Ohio Northern University Law Review

Volume 47 | Issue 1 Article 4

Huawei, Internet Governance, and IEEPA Reform

David W. Opderbeck

Huawei, Internet Governance, and IEEPA Reform

DAVID W. OPDERBECK*

* Professor of Law, Seton Hall University Law School, and Director, Gibbons Institute of Law, Science & Technology. Thanks to Prof. Margaret Lewis for helpful comments on an earlier draft of this paper.

I. INTRODUCTION

Fifth generation cellular networks (5G) could revolutionize the Internet, including the Internet of Things.[1] The massive Chinese telecommunications company Huawei is a global leader in 5G telecommunications infrastructure.[2] Some security experts are concerned, not without reason, that Huawei 5G equipment will include backdoors or other security vulnerabilities that could facilitate China's national and corporate espionage activities or enable China to compromise the U.S. telecommunications system in the event of a dispute or war.[3]

But Huawei 5G components are competitively priced, functional, and are being widely adopted worldwide.[4] Huawei equipment is integral to the 5G build in the Middle East and in much of Africa.[5] The EU member states believe any serious risks from Huawei 5G equipment can be contained.[6] The UK initially established a policy that sought to limit Huawei products to a percentage of the network's periphery, although that policy has recently changed.[7]

The U.S. has taken a much more aggressive approach.[8] One prong of the U.S. approach involves criminal charges filed by the Justice Department.[9] On December 1, 2018, Huawei's CFO, Meng Wanzhou, who is also Huawei's founder's daughter, was arrested in Canada based on U.S. charges of financial fraud relating to evasion of U.S. sanctions against Iran by a U.S. Huawei subsidiary.[10] In January 2019, Huawei was indicted by the U.S. Justice

---

1. *See, e.g.*, Steve Ranger, *5G: What it Means for IoT*, ZDNET, https://www.zdnet.com/topic/5g-what-it-means-for-iot/ (last visited Dec. 20, 2020); Don Rosenberg, *How 5G Will Change the World*, WORLD ECONOMIC FORUM (Jan. 18, 2018), https://www.weforum.org/agenda/2018/01/the-world-is-about-to-become-even-more-interconnected-here-s-how/.

2. *See, e.g.*, Brian Fung, *How China's Huawei Took the Lead over U.S. Companies in 5G Technology*, WASH. POST (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/; Dan Strumpf, et al., *How Huawei Took Over the World*, WALL STREET JOURNAL (Dec. 25, 2018), https://www.wsj.com/articles/how-huawei-took-over-the-world-11545735603?mod=article_inline.

3. *See infra* Part IV.A.

4. FED. COMMC'NS COMM'N, SECURITY VULNERABILITIES WITHIN OUR COMMUNICATION NETWORKS: FIND IT, FIX IT, FUND IT (Nov. 21, 2019) [hereinafter FIND IT, FIX IT, FUND IT].

5. *See* John Calabrese, *The Huawei Wars and the 5G Revolution in the Gulf*, MIDDLE EAST INST. (July 30, 2019), https://www.mei.edu/publications/huawei-wars-and-5g-revolution-gulf.

6. *See, e.g.,* Drew Hinshaw, *Allies Wary of U.S. Stance on Huawei and 5G*, WALL STREET JOURNAL (Apr. 9, 2020).

7. *Id.*

8. *See e.g.,* Superseding Indictment, United States v. Huawei Technologies Co. Ltd., Cr. No. 18-457 (S-2) (AMD) (E.D.N.Y. Jan. 24, 2019), https://www.justice.gov/usao-edny/press-release/file/1125036/download.

9. *Id.*

10. *Id.*; *Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud*, DEP'T OF JUSTICE (Jan. 28, 2009), https://www.justice.gov/usao-edny/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged [hereinafter *Wanzhou Meng Charged*].

Department in the Western District of Washington State for alleged theft of trade secrets from American telecommunications company T-Mobile and related charges.[11] The Justice Department also indicted Huawei in January 2019 for alleged wire fraud, money laundering, and violations of International Emergency Economic Powers Act (IEEPA).[12]

A second prong of the U.S. approach involves emergency economic sanctions blocking trade in Huawei technology.[13] On May 15, 2019, President Trump issued an Executive Order authorizing regulations to ban transactions involving telecommunications technology that poses risks to U.S. national security.[14] In addition, effective May 16, 2019, Huawei and its affiliates were added to the Department of Commerce "Entity List," which bans exports, reexports, and transfers involving designated entities without a special license.[15] Regulations proposed by the Commerce Department and the FCC under the May 2019 Executive Order target Huawei equipment, including a proposed FCC policy to "rip and replace" existing Huawei equipment in some networks.[16]

The U.S. approach regarding trade in Huawei equipment is unique not only because of the policy choice, but also because it is based in a national emergency declaration by the President, following on the heels of criminal charges that seem thin if not dubious, rather than in the ordinary processes of the rule of law.[17] President Trump's May 2019 Executive Order was issued in the heat of a broader trade war between the U.S. and China.[18] The principal statutory authority for the Order was IEEPA, a statute passed in 1978 to modify a portion of the earlier Trading with the Enemy Act (TWEA).[19] Some observers suggest that President Trump's actions towards Huawei were

---

11. Indictment, United States v. Huawei Device Co. Ltd., Cr. No. 19-010 (RSM) (W.D. Wash. Jan. 16, 2019).

12. Superseding Indictment, *Huawei Technologies*, Cr. No. 18-457.

13. Addition of Entities to Entity List, 84 Fed. Reg. 22,961 (May 21, 2019).

14. Exec. Order No. 13,873, 3 C.F.R. § 317 (2020), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

15. 84 Fed. Reg. 22,961; Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, 84 Fed. Reg. 43,493 (Aug. 21, 2019) (to be codified at 15 C.F.R. § 744).

16. *Protecting National Security Through FCC Programs*, 34 FCC Rcd. 11423 (14) (2019).

17. Exec. Order No. 13,873.

18. *See, e.g.,* Russell Brandom, *Trump's Latest Explanation for the Huawei Ban is Unacceptably Bad*, VERGE (May 23, 2019), https://www.theverge.com/2019/5/23/18637836/trump-huawei-ban-explanation-trade-deal-national-security-risk; *Bargaining Chips: Donald Trump Gets Tough on Huawei*, ECONOMIST (May 16, 2019), http://www.economist.com/business/2019/05/16/donald-trump-gets-tough-on-huawei (authors for The Economist are anonymous) [hereinafter *Tough on Huawei*].

19. *See* Scott R. Anderson & Kathleen Claussen, *The Legal Authority Behind Trump's New Tariffs on Mexico*, LAWFARE (June 3, 2019).

unprecedented and an abuse of Executive power, in circumstances where free markets and the ordinary rule of law should operate.[20]

There are also broader concerns outside the China trade war context about the use of IEEPA as a general trade policy tool rather than as a limited emergency measure. On May 30, 2019, President Trump invoked IEEPA to justify a five percent tariff on goods imported from Mexico in an effort to force Mexican cooperation with the Trump Administration's efforts to control the border.[21] The use of IEEPA to justify these tariffs alarmed some political leaders in both parties who considered it an abuse, or at least an uncomfortable stretch, of the IEEPA authorities.[22]

The Mexico tariff threat was curtailed through an agreement reached between the U.S. and Mexico on June 7, 2019.[23] Although the Mexico tariff crisis was averted, the episode prompted calls to reform IEEPA.[24] Lawmakers and policy analysts from very different perspectives are concerned that IEEPA grants authorities that have been abused not only by President Trump, but also by every other President since the statute was signed into law by President Carter.[25]

In July and August 2019, similar bills were introduced by Democrats in the House and Senate that would prohibit the President from imposing duties and import quotas under IEEPA.[26] In November 2019, a group of moderate Republicans in the Senate introduced the "Assuring that Robust, Thorough, and Informed Congressional Leadership is Exercised Over National Emergencies (or ARTICLE ONE) Act."[27] In February 2020, Democrat Representative Ilhan Omar introduced a package of bills she titled the Pathway to PEACE (Progressive, Equitable, and Constructive Engagement)

---

20. *See, e.g.,* Brandom, *supra* note 19; *Tough on Huawei*, *supra* note 19; Charles Rollet, *Huawei Ban Means the End of Global Tech*, FOREIGN POLICY (May 17, 2019), https://foreignpolicy.com/2019/05/17/huawei-ban-means-the-end-of-global-tech/.

21. *Statement from the President Regarding Emergency Measures to Address the Border Crisis*, WHITE HOUSE (May 30, 2019), https://www.whitehouse.gov/briefings-statements/statement-president-regarding-emergency-measures-address-border-crisis/.

22. *See* Anderson & Claussen, *supra* note 20; Elizabeth Goitein, *What a President Can Do Under the International Emergency Economic Powers Act*, NPR: ALL THINGS CONSIDERED (May 31, 2019), https://www.npr.org/2019/05/31/728754901/what-a-president-can-do-under-the-international-emergency-economic-powers-act (noting that "This is an unprecedented use of IEEPA. IEEPA has not been used by any previous president to impose tariffs on goods from another country.").

23. *U.S.-Mexico Joint Declaration*, U.S. DEP'T OF STATE (June 7, 2019), https://www.state.gov/u-s-mexico-joint-declaration/.

24. To prohibit the imposition of duties on the importation of goods under the International Emergency Economic Powers Act, H.R. 3557, 116th Cong. (2019).

