 17, 2021) at ¶ 13. The statute originally called the proposed list the "Covered Communications Equipment or Services List".

[71] *Id.* at ¶ 15.

[72] *See* Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program and the Competitive Bidding Program, 86 Fed. Reg. 46645-46 (Aug. 19, 2021) (to be codified at 47 C.F.R. pt. 2).

[73] *Id.* at 46653.

[74] *See Id.*

[75] *See* Federal Communications Commission, Public Notice on Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act (Mar. 25, 2022), https://www.fcc.gov/document/announcement-additions-covered-list.

[76] H.R. REP. NO. 117-148, at 2 (2021).

[77] Secure Equipment Act of 2021, 47 U.S.C. § 1601, Pub. L. 117-55, 135 Stat. 423-424 (2021).

[78] *See* Ron Amadeo, *The US Closes Huawei Loophole, Will No Longer Grant Exceptions for ISPs*, ARSTECHNICA (Nov. 12, 2021, 2:02 PM), https://arstechnica.com/gadgets/2021/11/the-us-will-no-longer-approve-exceptions-for-huawei-networking-gear/.

exporting *to* such foreign firms, via the older Entity List, and importing *from* them, due to the new statutes of 2020 and 2021.

III. POLITICAL AND NEWS FRAMING OF NATIONAL SECURITY THREATS

These new restrictions on both the import and export of telecommunications equipment from apparently untrustworthy foreign firms can be traced to several concurrent trends that gained traction in the 2010s. First was the obviously growing importance of interconnected global telecom networks and the equipment needed to sustain them. Second was the increasing use of the term "national security" in U.S. law with a definition that is incongruously tough to nail down. Third is a longstanding trend in the framing of America's geopolitical conflicts, particularly with China, which underwent a transformation during the Trump administration and exacerbated political arguments that in turn found their way into trade policy. These trends have continued under the Biden Administration, perhaps due to political inertia.

President Donald Trump's framing of collective threats, be they economic or otherwise, was rooted in right-wing populism, which promises to alleviate a nation's insecurities by naming enemies and drawing public support by vowing to counter those enemies.[79] Amplifying the threats themselves, and then amplifying how those threats contradict the values of the politician's supporters, is a fundamental aspect of this framing strategy.[80] Trump intensified this strategy with China in particular, linking America's longtime anti-Communist ideals with frequent references to "the Chinese Communist Party" and claims that the country was committed to an ideological struggle with the West.[81] Meanwhile, Trump's frequent use of the term "trade war," for what was in fact a complex economic and geopolitical entanglement, may have been intended to emphasize the simplistic term *war* as either the nature of the Chinese threat, or the nature of America's need to respond to that threat.[82]

In the realm of political discussion and understanding, framing is a well-researched phenomenon. In its most basic definition, the fashion in which an issue is "framed" has an impact on someone's opinions

---

[79] *See* Daniel Béland, *Right-Wing Populism and the Politics of Insecurity: How President Trump Frames Migrants as Collective Threats*, 18 POL. STUD. REV. 162, 164–65 (2020).
[80] *Id.* at 167.
[81] *See* Jacques deLisle, *When Rivalry Goes Viral: COVID-19, U.S.-China Relations, and East Asia*, 65 ORBIS 46, 50–51 (2021).
[82] *Id.* at 58.

toward and understanding of that issue.[83] Or in other words, the ordinary person uses mental shortcuts (frames) to comprehend a complex issue, but those mental shortcuts can be influenced by the source of the information. That source is likely to be a media outlet that the person consumes, a politician that the person admires, or the political party that the person supports.[84]

For politicians and policymakers, the framing process includes decisions on whether they should speak publicly about their substantive policy positions or emphasize the "horse race" competition with their political rivals. A similar choice must be made between emphasizing specific issues (like climate change or export/import policy) or generic values (like democracy or national security).[85] In particular, Donald Trump positioned geopolitical disagreements within his "America First" and "Make America Great Again" frames, in which other parties, be they political opponents or hostile nations, were depicted as threats to his supporters' values,[86] with "national security" frequently added to any such discussions that involved foreign affairs.[87] In the case of China, Trump's political framing of that nation as a threat to American values and safety intensified during the COVID-19 pandemic, with this adversarial stance finding its way into trade policy.[88]

Meanwhile, news framing is the process in which media professionals pick and choose portions of a complex topic for emphasis when explaining that topic to the audience, based on either explicit or implicit editorial guidelines that are themselves influenced by economic, cultural, and political perceptions among the news staff.[89] In other words, the news both influences and is influenced by the audience and

---

[83] *See* Fernando R. Laguarda, *Think of an Elephant? Tweeting as 'Framing' Executive Power*, 8 LEG. & POL'Y. BRIEF 32, 42-43 (2019).
[84] *Id.*
[85] *See* Britta C. Brugman & Christian Burgers, *Political Framing Across Disciplines: Evidence from 21st-Century Experiments*, 2018 RSCH. AND POL. 1, 1-2 (2018).
[86] *See* Darrius Hills, *Back to a White Future: White Religious Loss, Donald Trump, and the Problem of Belonging*, 16 BLACK THEOLOGY 38, 39, 46 (2018).
[87] *See* K. Jill Fleuriet & Mari Castellano, *Media, Place-Making, and Concept-Metaphors: The US-Mexico Border During the Rise of Donald Trump*, 42 MEDIA, CULTURE & SOC'Y 880, 890-91 (2020).
[88] *See* Angie Y. Chung et al., *COVID-19 and the Political Framing of China, Nationalism, and Borders in the U.S. and South Korean News Media*, 64 SOCIO. PERSP. 747, 752-53, 758 (2021). This trend arose from the widespread belief that China was responsible for the worldwide COVID-19 pandemic, regardless of whether it was purposeful or accidental.
[89] *See* Claes H. de Vreese, *News Framing: Theory and Typology*, 13 INFO. DESIGN J. 51, 55 (2005).

the country in which journalists reside, while political leaders also influence such editorial decision-making.[90]

There has been extensive professional research on how the American news media frames its home country's geopolitical conflicts with China. Attitudes toward that country are obviously relevant to the export/import trade policies discussed in this article because Chinese companies have received disproportionate attention during the supposed trade war. Researchers have detected a framing strategy among American news outlets that typically explains US-China relations as a zero-sum competition based on mistrust.[91] Such news coverage patterns in the American media, in which economic competition is framed as a conflict between enemy nations, is descended from coverage of true wars of military engagement in the 20th century, as opposed to peacetime coverage of mundane regulations and policymaking.[92] Such coverage frequently frames the disagreeing nations as "enemies" rather than "opponents," or as "adversaries" rather than "partners," [93] while the *war* in "trade war" is frequently emphasized.[94] Editorial viewpoints on purported conflicts in the race to develop new technologies have also been shown to influence news coverage, and therefore public opinion, of U.S.-China relations and the fortunes of the relevant high-tech companies.[95]

Specifically for U.S.-China relations, other researchers have found that this type of framing strategy in the American media can be traced to ancient perceptions among Westerners of themselves as civilized and rational while the Orient (the common term at the time) was perceived as backward and irrational, often to the point of imagining a good vs. evil dichotomy.[96] That dichotomy has its roots in the "Yellow Peril" of the 19th century, in which Asia was seen as a cultural threat to Western cultural values, followed by the "Red Peril" of the mid-20th century in

---

[90] *See* Dennis Nguyen & Erik Hekman, *A 'New Arms Race'? Framing China and the U.S.A. in A.I. News Reporting: A Comparative Analysis of the Washington Post and South China Morning Post*, 7 GLOB. MEDIA & CHINA 58, 60-61 (2022).
[91] *See* Peter Gries & Yiming Jing, *Are the US and China Fated to Fight? How Narratives of 'Power Transition' Shape Great Power War or Peace*, 32 CAMBRIDGE REV. INT'L. AFFAIRS 456, 460, 474 (2019).
[92] *See* Louisa Ha, Yang Yang, Rik Ray, Frankline Matanji, Peiqin Chen, Ke Guo, & Nan Lyu, *How US and Chinese Media Cover the US–China Trade Conflict: A Case Study of War and Peace Journalism Practice and the Foreign Policy Equilibrium Hypothesis*, 14 NEGOT. & CONFLICT MGMT. RSCH. 131, 133—34 (2021).
[93] *Id.* at 136.
[94] *Id.* at 145.
[95] *See* Nguyen & Hekman, *supra* note 90, at 63.
[96] Su-Mei Ooi & Gwen D'Arcangelis, *Framing China: Discourses of Othering in US News and Political Rhetoric*, 2 GLOB. MEDIA & CHINA 269, 270 (2017).

which Asia (and especially China) was seen as a vanguard of a worldwide Communist revolution.[97]

Longstanding American viewpoints on China have manifested themselves in geopolitical policy, from America's involvement in the Opium Wars of the mid-19th century to modern territorial tensions in the South China Sea.[98] The present article contends that this pattern can be seen in recent telecom-oriented export/import restrictions as well. The policymakers who enact those regulations are not immune to the effects of these framing patterns.[99]

IV. VAGUENESS AND POOR TRANSPARENCY IN EXPORT/IMPORT POLICY

When the American government first expressed concern about the possible threats posed by Chinese telecom firms, suspicions about the theft of American intellectual property and trade secrets were the first issue of investigation.[100] In fact, Huawei and ZTE have each been sued by American firms for patent infringement numerous times.[101] Chinese patent theft is estimated to cost American companies up to $600 billion every year.[102] In the years after those suspicions emerged, government investigations into the specific and esoteric matter of patent theft have morphed into less distinct and more dramatic political grandstanding about "national security." Granted, some commentators have noted that rampant intellectual property theft can have implications for national security, particularly regarding defense systems.[103]

But, beyond mundane patent disputes, "national security" is used in much looser ways for political impact. President Donald Trump's national security policy, and its associated regulatory documents, almost always mentioned China in particular, and typically framed the policy as a response to Chinese economic skullduggery, with the complex connection between economic competition and threats to national security taken as a given.[104] In fairness, this framing practice was merely an accelerated version of a strategy that had originated in the Obama

---

[97] *See id*. at 273.
[98] *See id*. at 271.
[99] *See* Gries & Jing, *supra* note 91, at 461.
[100] *See* Sullivan, *supra* note 19, at 330.
[101] *See id*. at 347.
[102] Sherisse Pham, *How Much Has the US Lost from China's IP Theft?*, CNN (Mar. 23, 2018, 5:35 AM), https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html.
[103] *See* Vilas Ramachandran, *A Regulatory Back Door: General Prohibition Ten and America's National Security*, 20 SANTA CLARA J. INT'L. L. 31, 34—35 (2022).
[104] *See* deLisle, *supra* note 81, at 66—67.

administration, during a period in which awareness of Chinese theft of American intellectual property (an economic misdeed) was growing.[105] Converting that esoteric concern into Trump's more exciting national security focus was a fairly easy rhetorical shift, especially because national security is both suitably emotional and wretchedly defined in American law.

The statutory meaning of "national security," despite the term's preponderance in export/import policy and many other areas of American law, is difficult to nail down. After World War II, "national security" expanded beyond fairly comprehensible military objectives into an amorphous conglomeration of law enforcement, terrorism, corruption, environmental protection, public health, economic strategy, and (most recently) export/import policy.[106] Efforts to refine the term to comprehensible dimensions has become a struggle of party politics, in which adversarial groups cite national security to advance their own causes.[107] The use, or overuse, of national security as a justification for any and all political projects exploded after the terrorist attacks of September 11, 2001, to the point of making the term nearly useless as a measure of political achievement, for either economics or security.[108]

The first appearance of the term "national security" in trade policy was in a 1975 executive order that established the Committee on Foreign Investment in the United States (CFIUS), which reviews the impact of foreign investments in American companies, though that order included no definition of the term.[109] The CFIUS currently operates under a statute stating that "[t]he term 'national security' shall be construed so as to include those issues relating to 'homeland security,' including its application to critical infrastructure," which in turn includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security."[110] This is the most distinct definition of the term to be found in the export/import regulatory regime, but whether all this terminology nails down the CFIUS's viewpoint on national security may be a moot point. The committee has often been

---

[105] *Id.* at 67.
[106] *See* J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020, 1034 (2020).
[107] *Id.* at 1034–35.
[108] *See id.* at 1047–50.
[109] *See* Exec. Order No. 11,858, 3 C.F.R. § 990 (1971–1975).
[110] This text is from a 1988 addendum, known as the Exon-Florio Amendment to the Defense Production Act. 50 U.S.C. §§ 4565(a)(1), (5). Various post-1975 provisions of that Act codify the CFIUS process of reviewing foreign investments.

accused of making its decisions via an unaccountable process that is incomprehensible and unreviewable for interested citizens.[111]