25. Anderson & Claussen, *supra* note 20; Goitein, *supra* note 23.

26. H.R. 3557; Trade Certainty Act of 2019, S. 2413, 116th Cong. (2019).

27. Assuring that Robust, Thorough, and Informed Congressional Leadership is Exercised Over National Emergencies Act, S. 764, 116th Cong. (2019).

that included the "Congressional Oversight of Sanctions Act" (COSA).[28] Each of these proposals would seek to impose some limits on Presidential authority under IEEPA.[29]

Although the Mexico tariff might have been the immediate prompt, the call for IEEPA reform also raises questions about President Trump's May 2019 Order regarding technology transactions and the subsequent addition of Huawei to the Entity List.[30] President Trump's May 2019 Order was not entirely unprecedented under IEEPA. IEEPA sanctions have often been applied by other Presidents against identified foreign individuals and in other circumstances that seem to fall far short of a national emergency.[31] Courts, including the Supreme Court, have interpreted the President's authority under the statute broadly, as have the administrative bodies charged with implementing that authority.[32]

The addition of Huawei to the Entity List was also not unprecedented– indeed, the Export Administration Regulations (EAR) under which the Entity List is promulgated date to 1996 and the Entity List names hundreds of individuals and companies in at least sixty-six countries, including over 175 listings (many naming multiple entities per listing) in China alone.[33] Not surprisingly, China, Hong Kong, Iran, Pakistan, Russia, Turkey, and the United Arab Emirates each account for multiple pages of listings.[34]

President Trump's Order does illustrate, however, that IEEPA should be amended for the Internet age. The powers delegated to the President under IEEPA are too broad and the decisions of the American President alone are unlikely to foster what should be the overarching policy goal–a robust, secure, open, globally-accessible Internet–particularly when the U.S. stands apart from decisions by other members of the global community about Internet infrastructure.[35] In relation to the Entity List, the question is

---

28. Congressional Oversight of Sanctions Act, H.R. 5879, 116th Cong. (2020); *Rep. Omar Introduces 'Pathway to PEACE,' A Bold Foreign Policy Vision for the United States of America*, HOUSE OF REPRESENTATIVES: ILHAN OMAR (Feb. 12, 2020), https://omar.house.gov/media/press-releases/rep-omar-introduces-pathway-peace-bold-foreign-policy-vision-united-states [hereinafter *Pathway to PEACE*].

29. H.R. 3557; S. 2413; *Pathway to PEACE*, *supra* note 29.

30. *See* Exec. Order No. 13,873.

31. *See e.g.,* CHRISTOPHER A. CASEY, ET AL., CONG. RESEARCH SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE (2020).

32. *See* Anderson & Claussen, *supra* note 20.

33. *See* 15 C.F.R. §§ 730-774 (1996-2020); *see also* 15 C.F.R. § 744.11 (2009); *Supplement No. 4 to Part 744 – ENTITY LIST,* BUREAU OF INDUST. & COMMERCE (Sept. 22, 2020), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file; *CBC FAQs - 2. What is the background and purpose of the Entity List?*, BUREAU OF INDUST. & COMMERCE, https://www.bis.doc.gov/index.php/cbc-faqs/faq/282-2-what-is-the-background-and-purpose-of-the-entity-list (last visited Dec. 20, 2020).

34. *Id.*

35. Rollet, *supra* note 21.

compounded because IEEPA is one of the statutory vectors through which an individual or company can be placed on the List.[36] Indeed, a recent amendment to U.S. export control laws, the Export Control Reform Act of 2018 (ECRA), appears to have significantly broadened the President's ability to restrict information technology transactions, including through Entity List designations, under IEEPA.[37]

Although there are bipartisan proposals in Congress to amend IEEPA, there are also bipartisan proposals to exclude Huawei form U.S. markets apart from IEEPA.[38] These proposals are blunt instruments that would only compound the problem Huawei's influence has over the global Internet backbone. The U.S. should construct a more robust policy framework, operating within the ordinary rule of law rather than as an emergency measure, to protect the security and reliability of U.S. Internet infrastructure and to position the U.S. as a leader in a global approach to Internet infrastructure governance.

Part II of this Article describes President Trump's May 2019 Order and proposed regulations published pursuant to the Order by the FCC and the Commerce Department.[39] Part III discusses IEEPA as a source of authority for President Trump's order based on the statutory text, legislative history, and subsequent interpretation, including the relationship between IEEPA and export control regulation.[40] Part IV discusses recent proposals in Congress and offers some alternative proposals for IEEPA reform against the broader policy goals of U.S. national security and global Internet governance.[41] Part V concludes.[42]

II. THE "HUAWEI" ORDER AND PROPOSED REGULATIONS

A. The Executive Order

In his May 2019 Executive Order, President Trump found that:

> [T]he unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and

36. 84 F.R. 22961.
37. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §§ 1741-1768, 132 Stat. 1636, 465-66, 485 (2019).
38. *See infra* Part IV.B.1.
39. *See infra* Part II.
40. *See infra* Part III.
41. *See infra* Part IV.
42. *See infra* Part V.

> 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.[43]

The Order authorizes various executive departments and agencies to issue implementing regulations against transactions that involve "information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" where the transaction

> (A) poses an 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;
>
> (B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
>
> (C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.[44]

The Order cites as sources of authority the International Economic Powers Act, the National Emergencies Act, and the general delegation statute.[45]

B. FCC Regulations and Proposed Regulations: Restricting Use of the USF and "Rip and Replace"

The FCC has taken steps to implement President Trump's May 2019 Order.[46] An FCC workshop on "Security Vulnerabilities in Our Communications Networks" was held at the FCC on June 27, 2019.[47] The Report of that workshop stated that "Huawei can be seen as an instrumentality of Chinese government to dominate global communications equipment markets and control the global flow of information."[48] The Workshop Report suggested that Huawei equipment could be used by China to access personal data of American citizens, degrade service during a crisis, and as a launch

43. Exec. Order No. 13,873.
44. *Id.*
45. 50 U.S.C. § 1701 (1977); 50 U.S.C. § 1601 (1976); 3 U.S.C. § 301 (1976).
46. *See generally* FIND IT, FIX IT, FUND IT, *supra* note 4.
47. *Id.* at 1.
48. *Id.* at 4.

point for cyber-attacks.[49] The Workshop noted a threat not only from the prospective use of 5G equipment supplied by Huawei and ZTE, another Chinese technology firm, but also from existing 3G and 4G equipment manufactured by these entities that already comprises part of U.S. cellular telecommunications networks.[50]

On November 26, 2019, the FCC issued a rule pursuant to the May 2019 Executive Order and other authorities concerning the use of the FCC Universal Service Fund (USF).[51] Under the Telecommunications Act of 1996, the USF is established through a tax on telecommunication service providers and is used to support the provision of telecommunications services in low income and high cost service areas, in schools and libraries, and among rural health care providers.[52] The FCC's Rule designates Huawei and ZTE as covered companies and prohibits the use of USF support funds to purchase equipment or services from those companies.[53] The FCC found that "Huawei's ties to the Chinese government and military apparatus, along with Chinese laws obligating them to cooperate with any request by the Chinese government to use or access their system, pose a threat to the security of communications networks and the communications supply chain."[54] The FCC also found that "[a]s with Huawei, ZTE has close ties to the Chinese military apparatus, having originated from the Ministry of Aerospace, a government agency."[55]

In addition to its Rule on the use of USF, the FCC simultaneously issued a further notice of proposed rulemaking that would require any telecommunications carriers that receive USF to remove and replace existing Huawei and ZTE equipment.[56] The FCC sought comment on how broad the removal and replacement obligation should extend, the timetable for removal and replacement, and possible reimbursement for removal and replacement costs.[57] This "rip and replace" order might cost one billion dollars to

49. *Id.*

50. *Id.* at 1-2.

51. *Protecting National Security Through FCC Programs*, 34 FCC Rcd. 11423 (14) (2019). The FCC stated that no further notice or comment was required for this Rule because of a prior Notice of Proposed Rulemaking issued by the FCC on April 18, 2018, titled "Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs." *See FCC Proposes to Protect National Security Through FCC Programs*, 33 FCC Rcd. 4058 (6) (2018), https://www.fcc.gov/document/fcc-proposes-protect-national-security-through-fcc-programs-0.

52. *See Universal Service Fund,* FED. COMMC'N COMM'N (Dec. 30, 2019), https://www.fcc.gov/consumers/guides/universal-service-support-mechanisms.

53. *Protecting National Security Through FCC Programs*, 34 FCC Rcd. 11423, 11424, 11433.

54. *Id.* at 11442.

55. *Id.* at 11447.

56. *Id.* at 11470.

57. *Id.* at 11478-11481.

implement.[58] Proposed bills in Congress (all proposed before the COVID-19 crisis) would have allocated $700 million to one billion in federal funds to support the rip and replace effort.[59]

C. Department of Commerce Proposed Regulations

On November 27, 2019, the U.S. Department of Commerce issued a notice of proposed rulemaking pursuant to President Trump's May 2019 Executive Order.[60] If adopted, this Rule would empower the Secretary of the Department of Commerce to evaluate any transaction that would fall within the Executive Order.[61] The Department of Commerce would reach a preliminary determination about the transaction, which the parties to the transaction could contest within thirty days of the preliminary determination.[62] Within thirty days after receiving any opposition, the Department of Commerce would issue a final determination concerning whether the proposed transaction is prohibited, permitted, or permitted with risk-mitigation measures.[63] The Rule would also include an emergency provision that would allow the Secretary of the Department of Commerce to make a summary determination, without any opportunity for opposition, "when public harm is likely to occur if the procedures are followed or national security interests require it."[64] The public comment period on these proposed rules closed on January 10, 2020.[65]

III. IEEPA AS AUTHORITY FOR PRESIDENT TRUMP'S "HUAWEI" ORDER

Many observers suggest that President Trump's May 2019 Order represents an unprecedented use of the powers delegated under IEEPA.[66] They argue that President Trump's invocation of IEEPA against specific Chinese companies during a trade war between the U.S. and China suggests the statutory authorities are being deployed for purposes beyond the "unusual

58. *See* Lily Hay Newman, *The FCC's Push to Purge Huawei from US Networks*, WIRED (Dec. 10, 2019), https://www.wired.com/story/fcc-rip-replace-huawei-zte/.