The phrase "national security" is used numerous times in the Export Administration Act of 1979, the statute from which modern restrictions flow.[112] That statute was renewed by several presidents, both Republican and Democrat, who cited its utility for ensuring national security.[113] Congress most recently used that justification in the Export Control Reform Act of 2018,[114] which was a precursor of the telecom-specific controls at the heart of the present article. That statute addresses "emerging and foundational technologies that . . . are essential to the national security of the United States," but with no definition of national security.[115] A related statute, the Foreign Investment and National Security Act of 2007, adds "critical infrastructure" and "critical technologies" with undefined applications for national security..[116]

Over time, those statutes have widened the focus of "national security" from short-term military threats to longer-term trends in innovation and supply chain management.[117] For export/import policy, ever-expanding ranges of industries and product categories are being lumped into threats to national security, and the associated statutes and regulations rarely attempt to define the term.[118] Section 15, Part 744 of the Code of Federal Regulations, which defines the Entity List and related export control rules, makes copious use of the phrase "national security or foreign policy interests of the United States," including in several sub-section titles, but with no precise definition of the term.[119] The Entity List itself is defined as consisting of parties "reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States."[120] Note the use of undefined signifiers like *reasonably* and *significant*. Also, that same block of text is typically copied into Department of Commerce documents as the only necessary justification

---

[111] Ioannis Kokkoris, *Assessment of National Security Concerns in the Acquisition of U.S. and U.K. Assets*, 12 J. NAT'L SEC. L. & POL'Y 349, 374 (2022).
[112] 50 U.S.C. § 2404; *see also* 50 U.S.C. §§ 2401–20.
[113] *See* Ramachandran, *supra* note 103, at 39–40.
[114] *See* 50 U.S.C. § 4811(8).
[115] 50 U.S.C. § 4817(a)(1). Recall from above that the term "critical infrastructure" also suffers from a vague regulatory definition; *see supra* note 53 and accompanying text.
[116] Foreign Investment and National Security Act of 2007, Pub. L. No. 110–49, 121 Stat. 246, §§ 2(a)(6)–2(a)(7).
[117] *See* Nathan Bush, *Chinese Antitrust in the Trade War: Casualty, Refugee, Profiteer, Peacemaker*, 84 ANTITRUST L.J. 209, 224 (2021).
[118] *See* Heath, *supra* note 106, at 1042.
[119] 15 C.F.R. § 744 (2022).
[120] 15 C.F.R. § 744.16 (2022).

for adding a company to the Entity List. Perhaps a clearer definition of national security can be inferred from the list of countries for which military-related exports are restricted: Belarus, Burma (Myanmar), Cambodia, China, Russia, and Venezuela;[121] while Iran, North Korea, and Syria are named due to various sanctions from the Department of Defense.[122] However, the Entity List includes purported national security threats from companies in many nations that are not currently involved in military disputes with the United States, including several allies like Austria and Belize.[123] Purported threats from those friendly places are usually due to rogue companies re-exporting products to America's enemies, but the regulatory documents are devoid of information on whether the allied nations are doing anything to stop such practices by their own firms, or if they are even expected to.[124]

The Trump administration, almost immediately after Trump took office in January 2017, added a new wrinkle by conflating national security with winning trade wars.[125] The administration soon adopted the mantra "economic security is national security."[126] While initially focusing his general trade policy on imports, which can cause deficits as American money exits the country, Trump later turned to export controls as well, in the belief that foreign purchasers of American products and services, particularly in the telecom sector, could infiltrate American industries and networks.[127] This has caused a conflation of economic and

---

[121] 15 C.F.R. § 744.21(a)(1) (2022). For Burma, that country's outdated name is used in the Department of Commerce regulations, but its current name Myanmar is used for actual companies in the Entity List.

[122] 15 C.F.R. §§ 744.19(a)–(b) (2022).

[123] 15 C.F.R. pt. 744 (Supp. 4 2022).

[124] For example, an Austrian subsidiary of Gulf Gate Spedition GmbH (headquartered in Dubai) is lumped in with several other international subsidiaries of the parent company for suspicion of trafficking American products through Taiwan and Hong Kong on their way to Iran. However, the regulatory document contains no information on whether the friendly nation of Austria suspects such practices, whether it is conducting any investigations of its own, or whether it contributed to the Department of Commerce decision in America. *See* Addition of Certain Persons and Removal of Certain Persons from the Entity List, 15 C.F.R. pt. 744 (2022).

The same pattern can be seen for Ecotherm-Cryo Limited of Belize, which was one of several companies lumped into a blanket accusation of providing equipment assisting Russia during its 2022 invasion of Ukraine. *See* Further Imposition of Sanctions Against Russia with the Addition of Certain Entities to the Entity List, 15 C.F.R. pt. 744 (2022).

[125] *See* Chad P. Bown, *Export Controls: America's Other National Security Threat*, 30 DUKE J. COMP. & INT'L. L. 283, 287 (2020).

[126] *See* Peter Navarro, *Why Economic Security Is National Security*, REAL CLEAR POLS. (Dec. 9, 2018), https://www.realclearpolitics.com/articles/2018/12/09/why_economic_security_is_national_security_138875.html.

[127] *See* Bown, *supra* note 125, at 289.

geopolitical objectives within U.S. trade policy, particularly toward China, with economic strategy becoming confused with defense strategy in possibly deleterious ways.[128] Research has shown that nations in a conflict that is framed in this fashion are likely to invoke threats to national security in order to bypass less exciting but more established regulatory processes.[129]

To further confuse the issue, human rights concerns were unexpectedly added to the Entity List in 2020, when the Department of Commerce listed various Chinese entities that were suspected of exploitation of the Uyghur ethnic group in the Xinjiang region.[130] This indicates further politicization of the Entity List and related regulations,[131] and a possible reaction to widespread media coverage of the plight of the Uyghurs,[132] as Democrats have pushed for more use of this export control technique against companies that sell their products to regimes that abuse human rights.[133] The Biden administration has actively added human rights concerns to its policies toward China, particularly suspicions of involvement by the nation's high-tech companies.[134]

The reasons for claiming that foreign firms are threats to national security are almost never cited in detail in the executive orders issued by presidents or in regulatory documents from the Department of Commerce or the Federal Communications Commission. Instead, vague political reasoning must often be gleaned from the associated press releases.[135] Regarding business with China in particular, national security rhetoric slowly emerged during the Obama administration but was amped up significantly during the Trump administration. This added increasingly expansive concerns about financial manipulation, military expansion, data surveillance, and telecommunications industry

---

[128] *See* Heath, *supra* note 106, at 1024.
[129] *Id.* at 1032.
[130] 15 C.F.R. pt. 744 (Supp. 4 2022).
[131] *See* Kokkoris, *supra* note 111, at 363.
[132] *See* James Griffiths, *From Cover-Up to Propaganda Blitz: China's Attempts to Control the Narrative on Xinjiang*, CNN (Apr. 17, 2021, 6:59 PM), https://www.cnn.com/2021/04/16/china/beijing-xinjiang-uyghurs-propaganda-intl-hnk-dst/index.html.
[133] *See* HOUSE COMM. ON OVERSIGHT & REFORM, 117ST CONG., MALONEY, WYDEN, SCHIFF, AND MEEKS LEAD HOUSE AND SENATE DEMOCRATS IN CALLING FOR MAGNITSKY ACT SANCTIONS AGAINST COMPANIES THAT ENABLE HUMAN RTS. ABUSES (Dec. 15, 2021), https://oversight.house.gov/news/press-releases/maloney-wyden-schiff-and-meeks-lead-house-and-senate-democrats-in-calling-for.
[134] *See* deLisle, *supra* note 81, at 72-73.
[135] *See* Kokkoris, *supra* note 111, at 366-67.

dominance to the catch-all term "national security."[136] This indicates a rising concern, if undeveloped, about the presence of Chinese firms in the American telecom marketplace, mixed with overuse of national security concerns to justify changes to trade policy.[137]

A plethora of statutes with inconsistent but equally vague definitions of national security, and oversight by many different agencies with their own definitions of the same, creates a non-transparent regime in which American watchdogs and listed firms are less able to review the effectiveness of export/import regulations in the telecom sector. Combined with inconsistent and inarticulate definitions of national security among the many agencies involved, there is no uniform method for enacting such restrictions or for the public to review the process. This also allows decisions to become politicized, and often with a retaliatory flavor.[138]

In a further twist, the Department of Commerce, when deciding that a foreign company should be added to the Entity List or subjected to other trade restrictions for national security reasons, is not required to provide that company or anyone else with an explanation, if that explanation would *also* endanger national security or if any of the relevant agency documents are classified,[139] thus creating a "catch-22" effect that can lead to non-transparent and politicized decision-making.[140] The Federal Communications Commission has added its own rule about withholding classified documents from citizen watchdogs and the companies that are denied subsidies under its own efforts to protect national security.[141] By definition, classified documents can never be released to citizens or journalists; this is often a valid concern for the government, but there is no way to tell if the decision to classify those documents is justified or legitimate in its own right, thus reducing transparency even further.[142]

---

[136] *Id.* at 369-71.
[137] *See Trump Blocks Broadcom's Bid for Qualcomm on Security Grounds*, BBC NEWS (Mar. 13, 2018), https://www.bbc.com/news/business-43380893.
[138] *See* Sullivan, *supra* note 19, at 325.
[139] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65321 (proposed Nov. 19, 2019) (to be codified at 15 C.F.R. § 7.104).
[140] *See* Burks, *supra* note 54, at 110-11.
[141] In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs Huawei Designation ZTE Designation, 34 FCC Rcd. 11423, at ¶ 41.
[142] *See* Benjamin W. Cramer, *Old Love for New Snoops: How Exemption 3 of the Freedom of Information Act Enables an Irrebuttable Presumption of Surveillance Secrecy*, 23 COMMC'N L. & POL'Y. 91, 99 (2018).

Trump's restrictions, particularly on Huawei and ZTE, have been retained and only slightly modified (with some more focus on personal data security) by the Biden administration,[143] with the new President stating that China is "the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system."[144] With so much telecom networking equipment coming from that country, this statement creates a conflict with Biden's goals of expanding broadband networks into underserved areas of the country.[145] Biden's multi-trillion-dollar infrastructure spending bills, introduced in 2021, placed special emphasis on extensive broadband network development;[146] such plans will require a lot of components that have now been restricted via the recent import regulations, and this dilemma seems to not have occurred to the Biden administration beforehand.

Some critics have claimed that recent governmental investigations into Chinese firms like Huawei and ZTE, and suspicions about their equipment in American telecom networks, is based on longstanding anti-Chinese rhetoric that frames the nation as a threat, but as of 2023 those investigations have failed to find a "smoking gun" of irrefutable evidence that the equipment is being used to funnel sensitive American data back to the Chinese government.[147] Thus, a corresponding "smoking gun" of

---

[143] *See* Exec. Order No. 14034, 40 Fed. Reg. 31423 (June 9, 2021).

[144] *See* THE WHITE HOUSE, INTERIM NATIONAL SECURITY STRATEGIC GUIDANCE 8 (Mar. 2021).

[145] *See* John Hendel, *Why Suspected Chinese Spy Gear Remains in America's Telecom Networks*, POLITICO (July 21, 2022, 4:30 AM), https://www.politico.com/news/2022/07/21/us-telecom-companies-huawei-00047045.

[146] *See* Michael Laris, *How the House Spending Bill Funds Additional Infrastructure*, WASH. POST (Nov. 19, 2021, 9:55 AM), https://www.washingtonpost.com/transportation/2021/11/19/infrastructure-biden-spending-bill/.

[147] In 2022, journalists uncovered evidence that ByteDance (the Chinese parent company of the popular TikTok social media application) had reprimanded some employees who violated company policies about accessing users' personal data. Such revelations have not yet fueled investigations by the U.S. government, and it should be noticed that these revelations concern the management of data that users supply to international networks voluntarily, as opposed to Chinese government theft of secured data as a national security offense.

See, e.g., Emily Baker-White, *Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China*, BUZZFEED (June 17, 2002), https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access; Drew Harwell, *TikTok's Chinese owner Fires Workers Who Gathered Data on Journalists*, WASH. POST (Dec. 22, 2022), https://www.washingtonpost.com/technology/2022/12/22/tiktoks-chinese-owner-fires-workers-who-gathered-data-journalists/.

widespread national security threats remains elusive as well. Subsequently, journalists have questioned if this xenophobic attitude prevents American officials from separating legitimate Chinese trade and investment from old-school espionage, and thus, national security.[148]

All of this leads to government documents that are not sufficiently informative for American watchdogs and listed firms. Documents announcing final decisions by the Department of Commerce or Federal Communications Commission to restrict exports/imports are readily available at U.S. government websites, and many are directly cited in this article. Such documents are usually thousands of words long, but with some crucial missing pieces. In short, they reveal the *what* of the decision but usually not the *why*. Supporting documents detailing the investigative and research processes that led to those ultimate decisions are not readily available, so the interested person must take the ultimate agency decision as a given. Per the themes of this article, this is not true transparency, and such practices could possibly be regarded as secrecy and obfuscation.