59. *See* Secure and Trusted Communications Networks Act of 2019, H.R. 4459, 116th Cong. (2019); United States 5G Leadership Act of 2019, S. 1625, 116th Cong. (2019); Linda Hardesty, *House Bill Asks for $1B to Rip and Replace Huawei Equipment*, FIERCE WIRELESS (Sept. 24, 2019), https://www.fiercewireless.com/regulatory/house-bill-asks-for-1b-to-rip-and-replace-huawei-equipment.

60. Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65,316 (proposed Nov. 27, 2019).

61. *Id.* at § 7.7.

62. *Id.* at § 7.103.

63. *Id.*

64. *Id.* at § 7.104.

65. *See* Securing the Information and Communications Technology and Services Supply Chain, 84 FR 70445 (proposed Dec. 23, 2019) (extending the comment period).

66. *See* Calabrese, *supra* note 5.

and extraordinary threat" trigger in the statute.[67] There are other tools, they argue, that empower, and limit, a President's ability to construct foreign trade policy, including the perceived problem of a negative balance of trade, which should be invoked in the ordinary course of lawmaking, not as emergency measures.[68]

As a textualist argument, based only on the plain language of the statute, this criticism seems to have merit.[69] Other elements of the statutory language, however, complicate the text. The most basic question left unresolved in the text itself is who decides what comprises an "unusual and extraordinary threat" instead of a "usual and ordinary" one. Beyond a limited kind of textualism, IEEPA's history, including its legislative history prior to adoption, the history of amendments to the original text, and the subsequent history of interpretation both by the Executive branch and by the courts, suggest President Trump's actions regarding Huawei are within the authority granted by the statute.[70]

A. IEEPA's Text

IEEPA was signed into law by President Carter on December 28, 1977.[71] It provides authorities that the President may exercise "to deal with any unusual and extraordinary threat, which has its source in whole or in substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat."[72] After stating this purpose, the statutory text immediately reiterates that "[t]he authorities granted to the President by . . . this title may only be exercised to deal with an unusual and extraordinary threat with respect to which a national emergency has been declared for purposes of this chapter and may not be exercised for any other purpose."[73]

The specific authorities granted to the President include the power to prohibit importation, exportation, or other transactions "involving any property in which any foreign country or a national thereof has any interest by any person, or with any property, subject to the jurisdiction of the United

67. Goitein, *supra* note 23 (noting that "This is an unprecedented use of IEEPA. IEEPA has not been used by any previous president to impose tariffs on goods from another country.").

68. *See generally*, Paul Hubschman Aloe, *Justiciability and the Limits of Presidential Foreign Policy Power*, 11 HOF. L. REV. 517 (1982).

69. *See generally,* Stephen M. Durden, *Plain Language Textualism: Some Personal Predilections are More Equal Than Others*, 26 QUINNIPIAC L. REV. 337 (2008).

70. Anderson & Claussen, *supra* note 20.

71. 50 U.S.C. § 1701.

72. *Id.*

73. *Id.* § (b).

States."[74] In addition to the emergency requirement, there are two limitations in the statute that could be relevant to the Huawei Order: the President is not given authority "to regulate or prohibit, directly or indirectly"

> (1) Any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value;
>
> . . . .
>
> (3) The importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. . . .[75]

There is an exception to this third limitation:

> The exports exempted from regulation or prohibition by this paragraph do not include those which are otherwise controlled for export under section 4604 of this title, or under section 4605 of this title to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by chapter 37 of title 18.[76]

The export controls mentioned in this section were repealed and replaced by the Export Control Reform Act of 2018 discussed in subpart III.E. below.[77]

IEEPA references the National Emergencies Act (NEA), which also was signed into law by President Carter.[78] The NEA states that, "[w]ith respect to Acts of Congress authorizing the exercise, during the period of a national emergency, of any special or extraordinary power, the President is authorized to declare such national emergency."[79] Under Section 202 of the (NEA), "[a]ny national emergency declared by the President in accordance with this subchapter shall terminate if . . . there is enacted into law a joint resolution terminating the emergency . . . ."[80] The NEA also states that any national emergency declared by the President under the NEA automatically terminates

74. *Id.* § 1702(a) (2004).
75. *Id.* §§ (b)(1), (3).
76. 50 U.S.C. § 1702(b)(3).
77. *See infra* Part III.E.
78. 50 U.S.C. § 1621 (1976).
79. *Id.* § (a).
80. *Id.* § 1622 (1985)

on its anniversary date unless the President provides notice within ninety days of the anniversary date that the emergency will continue in effect.[81] Under the NEA, the President must make periodic expense and other reports to Congress.[82]

IEEPA states that, even if the national emergency declaration is terminated under NEA or authorities exercised under IEEPA are otherwise terminated, the President may continue to prohibit transactions involving property in which a foreign country or a national thereof has any interest, "if the President determines that the continuation of such prohibition with respect to that property is necessary on account of claims involving such country or its nationals."[83] However, IEEPA also states that Congress can specifically include the termination of IEEPA authorities in an NEA concurrent resolution terminating a state of emergency.[84] Under IEEPA, the President must consult with Congress "in every possible instance" before invoking IEEPA and must provide a report to Congress that includes an explanation "why the President believes [the] circumstances constitute an unusual and extraordinary threat," which must be supplemented every six months.[85]

The NEA does not define what might comprise a "national emergency" and IEEPA does not specify what might comprise an "unusual and extraordinary threat" to the national security, foreign policy, or economy of the United States as to which a national emergency might be declared.[86] Taken in their ordinary sense, the words "emergency" and "unusual and extraordinary" seem to require something more than typical threats to the United States' national security, foreign policy, or economy.[87] The notion that some threats might be "unusual and extraordinary" suggests that there will exist other threats that are "usual" and "ordinary."[88] The mere presence of a threat, therefore, should not satisfy the statute.

Both the NEA and IEEPA, however, delegate the decision whether to declare a national emergency to the President, with the requirement only that the President report his or her decision to Congress.[89] Unless these statutes run afoul of the non-delegation doctrine–in which case they are fundamentally Constitutionally flawed–it appears that there is no textual

81. *Id.* (d).
82. *Id.* § 1641(c) (1976).
83. 50 U.S.C. §§ 1706(a)(1), (2) (1977).
84. *Id.* § (b).
85. *Id.* § (a), (b)(2) (1977).
86. *Id.* § 1621; *id.* § 1701.
87. *Emergency*, WEBSTER'S NEW WORLD DICTIONARY (2nd ed. 1982); *Unusual*, *id.*; *Extraordinary*, *id.*
88. *Unusual*, *id.*; *Extraordinary*, *id.*
89. 50 U.S.C. § 1621*; id.* § 1701.

ground on which any emergency declaration by a President could be subject to challenge.[90]

Although the requirement of an emergency declaration might rest in the President's discretion, the limitations in IEEPA relating to communications, information, and informational materials could bear on the Huawei Order's validity.[91] In the broadest sense, the Huawei Order reflects a debate about the future of Internet governance.[92] 5G technology will revolutionize the Internet, including the Internet of Things.[93] The Internet's traditional ethos is that the network is agnostic about hardware.[94] The Internet's beating heart are the code protocols that allow information to flow seamlessly across widely differing kinds of hardware.[95] The code protocols are kept open, and the market supplies hardware that works with the protocols.[96] Governments do not control either the code or the hardware infrastructure, because control leads to surveillance and censorship.[97]

The actual story of the Internet's hardware layer, of course, has always been more complicated than this libertarian folk tale. Some of the core Internet hardware infrastructure was originally built by governments, not least by the U.S. government.[98] Internet backbone infrastructure, even when privately constructed and owned, is often heavily subsidized by government grants, tax breaks, and license concessions.[99] In some other countries, such as China and Iran, government control of Internet infrastructure is a key part of a pervasive censorship program.[100]

In this context, an Order from an American President forbidding the use of Internet infrastructure equipment manufactured by one of the largest manufacturers of such equipment is a major change in U.S. policy and a

---

90. For a discussion of the non-delegation doctrine, *see infra* Part III.D.2.

91. Exec. Order No. 13,873.

92. *Id.*

93. *See, e.g.*, Rosenberg, *supra* note 1.

94. *See, e.g.*, Richard S. Whitt, *Formulating a New Public Policy Framework Based on the Network Layers Model,* in OPEN ARCHITECTURE AS COMMUNICATIONS POLICY 366 (Mark N. Cooper, ed., 2004) [hereinafter OPEN ARCHITECTURE].

95. *See, e.g.*, Robert Kahn & Vinton G. Cerf, *What is the Internet (And What Makes it Work)*, in OPEN ARCHITECTURE, *supra* note 95, at 18.

96. *Id.*

97. *Id.* at 26.

98. *See History and Evolution of Internet Backbones & Interconnection*, CYBERTELECOM (Oct. 12, 2019, 8:54 P.M.), http://www.cybertelecom.org/broadband/backbone3.htm.

99. *See, e.g., Broadband in the EU Member States: Despite Progress, Not all the Europe 2020 Targets Will be Met*, EUROPEAN COURT OF AUDITORS (2018), https://www.eca.europa.eu/Lists/ECADocuments/SR18_12/SR_BROADB AND_EN.pdf (noting that, to support its broadband objectives, "the EU has implemented a series of policy and regulatory measures and has made some 15 billion euro available to Member States in the period 2014-2020, through a variety of funding sources and types, including 5.6 billion euro in loans from the European Investment Bank (EIB).").