This pattern raises contradictions with American government transparency standards that may be ripe for litigation. For instance, the Administrative Procedure Act mandates that federal agencies must observe mandated decision-making processes, and includes rules for making the relevant documents available to the public.[149] Neither that statute nor its transparency requirements are mentioned in the federal regulations that govern the Entity List, or in President Trump's 2019 executive order, or in the statutes that instruct the FCC to maintain the newer Covered List of suspicious international telecom firms. This may be an honest oversight, but the practical result is that there is no mandated procedure for interested citizens or companies to find deliberative documents that influenced the ultimate decisions to restrict exports and imports.[150]

---

[148] *See* Katie Bo Lillis, *FBI Investigation Determined Chinese-Made Huawei Equipment Could Disrupt US Nuclear Arsenal Communications*, CNN (July 25, 2022, 4:12 PM), https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.

[149] *See* Administrative Procedure Act of 1946, 5 U.S.C. §§ 551-59.

[150] As a partial counterexample, the website for the Bureau of Industry and Security offers free access to official letters that were sent to individuals and companies that were charged for specific export violations. These documents typically offer evidence of regulatory or criminal transgressions. For example, in 2021, Princeton University was fined $54,000 for 37 incidents in which its scientific researchers shipped animal pathogens to researchers in other countries, which was a violation of export restrictions. *See* U.S. Dep't of Com., Bureau of Indus. and Sec., *Order Relating to Princeton University*, charging letter E2642, Feb. 1, 2021,

Meanwhile, the vague definition of "national security" in the regulations and statutes described herein causes another problem. Interested persons could possibly obtain obscure agency decision-making documents under the Freedom of Information Act (FOIA), but that statute includes an exemption that allows agencies to withhold any document deemed relevant for national security and they do not have to provide evidence on *why* it is relevant for national security.[151] That exemption is frequently abused by agencies that would like to keep certain documents secret.[152] As concluded by one legal researcher writing about the use of export/import restrictions during the Trump administration: "[i]f everything is about national security, nothing is about national security."[153]

And finally, the present article makes use of many *final* documents that are easily found online via Department of Commerce websites and the online version of the Federal Register, and the availability of these documents satisfies the requirements of a 1996 amendment to FOIA, known as eFOIA, that mandated online access for agency documents created after that year.[154] However, *decision-making* documents that informed those final decisions are typically unavailable through such channels, if they were ever recorded at all. In addition to unsupported claims of threats to national security, the lack of information on who arrived at those conclusions and how they arrived at those conclusions does further damage to the transparency of the process.

---

https://efoia.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=1287&Itemid=.

However, such documents apply to specific incidents in which charges were filed and either settled or sent through agency adjudication processes. Decision-making documents leading to wide export/import bans into the future for purposes of national security, which are the focus of the present article, cannot be found anywhere at the Department of Commerce website or linked to any of the final decision documents regarding the Entity List and related regulations as discussed herein.

[151] *See* Freedom of Information Act of 1966, 5 U.S.C. § 552(b)(1).

[152] *See, e.g.*, Martin E. Halstuk & Eric B. Easton, *Of Secrets and Spies: Strengthening the Public's Right to Know About the CIA*, 17 STAN. L. & POL'Y. REV. 353 (2006); Susan Nevelow Mart & Tom Ginsburg, *[Dis-]nforming the People's Discretion: Judicial Deference Under the National Security Exemption of the Freedom of Information Act*, 66 ADMIN. L. REV. 725 (2014); David B. McGinty, *The Statutory and Executive Development of the National Security Exemption to Disclosure Under the Freedom of Information Act: Past and Future*, 32 N. KY. L. REV. 67 (2005).

[153] *See* Bown, *supra* note 125, at 286.

[154] Electronic Freedom of Information Act Amendments of 1996, Pub. L. 104-231, 110 Stat. 3048.

V. THE RAMIFICATIONS OF EXPORT/IMPORT RESTRICTIONS IN TELECOMMUNICATIONS

Upon the issuance of President Trump's 2019 executive order banning American telecom firms from doing business with companies that purportedly pose national security risks, the Chinese Foreign Ministry urged the United States to "stop using the excuse of security issues to unreasonably suppress Chinese companies."[155] Huawei, which was banned from doing business in the United States by the Department of Commerce a few days later, argued that the restrictions "will not make the U.S. more secure or stronger; instead, this will only serve to limit the U.S. to inferior[,] yet more expensive alternatives, leaving the U.S. lagging behind in 5G deployment, and eventually harming the interests of U.S. companies and consumers."[156]

According to many experts, America needs Chinese telecom networking equipment. For instance, Huawei's 5G components are widely regarded as affordable and reliable, and they have been adopted worldwide, particularly in less developed regions that need inexpensive telecom infrastructure.[157] These advantages have been highlighted by the Pentagon, indicating that some parts of the U.S. government would like to continue using Huawei's components,[158] and those components have been adopted by many smaller American service providers, particularly those serving rural areas.[159] Policymakers in the European Union have noted that any risks apparently posed by Huawei equipment can be tackled via security protocols or contractual negotiations, rather than threats or restrictions.[160] Instead, the United States has taken a less-nuanced stance based on perceived national security threats but with little articulation on what exactly those threats may be, mixed in with economic goals related to gaining advantage in the U.S.-China trade war.[161]

---

[155] Chamberlain, *supra* note 62.
[156] Commerce Dept. Bans Huawei, *supra* note 66.
[157] *See* Opderbeck, *supra* note 60, at 166.
[158] *See* Kimberly A. Houser, *The Innovation Winter Is Coming: How the U.S.-China Trade War Endangers the World*, 57 SAN DIEGO L. REV. 549, 589-90 (2020).
[159] *See* Katie Mellinger, *TikTokers Caught in the Crossfire of the U.S.-China Technology War: Analyzing the History & Implications of Chinese Technology Bans on U.S. Domestic Expression and Access to Communications*, 11 WAKE FOREST J.L. & POL'Y. 689, 703-04 (2021).
[160] *See* Drew Hinshaw, *Allies Wary of U.S. Stance on Huawei and 5G*, WALL ST. J. (Apr. 9, 2020, 3:29 PM), https://www.wsj.com/articles/allies-wary-of-u-s-stance-on-huawei-and-5g-11586460582.
[161] *See* Russell Brandom, *Trump's Latest Explanation for the Huawei Ban Is Unacceptably Bad*, THE VERGE (May 23, 2019, 7:35 PM),

This gives the impression of political revenge against particular countries or companies rather than a coherent economic strategy.[162] Trump's executive order from 2019, which remains in effect, also allows the Department of Commerce to collect concerns about telecom-related national security threats from any private party that it deems credible.[163] This could lead to competitors tattling on each other, thus slowing down telecom network development for everyone. The inclusion of many different government agencies in the process can lead to mission creep as departments like Defense and Homeland Security meddle in telecom exports/imports to advance their own concerns about China or Russia.[164] Thus, a previously routine administrative process of assessing the export/import interests of American companies has been politicized to gain bargaining points in the trade war.[165] Even America's allies suspected that Trump's restrictions abused the "national security" frame for purposes of economic or political retaliation.[166] Those allies largely rebuffed Trump's efforts to push them into imposing their own restrictions against those firms.[167]

This has had an immediate impact on the Federal Communications Commission and its ability to foster advanced network development, which it is required to do by law.[168] When Trump issued his executive order, and when Commerce added Huawei and ZTE to the Entity List, the FCC adopted the administration's use of the national security frame and held a workshop in which various participants concluded that Huawei and ZTE equipment allows a hostile regime (China) to spy on American citizens and control the worldwide flow of information.[169] The commission next prohibited equipment from either company from being included in any telecom network development project that receives money from the Universal Service Fund,[170] because such funds should not be used to endanger national security, citing

---

https://www.theverge.com/2019/5/23/18637836/trump-huawei-ban-explanation-trade-deal-national-security-risk.

[162] *See* Burks, *supra* note 54, at 106.

[163] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65320-21 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7).

[164] *See* Burks, *supra* note 54, at 107-08.

[165] *See* Bown, *supra* note 125, at 286.

[166] *Id.* at 300.

[167] *See* Zhao Minghao, *US Perception of and Response to the Digital Silk Road*, 84 CHINA INT'L. STUD. 84, 93 (2020).

[168] Telecommunications Act of 1996, 47 U.S.C. § 706(a).

[169] *See* Opderbeck, *supra* note 60, at 171-72.

[170] *See* Brian Fung, *US Regulators Rule That China's Huawei and ZTE Threaten National Security*, CNN (Nov. 22, 2019, 12:07 PM), https://www.cnn.com/2019/11/22/tech/fcc-huawei-zte/index.html.

suspected company links to the Chinese government.[171] The commission added suspicions that those companies' telecom network equipment could collect personal data or inject malware and viruses into American networks.[172] These claims were supported with citations to the 2019 Department of Commerce document that added Huawei to the Entity List, which as previously described, mentions national security many times without defining it or presenting specific evidence that it had been threatened by those firms.[173]

American telecom service providers have noted the disconnect when an equipment ban is framed as an urgent national security solution, but on-the-ground replacement of network components is not given the same consideration.[174] After deciding that equipment from Huawei and ZTE should not be used in American telecom networks in 2019, the FCC mandated a "rip and replace" policy requiring network providers to remove such components from their networks and replace them with others from supposedly friendlier firms.[175] The offending components are not so easy to remove from an integrated telecom network, and can be found in many different locations around such a network, including inside subscribers' homes and under busy streets.[176] FCC funding for this laborious effort was not made available until late 2020.[177] After being ordered to remove offending equipment from their networks, American service providers have claimed costs of $5.6 billion to remove those components and replace them with new ones, and this assumes that non-threatening replacements will be easily available and in sufficient quantities. In June 2022 Congress proposed emergency funding to cover about two-thirds of those costs in the form of direct subsidies, with the rest to be covered by the FCC.[178]

---

[171] *See* Fed. Commc'ns Comm'n, *Protecting National Security Through FCC Programs*, Report and Order, WC Docket No. 18-89, 34 FCC Rcd. 11423 (Nov. 26, 2019), at ¶¶ 48-54.
[172] *See* Todd Shields, *Huawei and ZTE Targeted While Security Ban Advances at U.S. FCC*, BLOOMBERG (Apr. 17, 2018, 11:06 AM), https://www.bloomberg.com/news/articles/2018-04-17/huawei-zte-targeted-as-security-ban-advances-at-u-s-fcc#xj4y7vzkg.
[173] *See* Additions to the Entities List, 84 Fed. Reg. 22,961, 22,961–62 (May 21, 2019); 15 C.F.R. pt. 744 (Supp. 4 2022)
[174] *See* Hendel, *supra* note 145.
[175] In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs Huawei Designation ZTE Designation, 34 FCC Rcd. 11423, at ¶¶ 108-17.
[176] *See* Hendel, *supra* note 145.
[177] *Id.*
[178] *See* Joseph Marks, *A Plan to Strip Huawei from Rural Telecoms Is Still Short Billions,* WASH. POST (June 15, 2022, 7:36 AM),

Until those funds are in place, there are several possible ramifications for America's advanced telecom services. Some smaller (and especially rural) service providers will be unable to remove Huawei equipment for the time being; leaving their networks open to the suspected security risks; while other providers may be able to remove the Huawei equipment in the short term but will be unable to replace it rapidly, thus leaving their customers underserved.[179] There is another problem with existing Huawei or ZTE network equipment: if components that are currently in use malfunction or suffer wear and tear, they now cannot be easily replaced unless equivalents from approved firms can be found and integrated into the networks immediately. The recent regulations even prevent providers from calling Huawei or ZTE customer service when there are problems with currently installed components.[180] In fact, many of the 3G and 4G networks that still serve much of the United States contain networking equipment from Huawei and ZTE, and will continue to do so, until the unlikely advent of upgrades to 5G networks made up entirely of equipment from nations with which America is not engaged in trade wars.[181]

There is yet another way that these export/import restrictions can create negative impacts, and this time American high-tech firms will feel them. For example, Google could face a significant setback if it is unable to export its Android operating system to smartphones manufactured overseas by Huawei or ZTE.[182] Other American companies have been known to suffer sharp hits to their revenues, and stock valuations, if they are suddenly restricted from selling their products and services to Chinese customers in the world's largest marketplace.[183] Meanwhile, the recent export restrictions will have immediate effects on the U.S. economy. For instance, Huawei purchased $11 billion in equipment and services from American firms in the year before the company was placed on the Entity List—a sizeable amount of incoming money that was suddenly cut off by the export restrictions.[184] Restrictions on Huawei's

---

https://www.washingtonpost.com/politics/2022/06/15/plan-strip-huawei-rural-telecoms-is-still-short-billions/.