100. *See generally*, *Freedom on the Net*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net (last visited Dec. 20, 2020).

significant development in Internet governance.[101] This action at least "indirectly" regulates communications and the exchange of "information" and "information materials."[102] Surely IEEPA is not a blank check for the President to control the Internet. Further, the equipment at issue is not comprised only of dumb cables and antennas. The equipment includes computer code, which should fall under the statutory language of "information and communications technology or services" [103]

Although this line of argument is appealing, and although the radios, antennas, routers, multiplexers and other hardware that make up 5G infrastructure are embedded with computer code, they do not seem directly analogous to the "publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds" mentioned in the statute.[104] Further, as discussed in Parts III.D. and E. below, the courts, the Executive branch, and Congress have each assumed, with varying degrees of vigor, that IEEPA's reach over technology infrastructure is broad.[105] The textual conclusion that President Trump's May 2019 Order satisfies IEEPA's plain language is supported by the legislative history and by subsequent judicial interpretation and Executive practice.[106]

B. Legislative History: IEEP and TWEA

IEEPA replaced the Trading With the Enemy Act (TWEA), which was passed in 1917 as the U.S entered the First World War.[107] TWEA authorized the Executive to impose tariffs on goods and services produced by entities in states designated as enemies of the U.S. or to prohibit transactions with such entities.[108] IEEPA was Congress' response to extensive invocations of Presidential authority under the TWEA and an effort to coordinate the President's economic emergency powers with the then-recently passed National Emergencies Act of 1977.[109]

The key provision of TWEA for our purposes was Section 5(b), which authorized the President, "[d]uring the time of war," to regulate bank credit transactions and "the importing, exporting, hoarding, melting, or earmarking of gold or silver coin or bullion, currency, or securities," and to prohibit or

101. *See*, Exec. Order No. 13,873.
102. *Id.*
103. *Id.*
104. 50 U.S.C. § 1702(b)(3).
105. *See infra* Part III.D-E.
106. *See infra* discussion, Part III.B.
107. CASEY, *supra* note 32.
108. *Id.*
109. *See* S. REP. NO. 95-466, at 1 (1977).

otherwise regulate transactions involving "any property in which any foreign country or a national thereof has any interest."[110] Although TWEA was passed specifically in connection with World War I, it was also envisioned as a set of authorities for subsequent wars.[111] As originally enacted Section 5(b) gave the President broad powers relating to property relating to any foreign country or national–not just those with which the U.S. was at war–but it limited these powers to wartime.[112]

In 1933, during the Great Depression, President Franklin D. Roosevelt invoked Section 5(b) of TWEA to declare a banking holiday.[113] This was an effort to prevent a panic and to control the export of gold.[114] President Roosevelt issued five emergency Executive Orders under this provision between 1933-1934 under Section 5(b).[115] The United States was not at war as required to invoke TWEA, but in 1934 Congress ratified President Roosevelt's actions by passing the Emergency Banking Act.[116]

The 1934 Emergency Banking Act amended Section 5(b) of TWEA to state that "[d]uring time of war or during any other period of national emergency declared by the President," the President may regulate foreign banking transactions and export, hoarding, melting, or earmarking of gold or silver coin or bullion or currency by any person subject to U.S. jurisdiction.[117] Statements in the legislative history reflect the sense of urgency that accompanied this amendment. For example, Sen. Tom Connally, a Texas Democrat, stated that:

> [I]n time of peace we have perhaps never been called upon to vest such transcendent powers in the Executive as are provided for in this bill. . . . [The Great Depression] is an emergency which can be adequately dealt with only by the strong arm of Executive power, and therefore I expect to vote for the bill, though it contains grants of powers which I never before thought I would approve in time of peace.[118]

President Roosevelt invoked Section 5(b), as amended by the Emergency Banking Act, once again as Europe descended into World War II, to protect assets of residents of Norway and Denmark residing in the United States

110. 50 U.S.C. app. § 5(b)(1)(A)-(B) (1917).
111. 120 CONG. REC. 34,013 (1974); CASEY, *supra* note 32, at 8.
112. 50 U.S.C. app. § 5(b)(1)(A)-(B).
113. 120 CONG. REC. 34,013.
114. *Id.*
115. *Id.* at 34016.
116. *Id.*
117. Emergency Banking Act, Pub. L. No. 73-1, 48 Stat. 1 (1933).
118. 120 CONG. REC. 34,016.

when Germany invaded those countries in April 1940.[119] That Order did not declare a state of emergency.[120] However, in September 1939, President Roosevelt had declared a national emergency in a proclamation stating the United States' neutrality in the European war.[121] Moreover, on May 7, 1940, Congress passed a resolution stating that President Roosevelt's April 1940 action was a proper exercise of Section 5(b).[122]

President Roosevelt subsequently issued additional Executive Orders under Section 5(b) relating to Germany, Japan, and Italy, as the U.S. entered World War II.[123] The Executive Orders relating to World War II were superseded after the War as the U.S. embarked on the Marshall Plan to rebuild Europe.[124]

Although the crises faced by President Roosevelt in the 1930's and 1940's–the Great Depression and World War II–had subsided, TWEA, as amended during the 1930's banking crisis, allowed the President to refer to any existing declared state of emergency to implement economic restrictions, even if the restricted transactions had nothing to do with the declared emergency.[125] By 1977, there were four declarations of emergency still in effect that had provided a basis for authorities invoked under TWEA: (1) the 1933 declaration about the banking crisis by President Roosevelt; (2) a 1950 declaration by President Truman about the Korean conflict; (3) a 1970 declaration by President Nixon concerning a Post Office strike; and (4) a 1971 declaration by President Nixon concerning currency restrictions and foreign trade.[126]

One of President Truman's actions relating to the Korean War, of course–his seizure of the steel mills during the 1951 steel workers' strike–led to the famous *Youngstown Sheet & Tube Co. v. Sawyer*[127] case, a touchstone for any discussion of executive power.[128] President Truman did not invoke TWEA in relation to the steel seizure or otherwise during the Korean crisis, but the national emergency declared by President Truman during the Korean crisis was still technically in effect in 1968, when President Johnson imposed foreign direct investment controls on U.S. investors under section 5(b) of TWEA.[129] Although this Order from President Johnson was signed during

119. *Id.*
120. *Id.*
121. *Id.*
122. 54 Stat. 179 (1940).
123. 120 CONG. REC. 34,017.
124. *See, The Marshall Plan*, THE GEORGE C. MARSHALL FOUNDATION, https://www.marshallfoundation.org/marshall/the-marshall-plan/ (last visited Dec. 20, 2020).
125. Trading With the Enemy Act Reform Legislation, 120 CONG. REC. 22,473 (1977).
126. CASEY, *supra* note 32.
127. 343 U.S. 579 (1952).
128. *Id.* at 582.
129. Exec. Order No. 11,387, 33 Fed. Reg. 47 (1968).

the Vietnam conflict, it more broadly addressed a rise in the U.S. balance-of-payments deficit, which related only tangentially to the Vietnam War and not at all to the Korean conflict.[130]

President Nixon's currency restrictions and tariffs in 1971 also represented an effort to address the U.S. balance-of-trade deficit in the face of increased competition from Europe and Japan, growing inflation, and stagnant economic growth.[131] These actions ended the convertibility of dollars to gold, thereby abruptly transitioning the U.S. dollar to a fiat currency and effectively dissolving the Post-WWII Bretton Woods Agreement.[132] President Nixon also imposed tariffs on foreign imports.[133] None of these actions directly invoked section 5(b) of TWEA, but that provision was raised in defense of a legal challenge to the import tariffs by Yoshida International, a Japanese zipper manufacturer.[134] In *United States v. Yoshida International, Inc.*,[135] the Court of Customs and Patent Appeals upheld President Nixon's actions.[136] The court noted that "the express delegation in s 5(b) of the TWEA is broad indeed . . . . It appears incontestable that s 5(b) does in fact delegate to the President, for use during war or during national emergency only, the power to 'regulate importation.' . . . The delegation in s 5(b) is broad and extensive . . . ."[137]

After the Vietnam War Congress passed a number of statutes designed to curtail executive power and impose accountability on the defense and intelligence agencies.[138] For example, the War Powers Resolution, passed in 1973, restricted the President's ability to commit troops into armed conflict without Congressional authorization, and the Foreign Intelligence Surveillance Act (FISA), passed in 1978, required intelligence agencies to obtain a court order before engaging in certain foreign surveillance activities not otherwise restrained by the Fourth Amendment.[139]

The National Emergencies Act of 1977 was another of these post-Vietnam-era efforts to curtail executive power.[140] The NEA terminated states

130. Lyndon B. Johnson, *Action Program on the Balance of Payments*, 58 DEP'T ST. BULL. 110, 114 (1968).

131. *See* Sandra Kollen Ghizoni, *Nixon Ends Convertibility of U.S. Dollars to Gold and Announces Wage/Price Controls*, FED. RESERVE HISTORY (Aug. 1971), https://www.federalreservehistory.org/essays/gold_convertibility_ends.

132. *Id.*

133. Proclamation No. 4074, 85 Stat. 926 (1971).

134. *United States v. Yoshida Int'l, Inc.*, 526 F.2d 560, 569-570 (C.C.P.A. 1975).

135. *Id.* at 560.

136. *Id.* at 583.

137. *Id.* at 573.

138. *See e.g.*, 50 U.S.C. § 1541 (1973); 50 U.S.C. § 1601.

139. The FISA statute was amended after the 9/11 attacks to provide broader surveillance authorities that became the basis of the NSA's controversial bulk metadata collection. *See, e.g.*, David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795 (2012); 50 U.S.C. § 1541.

140. 50 U.S.C. § 1601.

of emergency that had been declared as of September 14, 1976, and provided a procedure for Congressional oversight of future emergency declarations.[141] Congress recognized, however, that TWEA included some important provisions relating to the President's war and foreign affairs powers that should not fall under NEA's general provisions.[142] NEA, therefore, exempted emergency authorities exercised under the TWEA so that Congress could consider how to revise it.[143]

IEEPA replaced TWEA's economic emergency powers provisions.[144] As one of the sponsors of IEEPA, Rep. Jonathan Bingham, stated, TWEA was flawed and needed to be revised because "through usage and amendment, [TWEA] has become essentially an unlimited grant of authority for the President to exercise, at his discretion, broad powers in both the domestic and international economic arena, without congressional review."[145] IEEPA limited the authorities under the Trading With the Enemy Act to circumstances of declared war and created new authorities for emergency economic actions under new limitations.[146] In addition to Congressional power to terminate the state of emergency under the NEA, IEEPA removed the executive's power to control purely domestic transactions for states of emergency short of war that exists under TWEA.[147]

The overriding concern in the IIEPA legislative history thus was to curb the President's ability to implement open-ended economic controls with little connection to war or a true emergency.[148] As the House Committee on International Relations' Report on the bill that became IIEPA stated, "[a] national emergency should be declared and emergency authorities employed only with respect to a specific set of circumstances which constitute a real emergency, and for no other purpose . . . . A state of national emergency should not be a normal state of affairs."[149]

IEEPA was broadened somewhat by the PATRIOT ACT amendments after the 9/11 attacks.[150] The operative provision of IEEPA relating to the Huawei Order is section 1702(a)(1)(B), which authorizes the President to:

> investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition,

---

141. *Id.*
142. CASEY, *supra* note 32, at 8-10.
143. *Id.* at 8-9.
144. JONATHAN B. BINGHAM, TRADING WITH THE ENEMY ACT REFORM LEGISLATION, H.R. REP. NO. 95-459, at 1 (1977).
145. *Id*. at 7.
146. *Id.* at 2.
147. *Id.* at 2, 6-7, 15.
148. *Id.* at 1.
149. H.R. REP. NO. 95-459 at 10.
150. CASEY, *supra* note 32.

> holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or any exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States . . . .[151]

The PATRIOT Act (1) added the phrase "block during the pendency of an investigation" and (2) clarified the jurisdictional trigger to state that a covered transaction could include property in which a foreign country or national has any "interest by any person, or with respect to any property, subject to the jurisdiction of the United States."[152] These broadening amendments did not change the requirement of a national emergency to invoke IEEPA.[153]

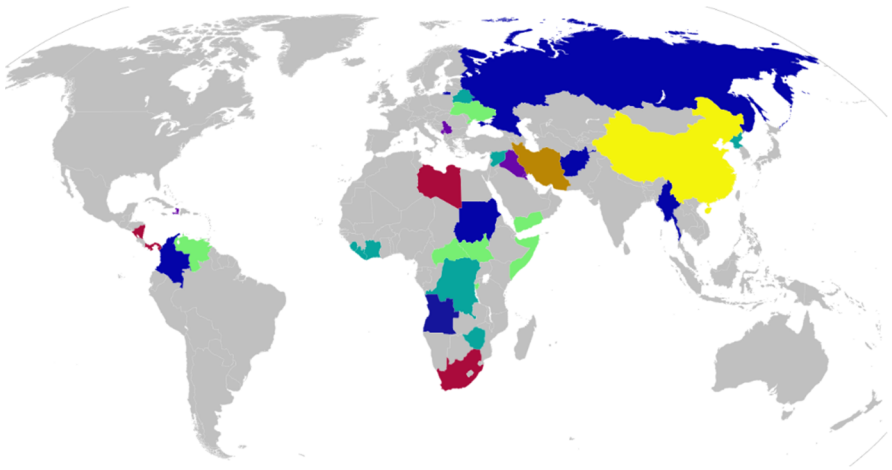
C. Subsequent History: Executive Orders Under IEEPA

Although the legislative history shows that IEEPA was designed to curtail previously broad exercises of executive power under TWEA, in practice it has been used by Presidents of both parties as nearly a blanket authorization for the invocation of economic sanctions to achieve various foreign policy goals in circumstances that often seem to fall far short of national emergencies.[154] There have been at least forty-seven original Executive Orders invoking IEEPA, as follows:[155]

President	**Original Orders Under IEEPA**
Carter	1
Reagan	5
George H.W. Bush	5
Clinton	7
George W. Bush	9
Obama	10
Trump	10

151. 50 U.S.C. § 1702(a)(1)(B).
152. *See* USA PATRIOT Act, Pub. L. 107-56, § 106, 115 Stat. 272 (2001).
153. CASEY, *supra* note 32.
154. 50 U.S.C. § 1703(a), (b)(2) (1977).
155. By "original orders" I mean an initial order relating to a specific declaration of a state of emergency. Most of these orders were extended multiple times, sometimes with amendments, and sometimes by a successor to the President who first issued them. *See* Executive Orders listed at 50 U.S.C. § 1701; *see infra* Appendix A.

The following map shows the countries to which these original Orders have applied.[156]



This map illustrates that, with a few exceptions relating to the war on drugs in Latin America, the pattern of IEEPA Orders reflects the familiar geopolitical alignments of the late Cold War and War on Terror eras.[157]

In addition, Executive Orders issued under IEEPA show that IEEPA has been used not only to sanction countries, but also to sanction individuals.[158] For example, Executive Order 13,288, signed by President George W. Bush on March 6, 2003, includes an appendix that names then-President of Zimbabwe, Robert Gabriel Mugabe, along with seventy-six other Zimbabwean government officials.[159] An additional eight Orders issued pursuant to IEEPA do not include such an appendix, but do block transactions related to classes of individual persons, with specific names subsequently to be supplied by the Secretary of the Treasury and the Secretary of State.[160] For example, Executive Order 13,611, signed by President Obama on May 16, 2012, blocks property transactions of persons who "have engaged in acts that directly or indirectly threaten the peace, security, or stability of Yemen, such as acts that obstruct the implementation of the agreement of November 23, 2011, between the Government of Yemen and those in opposition to it, which

156. A large color version of this map is available at https://drive.google.com/open?id=1L3-tavtiPDCLtt5wSXhYIoTuZ0lBlMVl.

157. *The Cold War*, JOHN F. KENNEDY PRESIDENTIAL LIBRARY & MUSEUM, https://www.jfklibrary.org/learn/about-jfk/jfk-in-history/the-cold-war (last visited Dec. 20, 2020).

158. *See* Exec. Order No. 13,288, 3 C.F.R. § 186 (2004); 7 Exec. Order No. 13,611, 3 C.F.R. § 260 (2013).

159. Exec. Order No. 13,288, 3 C.F.R. § 186.

160. *See infra* Appendix A.

provides for a peaceful transition of power in Yemen . . . determined by the Secretary of the Treasury, in consultation with the Secretary of State."[161]

Other Orders under IEEPA are aimed at broad problems as opposed to specific countries or individuals.[162] For example, Executive Order 12,947, issued by President Clinton, prohibits transactions with certain "terrorist organizations which threaten to disrupt the middle east peace process"; Executive Order 13,694, issued by President Obama, blocks transactions involving "any person determined . . . to have engaged in, directly or indirectly, cyber-enabled activities originating from . . . outside the United States that are reasonably likely to result in . . . a significant threat to the national security, foreign policy, or economic health or financial stability of the United States . . . " and that have certain criminal purposes; and Executive Order 12,978, also issued by President Clinton, addresses "narcotics traffickers centered in Columbia . . . ."[163]

The fact that more than a third of the original Presidential actions taken under IIEPA relate to specifically named or to-be-named individuals raises questions about how the statute's "unusual and extraordinary threat" and "national emergency" language has been interpreted by Presidents of both parties.[164] Certainly, it is part of U.S. foreign policy to promote democracy and the rule of law in places like Zimbabwe and Yemen.[165] In a country such as Yemen, U.S. foreign policy is particularly sensitive because an Al Qaeda affiliate, which perpetrated the October, 12, 2000 attack on the U.S.S. Cole, is located there, the country has been engulfed in a civil war, and ISIS also has a Yemeni presence.[166] But it seems a stretch to call these *unusual* and *extraordinary* threats.

Likewise, it is difficult to see how broad criminal threats, such as terrorism, the drug trade, or cybercrime, are *unusual* and *extraordinary* threats. In some sense, perhaps *all* criminal activity is unusual and extraordinary–after all, ordinary people, acting in ordinary ways, are not committing crimes, unless there is something gravely wrong with the criminal law. But if all criminal activity satisfies the "unusual and extraordinary" emergency standard, then the entire criminal law is an "emergency" measure,

---

161. Exec. Order No. 13,611, 3 C.F.R. § 260.

162. *See* Exec. Order No. 12,947, 60 Fed. Reg. 5,079 (Jan. 23, 1995); Exec. Order No. 12,978, 60 Fed. Reg. 54,579 (Oct. 21, 1995); Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 1, 2015).

163. Exec. Order No. 12,947, 60 Fed. Reg. 5,079 (Jan. 23, 1995); Exec. Order No. 12,978, 60 Fed. Reg. 54,579 (Oct. 21, 1995); Exec. Order No. 13,694, 3 C.F.R. § 297 (2016).

164. *See infra* Appendix A.

165. CONG. RESEARCH SERV., R44858, DEMOCRACY PROMOTION: AN OBJECTIVE OF U.S. FOREIGN ASSISTANCE (2019) (author names redacted from official report).