[179] *Id.*

[180] Hendel, *supra* note 145.

[181] *See* Houser, *supra* note 158, at 565.

[182] *See* Yang Jie & Dan Strumpf, *Who Needs Google's Android? Huawei Trademarks Its Own Smartphone OS*, WALL ST. J. (May 24, 2019, 6:19 AM), https://www.wsj.com/articles/who-needs-googles-android-huawei-trademarks-its-own-smartphone-os-11558693195.

[183] *See* Jay Greene, *In ZTE Battle, U.S. Suppliers Are Collateral Damage*, WALL ST. J. (Apr. 24, 2018, 5:30 AM), https://www.wsj.com/articles/in-zte-battle-u-s-suppliers-are-collateral-damage-1524562201.

[184] *See* Houser, *supra* note 158, at 584.

business have also resulted in significant layoffs of American workers at Huawei-affiliated facilities in the United States.[185]

And while export restrictions may result in an American firm's products remaining in the country rather than being sold to someone else, this is not a guarantee that the American marketplace can absorb the quantities that would have been exported. Thus, the benefits for national security are unlikely to outweigh the economic losses for American companies and consumers. Furthermore, restricting American exports can cause the items in question (or their technological equivalents) to become more expensive on the international market, thus hurting consumers and economies in all nations, including America and its allies.[186]

There is more bad news on the geopolitical front. Per Chinese law, companies are required to support government requests for espionage or the dissemination of propaganda. This is an offshoot of the country's history of Communist ideology, and the new breed of Chinese high-tech firms are not yet fully independent from government demands.[187] A 2021 investigation by the *Washington Post* revealed documents showing collaboration between Huawei and Chinese government agencies that conduct surveillance of the population,[188] and an investigation by the British Parliament the previous year found the same.[189] The company has long claimed that its relationship with the government is "no different" than that of any other private Chinese firm and it is unable to resist such demands.[190] It should also be noted that neither investigation uncovered evidence that the company's tactics inside China are repeated in other countries where its products are used.

Regardless, the close corporate/government ties in China mean that an attack (either rhetorical or economic) on a company is felt by the

---

[185] *See* Zak Doffman, *Huawei Blacklisting Is Forcing 'Extensive Layoffs' in U.S.*, FORBES (July 14, 2019, 2:20 AM), https://www.forbes.com/sites/zakdoffman/2019/07/14/huawei-blacklisting-now-forcing-extensive-layoffs-in-u-s-reports/?sh=5bcfa0fd67e9.
[186] *See* Bown, *supra* note 125, at 301.
[187] *See* Mellinger, *supra* note 159, at 696-97.
[188] *See* Eva Dou, *Documents Link Huawei to China's Surveillance Programs*, WASH. POST (Dec. 14, 2021, 4:00 AM), https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.
[189] *See* Gordon Corera, *Huawei: MPs Claim 'Clear Evidence of Collusion' with Chinese Communist Party*, BBC (Oct. 8, 2020), https://www.bbc.com/news/technology-54455112.
[190] *See* Li Tao, *Huawei Says Relationship with Chinese Government 'No Different' from Any Other Private Company in China*, S. CHINA MORNING POST (Dec. 26, 2019, 5:02 PM), https://www.scmp.com/tech/big-tech/article/3043558/huawei-says-relationship-chinese-government-no-different-any-other.

nation's leaders much quicker in China than in the United States. For Chinese companies like Huawei and ZTE, those firms are so closely tied to the Chinese regime that restricting them from doing business with or in the United States is likely to have serious geopolitical repercussions, as Premier Xi Jinping has been known to frame criticism of such companies as attacks on China itself.[191] This may result in poorly-considered retaliation, leading to a sense of burgeoning threats in the United States, which in turn leads to more retaliation and a cycle that ultimately benefits neither country.[192]

Export/import restrictions have thus emerged as a weapon in trade wars, but they are blunt and clumsy.[193] Overuse of such controls for political purposes can create an atmosphere of uncertainty in which America becomes a less attractive environment for research, development, and production by international firms. This can have direct economic effects if those activities are no longer performed on American soil, while other countries could take the lead in crucial emerging markets like 5G.[194] The development of 5G and future telecom technologies will require the two leading manufacturing nations—the United States and China—to admit their interdependence and to cooperate instead of engaging in short-term trade war tactics.[195]

Back-and-forth trade war restrictions are likely to increase tensions between the two nations, and they may no longer cooperate on mutually beneficial matters of bilateral trade. Thus, the restrictions achieve neither national security nor improvements to the balance of trade,[196] which is the apparent goal of recent statutes and regulations that tie those two concerns together. In telecommunications, the United States has a robust manufacturing sector for chips and coding, but the leading hardware manufacturers are in other countries, especially China.[197] While America was a leader in the development of 3G and 4G technologies, its newfound refusal to cooperate with China is likely to allow that nation to become a dominant force in 5G, with American firms that need components being relegated to navigating their own country's

---

[191] *See* Sullivan, *supra* note 19, at 348.
[192] *See* Biao Zhang, *The Perils of Hubris? A Tragic Reading of "'Thucydides' Trap'" and China-US Relations*, 24 J. CHINESE POL. SCI. 129, 139 (2019).
[193] *See* Bush, *supra* note 117, at 247.
[194] *See* Bown, *supra* note 125, at 294-95.
[195] *See* Houser, *supra* note 158, at 551-52.
[196] *Id.* at 592.
[197] *See* Brian Fung, *How China's Huawei Took the Lead over U.S. Companies in 5G Technology*, WASH. POST (Apr. 10, 2019, 4:01 PM), https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/.

export/import regulations plus whatever retaliatory sanctions China may enact. In the meantime, China (and possibly the European Union) may enjoy the opportunity to set 5G technical standards.[198]

Upon the advent of the Trump administration's trade war strategy against China, China instituted some of its own retaliatory restrictions on American products and services.[199] In fact, the two nations may be headed toward what political scientists call "the Thucydides Trap," in which adversarial leaders try to one-up each other with emotional accusations that drift away from political realism, to the point at which both nations are disadvantaged.[200] The Thucydides Trap also arises when an established power (in this case, the U.S.) perceives threatening competition from a rising upstart (China), while the upstart gains exaggerated self-confidence from watching the established power stumble. This leads to even more emotional battles at the expense of reasoned negotiations.[201] Non-transparent export/import restrictions, that are based on vague definitions and closed-door processes in deciding that something is a national security risk, are unlikely to lead to the reasoned decision-making that is necessary for avoiding the Thucydides Trap.