166. *See Al Qaeda in Yemen*, STANFORD CTR. FOR INT'L SEC. & COOPERATION (July 2015), https://cisac.fsi.stanford.edu/mappingmilitants/profiles/al-qaeda-yemen; Adam Baron, *Mapping the Yemen Conflict*, EUROPEAN COUNCIL ON FOREIGN RELATIONS (July 2019), https://www.ecfr.eu/mena/yemen.

and there is *never* an "ordinary" rule of law.[167] Perhaps the difference is that the drug trade, cybercrime, and terrorism are often coordinated by organized groups that can inflict large-scale harm.[168] Organized crime, however, is as old as crime itself, and the non-state actors who perpetrate these kinds of crimes often are supported, abetted, or sheltered by nation-states–all of which falls under existing domestic and international law.[169]

Nevertheless, the long-established Executive branch practice has been to read IEEPA broadly enough to cover such seemingly usual and ordinary threats, without any objection by Congress.[170] This suggests something both about the interpretation of the statute and about the statute's relation to inherent Presidential powers over foreign affairs.[171] Concerning statutory interpretation, many courts have recognized that a consistent interpretation of a statute by the agency entrusted with its enforcement is entitled to some weight.[172] A longstanding administrative interpretation is entitled to even greater weight when Congress has "left the [administrative] practice untouched."[173] Although the President acts directly under IEEPA, responsibility for specific implementation of Executive Orders issued under IEEPA falls to other executive branch agencies, including Treasury Department's Office of Foreign Assets Control (OFAC).[174] Congress has never acted to contravene any OFAC or other executive branch agency's regulations issued pursuant to IEEPA.[175]

There is a further presumption involving inherent and delegated Executive power when the President acts directly and Congress does not object.[176] As the Supreme Court stated in U.S. v. Midwest Oil Co,[177] in 1915:

> [G]overnment is a practical affair, intended for practical men. Both officers, lawmakers, and citizens naturally adjust themselves to any long-continued action of the Executive Department, on the presumption that unauthorized acts would not have been allowed to

---

167. *See* 50 U.S.C. § 1701.

168. *See generally* William J. Chambliss, *State Organized Crime*, 27 CRIMINOLOGY 183, 196 (1989).

169. *See generally id.* at 201-03.

170. *See* Dames & Moore v. Regan, 453 U.S. 654, 672-73, 678 (1981).

171. *See generally* Saxbe v. Bustos, 419 U.S. 65, 74 (1974); United States v. Midwest Oil Co., 236 U.S. 459, 472-73 (1915); *Youngstown,* 343 U.S. at 610-11.

172. *See, e.g.,* Mass. Trs. of E. Gas & Fuel Assocs. v. United States, 377 U.S. 235, 241-42 (1964).

173. *Saxbe*, 419 U.S. at 74.

174. *See generally* Barbara J. Van Arsdale, *Appendix M. Validity, Construction, and Operation of International Emergency Economic Powers Act, 50 U.S.C.A. §§ 1701 to 1707*, *in* HOMELAND SECURITY ACT SUMMARY (2020).

175. Louisa C. Slocum, *OFAC, The Department of State, and the Terrorist Designation Process: A Comparative Analysis of Agency Discretion*, 65 ADMIN. L. REV. 387, 412 (2013).

176. *See generally Midwest Oil Co.*, 236 U.S. at 472-73.

177. 236 U.S. 459.

> be so often repeated as to crystallize into a regular practice. That presumption is not reasoning in a circle, but the basis of a wise and quieting rule that, in determining the meaning of a statute or the existence of a power, weight shall be given to the usage itself,-even when the validity of the practice is the subject of investigation.[178]

Justice Frankfurter picked up this theme in his concurrence in *Youngstown*, which is less famous than Justice Jackson's concurring opinion for the 1952 case, but no less eloquent:

> The Constitution is a framework for government. Therefore the way the framework has consistently operated fairly establishes that it has operated according to its true nature. Deeply embedded traditional ways of conducting government cannot supplant the Constitution or legislation, but they give meaning to the words of a text or supply them. It is an inadmissibly narrow conception of American constitutional law to confine it to the words of the Constitution and to disregard the gloss which life has written upon them. In short, a systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned, engaged in by Presidents who have also sworn to uphold the Constitution, making as it were such exercise of power part of the structure of our government, may be treated as a gloss on 'executive Power' vested in the President by s 1 of Art. II.[179]

These principles, of course, are contestable both on their face and in any specific application. A longstanding executive branch practice may have actually been wrong; Congress' acquiescence may have constituted a dereliction of duty; and, therefore, the matter might be well overdue for judicial correction.[180] At the very least, however, President Trump's May 2019 Order is not inconsistent with the many other occasions on which IEEPA has been employed for what seem like general policy goals.[181]

D. Case Law

Presidential actions under IEEPA have been challenged in court for several reasons.[182] The most important for purposes of this paper include a broad challenge addressed by the Supreme Court in 1981; later challenges

178. *Midwest Oil Co.*, 236 U.S. at 472-73.
179. *Youngstown*, 343 U.S. at 610-11.
180. *See* Slocum, *supra* note 176, at 420-21, 423-24.
181. Exec. Order No. 13,873.
182. *See* discussion *infra* Sections III.D.1-3.

under the non-delegation doctrine; and challenges to specific actions under IEEPA's "information and information materials" exclusion.[183] In each case except one–and that only in a trial court–the courts have interpreted IEEPA broadly to uphold the President's actions.[184] These categories of cases are discussed in turn below.

1. Dames & Moore v. Regan

The most significant case under IEEPA was Dames & Moore v. Regan, decided by the Supreme Court in 1981.[185] The case arose out of the settlement of the Iranian hostage crisis.[186]

Prior to the hostage crisis, during a period when the U.S. still had friendly relations with Iran, a Dames & Moore subsidiary had entered into a contract with the Atomic Energy Organization of Iran, a department of the Iranian government, "to conduct site studies for a . . . nuclear power plant in Iran."[187] The Iranian Atomic Energy Organization terminated that contract on June 30, 1979–also prior to the hostage crisis, but in the midst of the Iranian Revolution, which shattered U.S.-Iranian relations.[188]

The American Embassy, located in Tehran, was seized on November 4, 1979.[189] President Carter declared a national emergency under IEEPA on November 14, 1979.[190] As part of the emergency measures, President Carter issued an Executive Order under IEEPA blocking the removal or transfer of Iranian property subject to the jurisdiction of the United States.[191] Pursuant to that order, OFAC issued a regulation declaring null and void "any attachment, . . . lien, . . . or other judicial process . . . with respect to any property in which on or since [November 14, 1979,] there existed an interest of Iran."[192]

---

183. *Id.*

184. *See* discussion *infra* Section III.D.3.

185. *Dames & Moore*, 453 U.S. 654.

186. *Id.* at 662.

187. *Id.* at 663-64.

188. *Id.* at 664. Dames & Moore was caught in a turbulent time in Iranian history and U.S.-Iranian relations. – the Iranian or Islamic Revolution. When Dames & Moore entered into its original contract, the government of Shah Mohammad Reza Pahlavi was friendly to the West and was supported by the United States. Demonstrations against the Shah began in 1977, leading to massive civil unrest in 1978. The Shah left the country in exile on January 16, 1979, and on February 11, 1979, his remaining loyal troops were defeated by forces loyal to the Islamic leader Grand Ayatollah Ruhollah Khomeini. By December 1979 Khomeini had become supreme leader of an Islamic theocracy in conflict with the United States. Suzanne Maloney & Keian Razipour, *The Iranian Revolution – A Timeline of Event*s, BROOKINGS INST. (Jan. 24, 2019), https://www.brookings.edu/blog/order-from-chaos/2019/01/24/the-iranian-revolution-a-timeline-of-events/.

189. *Dames & Moore*, 453 U.S at 662.

190. *Id.*

191. *Id.* at 662-63.

192. *Id.* at 663 (quoting 31 C.F.R. § 535.203(e) (1980)).

On November 26, 1979, President Carter issued a general license allowing certain claims to proceed against Iran, and, on December 19, 1979, OFAC issued a clarifying regulation allowing such claims to include pre-judgment attachments.[193] These actions were designed to preserve the claims of U.S. persons and entities against Iran until the crisis could be resolved.[194] The day the OFAC clarifying regulation was issued, Dames & Moore filed a claim in federal district court in California for over $3.4 million it claimed it was owed under the contract.[195] The District Court issued orders of [pre-judgment] attachment, including orders directed to accounts in some Iranian banks, "to secure any judgment that might be . . . " issued in Dames & Moore's favor.[196]

While Dames & Moore's case was still pending, the hostage crisis was resolved under an agreement between the U.S. and Iran.[197] The agreement established an Iran-United States Claims Tribunal to arbitrate claims between nationals of the two countries, and stated that the United States must terminate all legal proceedings involving U.S. persons and Iranian state enterprises and nullify all judgments or attachments issued in any such proceedings.[198] President Carter issued a string of Executive Orders effecting this agreement on January 19, 1981, including an Order requiring banks "holding Iranian assets to transfer them 'to the Federal Reserve Bank of New York' . . . " for ultimate transfer back to Iran.[199] These Orders were subsequently ratified and extended by President Reagan through an Executive Order issued on February 24, 1981.[200]

In between these Orders by Presidents Carter and Reagan, on January 27, 1981, Dames & Moore obtained summary judgment in its California federal lawsuit.[201] When Dames & Moore subsequently sought to execute on this judgment, the California District court vacated its prior writs of attachment and stayed all proceedings "in light of the Executive Orders . . . " implementing the hostage settlement.[202] Dames & Moore then filed a claim for declaratory and injunctive relief in federal court claiming the Executive Orders were unconstitutional, both as an overreach of executive power and

193. *Id.*
194. *See* 31 C.F.R. § 535.203 (2020).
195. *Dames & Moore*, 453 U.S at 663-64.
196. *Id.* at 664.
197. *Id.* at 663-64.
198. *Id.* at 665.
199. *Id.* at 665-66.
200. *Dames & Moore*, 453 U.S at 666.
201. *Id.*
202. *Id.*

as a taking without compensation.[203] That case eventually reached the Supreme Court.[204]

Justice Rehnquist, writing for the majority, viewed the matter in historic terms: "[t]he questions presented by this case," he said, "touch fundamentally upon the manner in which our Republic is to be governed."[205] After mentioning John Jay, Alexander Hamilton, James Madison, Alexis deTocqueville and James Bryce–in the space of one breathless sentence– Justice Rehnquist proceeded to discuss how President Carter's and Reagan's Orders fit into the *Youngstown* framework.[206] In fairness to Justice Rehnquist, the tidal effect of a process that, at first, seemed to preserve private civil claims against Iran and then dumped all those claims into an uncertain arbitration process, while transferring Iranian assets that might satisfy an arbitration award back to Iran, left claimants like Dames & Moore stranded.[207] Iran was not the enemy when Dames & Moore first entered into its contract, so the traditional power to restrict trade with the enemy did not precisely apply.[208] Even though the final hostage deal established a claims arbitration process, it looked suspiciously like private claimants were footing the bill for a ransom payment.[209] Further, President Carter's and Reagan's Orders had the effect of depriving American citizens and companies of access to the courts, exacerbating the separation of powers problem.[210]

The key question for Justice Rehnquist was whether IEEPA authorized the President to nullify the writs of attachment, suspend civil claims in favor of arbitration, and order the transfer of Iranian funds to the Federal Reserve for repatriation in Iran.[211] To address this issue, Justice Rehnquist first turned to the *Youngstown* framework.[212] The *Youngstown* framework, drawn from Justice Jackson's concurrence in that case, recognizes three zones of Presidential action: (1) when the President acts with express or implied authorization from Congress, the President's power carries a strong presumption of validity; (2) when the President acts without Congressional authorization, there is a "zone of twilight in which [the President] and Congress may have concurrent authority," which will require a more nuanced analysis of the validity of the President's actions; and (3) when the President acts contrary to the will of Congress, when the President's power is "at its

203. *Id.* at 666-67.
204. *Id.* at 668.
205. *Dames & Moore*, 453 U.S at 659.
206. *Id.* at 659-60, 668.
207. *Id.* at 669.
208. *Id.* at 662-64.
209. *See id.* at 665.
210. *Dames & Moore*, 453 U.S. at 662-63, 665-66.
211. *Id.* at 669-70.
212. *Id.* at 668-69.

lowest ebb" and the Court must find Congress does not have the power to act on the subject in order to sustain the President's action.[213]

There was no dispute in *Dames & Moore* over President Carter's declaration of emergency.[214] The dispute centered on Section 1702(a)(1)(B) of IEEPA, which, given a properly declared emergency, authorized the President to:

> investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States.[215]

Concerning the nullification of writs of attachment, Justice Rehnquist noted that this provision was derived from the TWEA and that "the legislative history and cases interpreting the TWEA fully sustain[ed] the broad authority of the Executive when acting under this congressional grant of power."[216] According to Justice Rehnquist, "[a]lthough Congress intended [in IEEPA] to limit the President's emergency power in peacetime, we do not think the changes brought about by the enactment of the IEEPA in any way affected the authority of the President" to nullify the writs of attachment.[217]

Concerning the suspension of civil claims, however, Justice Rehnquist concluded that "[t]he terms of the IEEPA . . . do not authorize the President to suspend claims in American courts."[218] Civil claims regarding foreign policy, Justice Rehnquist stated, are not in themselves "transactions," and any resulting judgment is not a form of "property" within the jurisdiction of the United States as contemplated by IEEPA.[219] The Court also concluded that another statute advanced by the Government, the Hostage Act of 1868, likewise did not authorize the suspension of civil claims.[220]

But the restriction of the President's ability to suspend civil claims did not mean the President's actions were improper.[221] Both IEEPA and the

213. *Youngstown*, 343 U.S. at 635-637 (Jackson, J., concurring).
214. *Dames & Moore*, 453 U.S. at 662 n.1.
215. 50 U.S.C. § 1702(a)(1)(B).
216. *Dames & Moore*, 453 U.S. at 672.
217. *Id.* at 672-73.
218. *Id.* at 675.
219. *Id.*
220. *Id.* at 676.
221. *Dames & Moore*, 453 U.S. at 677.

Hostage Act, the *Dames & Moore* Court suggested, demonstrated "congressional acceptance of a broad scope for executive action in circumstances such as those presented in this case."[222] Since "Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take or every possible situation in which he might act," a "failure of Congress specifically to delegate authority does not, 'especially . . . in the areas of foreign policy and national security,' imply 'congressional disapproval' of action taken by the Executive."[223] Further, Congress had previously approved similar foreign claim settlement procedures in Yugoslavia, China, East Germany, and Vietnam under the International Claims Settlement Act of 1949.[224]

In addition, the Court previously "recognized that the President does have some measure of power to enter into executive agreements without obtaining the advice and consent of the Senate." Different Presidents have entered into such agreements in the past to settle claims without any objection from Congress.[225] Here Justice Rehnquist quoted from Justice Frankfurter's concurring opinion in *Youngstown* that "a systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned . . . may be treated as a gloss on 'Executive Power' vested in the President by § 1 of Art. II."[226] The Court therefore upheld President Carter's and Reagan's Orders against Dames & Moore's challenge.[227]

2. Cases Asserting Non-Delegation Challenges

A number of cases have raised non-delegation challenges to IEEPA.[228] Many of these cases stem from criminal convictions of individuals and corporations that did business with or traveled to countries subject to U.S. sanctions, including Iran and Iraq.[229] Not surprisingly, none of these challenges succeeded.[230]

---

222. *Id.*
223. *Id.* at 678.
224. *Id.* at 680-81.
225. *Id.* at 682.
226. *Dames & Moore*, 453 U.S. at 686.
227. *Id.* at 689-90 (The majority also rejected Dames & Moore's takings claim as not yet ripe for adjudication, pending the results of any arbitration under the procedure established in the hostage agreement.).
228. *See e.g.*, United States v. Amirnazmi, 645 F.3d 564, 571 (3rd Cir. 2011); United States v. Nejad, 18-cr-224, 2019 WL 6702361, at *10 (S.D.N.Y. 2019); United States v. Nazemzadeh, 11 CR 5726 L., 2014 WL 310460, at *2 (S.D. Cal. 2014).
229. *See e.g.*, *Amirnazmi*, 645 F.3d at 567-68, 570; *Nejad*, 18-cr-224, 2019 WL 6702351 at *1; *Nazemzadeh*, 11 CR 5726 L., 2014 WL 310460, at *1.
230. *See e.g.*, *Amirnazmi*, 645 F.3d at 567-68, 577; *Nejad*, 18-cr-224, 2019 WL 6702361, at *10; *Nazemzadeh*, 11 CR 5726 L., 2014 WL 310460, at *8.

For example, in *U.S. v. Amirnazmi*,[231] the defendant, a dual U.S. and Iranian citizen, sold chemical plant software and related consulting services to the state-owned National Petrochemical Company of Iran and engaged in other business in Iran, including taking a private audience with Iranian President Mahmoud Ahmadinejad. The *Amiranazmi* defendant was convicted of criminal violations of OFAC regulations issued under IEEPA and other related charges.[232] The *Amirnazmi* case illustrates that IEEPA restrictions can have a long shelf life, with serious consequences for businesses and individuals who violate them.[233]

On March 15, 1995, President Clinton issued an Executive Order that found "'an unusual and extraordinary' threat posed to the national security, foreign policy, and economy of the United States" arising from "'the actions and policies of the Government of Iran.'"[234] That Executive Order imposed restrictions on transactions involving the Iranian petroleum industry.[235] This Order was supplemented by another Executive Order signed by President Clinton on May 6, 1995, implementing a complete trade embargo between the U.S. and Iran.[236] These sanctions were imposed by the Clinton Administration's increased concerns about terrorism, and Iran's effort to develop nuclear weapons.[237] The OFAC regulations issued pursuant to these Orders prohibited the "'exportation, reexportation, sale, or supply . . . of any goods, technology, or services to Iran or the Government of Iran.'"[238] The OFAC regulations incorporated the IEEPA exception for information materials, but did not exempt such materials "not fully created and in existence at the date of the transactions, or to the substantive or artistic alteration or enhancement of informational materials."[239] Although the defendant in *Arinazmi* was charged in 2008 for activities that occurred from 2001-2008, these regulations were still in effect.[240]

The non-delegation doctrine challenge in a criminal case such as this is a desperate Hail Mary pass, and, not surprisingly, it never results in a game-saving touchdown. The Third Circuit analyzed IEEPA under the "intelligible

231. 645 F.3d 564.
232. *Id.* at 567-68, 570-71.
233. *Id.* at 567-68.
234. *Id.* at 574. *See also* Exec. Order No. 12,957, 60 Fed. Reg. 14,615, (Mar. 15, 1995).
235. *See generally id.* (President Clinton prohibiting any contractual activities related to the development of petroleum resources in Iran by any United States citizen or entity).
236. *Amirnazmi*, 645 F.3d at 574 (The order signed by President Clinton "fortified the sanctions regime by banning U.S. firms from exporting to Iran, importing from Iran, or investing in Iran, subject to the exemptions provided in IEEPA.").
237. Todd S. Purdum, *Clinton to Order A Trade Embargo Against Teheran*, N.Y. TIMES (May 1, 1995), http://www.nytimes.com/1995/05/01/world/clinton-to-order-trade-embargo-against-teheran.html.
238. *Amirnazmi*, 645 F.3d at 574 (quoting 31 C.F.R. § 560.204 (2010)).
239. *Id.* (quoting 31 C.F.R. § 560.210(c) (2010)).
240. *Id.* at 568-69, 580.

principle" requirement of the non-delegation doctrine.[241] The court noted that the requirement of a national emergency declaration, along with the congressional consultation, review, and termination provisions in IEEPA, easily satisfied the intelligible principle standard.[242]

3. "Information Materials": Chevron and First Amendment Challenges

Another important line of challenge to Presidential actions under IEEPA relates to the statutory exclusion of "information materials."[243] Section 1702(b)(3) of IEEPA states that:

> The authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly– . . . the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.[244]

This provision originally was added to IEEPA in 1988 by the "Berman Amendment" (named after its sponsor, Representative Howard L. Berman) and was supplemented in 1994 by the "Free Trade in Ideas Act" (also sponsored by Rep. Berman).[245]

The original Berman Amendment was a response to seizures of books and magazines from Cuba under the prior version of IEEPA.[246] It excluded Presidential authority to regulate the importation or exportation of "publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes," or other informational materials not otherwise subject to

241. *Id.* at 575 (quoting Toby v. United States, 500 U.S. 160, 165-66 (1991)).