Geopolitical conflicts are not always played out on the battlefield, and may instead take the form of regulatory battles within economic and administrative institutions. The overuse of "national security" as a justification for such battles degrades those institutions and increases the likelihood of non-transparent economic warfare in which established regulations are flouted, the affected parties are unable to evaluate what happened, and obscure policymakers remain unaccountable.[202]

CONCLUSION

The transparency of governmental operations requires more than just final documents. Understanding such documents requires context that may be found in related documents that are not so easily available, or which describe deliberations that may have never been recorded in the

---

[198] *See* Houser, *supra* note 158, at 601-03.
[199] *Id.* at 560-61.
[200] *See* Gries & Jing, *supra* note 91, at 456-57. Thucydides (c. 460-400 BCE) was an ancient Greek historian who theorized that emotional one-upmanship among leaders rather than reasoned political negotiations caused the Peloponnesian War between Athens and Sparta.
[201] *See* Zhang, *supra* note 192, at 131.
[202] *See* Heath, *supra* note 106, at 1096.

first place.[203] While Department of Commerce documents explaining that a company was added to the Entity List are plentiful, this may only serve as a convenient diversion away from a true understanding of the decisions announced therein. Thus, the interested person's attention is monopolized by the big picture, with a loss of much-needed details.[204]

This article has examined two different manifestations of non-transparency: (1) confusing agency procedures, and (2) poorly defined terminology that is used to justify final agency decisions. The first is the result of a mishmash of government agencies taking part in discussions of whether a foreign firm and its products are a threat, while the final regulatory documents are issued by two different agencies. The regulatory documents from the Department of Commerce and the Federal Communications Commission, in which companies are forbidden from conducting exports or imports because of national security threats, give the strong impression of being based on suspicions rather than hard evidence. This may not be the intention, but documents that are released to the public on this matter typically say that the entity in question has been determined to be a threat to national security, with occasional citations to related documents in which some other inscrutable agency practically said the same thing. This is circular logic at best and the interested citizen is unable to find actual deliberations that led to the ultimate decision.

The second manifestation of non-transparency revolves around the elusive definition of "national security," and sometimes related terms like "critical infrastructure." The same circular logic is at play. National security is named in many American statutes and regulations, but they often cite each other on the term's definition, or assume that it needs no definition at all. It becomes difficult, if not impossible, for the interested person to know which agency applied which working definition of national security to determine a threat that is then announced by either the Department of Commerce or the Federal Communications Commission.

On the matter of foreign threats, it is no secret that most (possibly all) telecom networks and applications can collect personal information, trade secrets, government documents, and any other unsecured digitized data and store it in databases. And some of that sensitive material may

---

[203] *See* Benjamin W. Cramer, *What the Frack: How Weak Industrial Disclosure Rules Prevent Public Understanding of Chemical Practices and Toxic Politics*, 25 S. CAL. INTERDISC. L.J. 67, 89 (2016).

[204] *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 94-95 (2014).

very well be leaked or even sold to unsavory characters. The present author acknowledges that foreign telecom equipment probably is being used by foreign governments to collect data on Americans and would not be surprised if the long-elusive "smoking gun" comes to light. But, for purposes of international policy, the present author also believes that this is a red herring because the U.S. government spies on its own citizens with impunity and has openly roped American telecom firms into the effort.[205] The only difference is that American officials say it is for our own safety,[206] while foreign governments who do the same thing are condemned as malicious.[207] When American government officials condemn foreign countries and their firms for spying on us, with a burning need for retaliation, those officials should look in the mirror. The facial images they will see are already plastered across the Internet.

More specifically for the telecommunications matters discussed in this article, banning foreign firms like Huawei and ZTE from the American marketplace will have significant impacts on a national network that requires imported components for building much-needed infrastructure, and that marketplace also benefits from exports that keep American manufacturers solvent. Governmental restrictions that damage this marketplace should be fully transparent. Perhaps residents of an underserved rural community would like to know why they are still waiting for advanced networks to be built. Given current transparency patterns, they may be able to locate a document in which a company that supplies affordable and much-needed components has been banned from the marketplace because an agency decided the company is a threat to national security, but with no further information available on how that determination was reached or the nature of the threat to national security, much less what that ideal means in the first place.

One researcher who has studied Trump's 2019 executive order for a widespread ban of telecommunications equipment concluded that "[t]he U.S. President alone should not hold so much control over the

---

[205] *See* Julia Angwin, Jeff Larson, Charlie Savage & James Risen, *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, PROPUBLICA (Aug. 25, 2015), https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help.

[206] *See* Michael Chertoff, *NSA Surveillance Vital to Our Safety*, USA TODAY (Sept. 11, 2013, 9:00 AM), https://www.usatoday.com/story/opinion/2013/09/11/nsa-privacy-chertoff-911-column/2793063/.

[207] *See* Jake Maxwell Watts & Adam Pasick, *NSA Surveillance Just Gave China's President the Perfect Come-Back Line*, QUARTZ, (July 21, 2022), https://qz.com/92047/nsa-surveillance-just-gave-chinas-president-the-perfect-come-back-line/.

future shape of the Internet,"[208] and related telecom technologies like 5G. The President's influence arises from the questionable use of executive orders reacting to unarticulated emergencies, and a regulatory structure in which the President's underlings in the Executive Branch must follow suit. Those agencies then face few requirements for the transparency of their ultimate regulatory decisions.

For America to serve the networking needs of its own citizens, and to remain a world leader in telecom research and development, a spirit of cooperation with partner nations is sorely needed. Export/import restrictions, based on poorly defined national security concerns, are blunt solutions for a challenge that requires finesse. If America chooses to remain suspicious of foreign networking components, the European Union's stance on security protocols and multilateral negotiations, rather than bans and restrictions,[209] will bring current trade war tensions back into the mundane but manageable realm of established regulations. Otherwise, back-and-forth bickering between nations will accomplish nothing for underserved communities at home.

[208] *See* Opderbeck, *supra* note 60, at 221.
[209] *See* Hinshaw, *supra* note 160.