242. *Id.* at 576-77. This result was not surprising because the Supreme Court has invalidated only two statutes under the non-delegation doctrine and the "intelligible principle" standard announced in *Touby v. United States*, 500 U.S. 160 (1991) is an easy threshold to cross. *See* United States v. Dhafir, 461 F.3d 211, 218-19 (2nd Circ. 2006) (upholding sanctions for activities involved with Iraq under IEEPA using the intelligible principle standard); United States v. Arch Trading Co., 987 F.2d 1087, 1096 (4th Cir. 1993) (same).

243. 50 U.S.C. § 1702(b)(3).

244. *Id.*

245. Kalantari v. NITV, Inc., 352 F.3d 1202, 1205 (9th Cir. 2003); Capital Cities/ABC, Inc. v. Brady, 740 F. Supp. 1007, 1009 (S.D.N.Y. 1990).

246. Laura A. Michalec, Note, *Trade with Cuba Under the Trading With the Enemy Act: A Free Flow of Ideas and Information?*, 15 FORDHAM INT'L L.J. 808, 816-18 (1991/1992); Burt Neuborne & Steven R. Shapiro, *The Nylon Curtain: America's National Boarder and the Free Flow of Ideas*, 26 WM. & MARY L. REV. 719, 730-33 (1985).

export control restrictions.[247] The Berman Amendment applied both to IEEPA and to a related provision in TWEA.[248]

A dispute about the Berman Amendment as applied to TWEA arose in 1989 concerning an exhibition and auction of Cuban art at the Cuban Museum in Miami–which included not only legal wrangling, but also death threats and a bombing attack.[249] Pursuant to the OFAC regulations implementing TWEA as it related to the ongoing trade embargo with Cuba that had begun in 1962, the U.S. Customs service seized approximately 200 paintings of Cuban origin from the personal residence and business office of Ramon Cernuda, an executive at the Cuban Museum.[250] Cernuda was not charged with any crimes and sought an order for the return of the paintings.[251] The government argued that "original art is not 'informational' but merely aesthetic and thus not exempt from the TWEA."[252] A district court in Florida rejected the government's argument.[253] The court stated that "statutory construction and the legislative history of the 1988 TWEA amendment show[ed] that Congress amended the TWEA to exempt 'informational materials,' in order to prevent the statute from running afoul of the First Amendment" and that "[o]riginal paintings fall within the statutory exception."[254] Accordingly, the court ordered the government to return the paintings to the museum[255]

The Berman Amendment also was the subject of a dispute between OFAC and the ABC Television Network in 1991, when OFAC refused a license under TWEA for ABC to enter into a contract for rights to televise the 1991 Pan American Games, which were scheduled to occur in Cuba.[256] OFAC's regulations, as revised after the Berman Amendment was passed, "exclude[ed] 'intangible items such as telecommunications transmissions'" from the "definition of 'informational materials."[257] ABC claimed that this interpretation was *ultra vires* because television broadcasts were within the protection of the First Amendment and therefore should be covered by the Berman Amendment.[258] In an opinion that remarkably did not mention the *Cernuda* case, a district court in New York upheld OFAC's interpretation of the statute.[259] According to the court, the Berman Amendment was

247. 50 U.S.C. § 4305(b)(4) (2015).
248. *Amirnazmi*, 645 F.3d at 584.
249. Cernuda v. Heavy, 720 F. Supp. 1544, 1545 (S.D. Fla. 1989).
250. *Id.* at 1545-46.
251. *Id.* at 1546.
252. *Id.* at 1549.
253. *Id.* at 1550.
254. *Cernuda*, 720 F. Supp. at 1553.
255. *Id.* at 1554.
256. *Capital Cities/ABC*, 740 F. Supp. at 1009-10.
257. *Id.* at 1009 (quoting 31 C.F.R. § 515.332(b)(2) (1995)).
258. *Id.* at 1010-11.
259. *See generally Capital Cities/ABC*, 740 F. Supp. 1007.

ambiguous relating to television broadcasts and the OFAC regulation was neither arbitrary nor irrational.[260] The court further stated that the government has flexible authority to regulate speech relating to foreign affairs.[261]

> The subsequent Free Trade in Ideas Act, also introduced by Representative Berman, was an effort to broaden the information materials exemption in response to the ABC Television case and other similar actions by OFAC.[262] A House Report accompanying the Free Trade in Ideas Act noted that the original Berman Amendment "was explicitly intended, by including the words 'directly or indirectly,' to have a broad scope," but that further amendment was needed because "the Treasury Department has narrowly and restrictively interpreted the language in ways not originally intended."[263] The Report also noted that the Free Trade in Ideas Act sought to protect the constitutional rights of Americans to educate themselves about the world by communicating with peoples of other countries in a variety of ways, such as by sharing information and ideas with persons around the world, traveling abroad, and engaging in educational, cultural and other exchanges with persons from around the world.[264]

Notwithstanding the Free Trade in Ideas Act amendment, when the *Amirnazmi* case was decided, the OFAC regulations retained an earlier prohibition on "informational materials 'not fully created and in existence at the date of the transactions, or to the substantive or artistic alteration or enhancement of informational materials.'"[265] This carve-out applied to the defendant in *Amirnazmi* because he was customizing software for his Iranian customers.[266] The *Amirnazmi* defendant challenged this prohibition as *ultra vires*.[267]

The Third Circuit rejected this challenge.[268] According to the Third Circuit, it was significant, given the history from *Cernuda* and *Capital Cities/ABC* to the Free Trade in Ideas Act, that Congress had allowed the "not fully created and in existence" carve-out of the OFAC regulations to stand.[269]

---

260. *Id.* at 1012.
261. *Id.* at 1012-13.
262. *See* Amirnazmi, 645 F.3d at 585-86.
263. H.R. REP. NO. 103-482, at 239 (1994) (Conf. Rep.).
264. *Id.* at 238.
265. *Amirnazmi*, 645 F.3d at 584.
266. *Id.* at 582-83.
267. *Id.* at 583.
268. *Id.*
269. *Id.* at 585, 587 (citing Chevron U.S.A. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984)).

The court held that, under the *Chevron* doctrine, OFAC's interpretation was a permissible construction of the statute.[270] The court cited the canon of statutory construction that if Congress knows how an agency interprets a statute, but does not attempt to adjust that interpretation while changing another part of the statute, courts may understand Congress's inaction as approval of the agency's interpretation.[271] The Third Circuit also noted that OFAC had provided further guidance about the "not fully created and in existence" carve-out without any negative response from Congress.[272]

The Supreme Court's opinion in *Dames & Moore*, together with the other cases discussed above, show that courts are highly reluctant to invalidate Executive actions taken under IEEPA or under related provisions of TWEA.[273] There is no doubt that the Iranian hostage crisis satisfied any reasonable definition of a "national emergency," and the Court was unwilling to touch President Carter's hostage settlement deal, even if it did appear that some private property and contract claims had been offered up as a ransom payment.[274] Later cases involving ongoing tensions between the U.S. and countries such as Iran and Cuba arguably involved regular and longstanding diplomatic tensions rather than emergencies, but in those cases lower courts also read the Executive's authority broadly, with the exception of the Florida district court in *Cernuda*.[275] The *Capital Cities/ABC* and *Amirnazmi* cases show that courts may continue to give the Executive a long leash even when Congress has specifically tried to narrow the statute, as in the Berman and Free Trade in Ideas Act Amendments to IEEPA.[276] Although there is not a large amount of precedent and none of the prior cases, including *Dames & Moore*, involve facts analogous to the large scale build out of 5G Internet infrastructure, the existing case law does not suggest a challenge to President Trump's May 2019 Order on Constitutional or statutory grounds would likely succeed.[277]

Recent developments concerning the TikTok video sharing service and the WeChat texting platform, however, could suggest courts might read the "information materials" exception more closely. On August 6, 2020,

---

270. *Amirnazmi*, 645 F.3d at 586.

271. *Id.* at 587 (quoting Barrera-Echavarria v. Rison, 44 F.3d 1441, 1444-45 (9th Cir. 1995)).

272. *Id.* at 587. That guidance was an international trade regulation that stated "'[t]ransactions that are prohibited notwithstanding this section include, but are not limited to, payment of advances for information and informational materials not yet created and completed . . . and provision[s] of services to market, produce or co-produce, create or assist in the creation of information and informational materials.'" 31 CFR § 560.210(c)(2) (2008).

273. *See Dames & Moore*, 453 U.S. at 672-73; *Amirnazmi*, 645 F.3d at 591; *Capital Cities/ABC*, 740 F. Supp. at 1015; *Cernuda*, 720 F. Supp. at 1554.

274. *See Dames & Moore*, 453 U.S. at 679-80.

275. *See e.g.*, *Capital Cities/ABC*, 740 F. Supp. at 1009, 1014; *Cernuda*, 720 F. Supp. at 1545, 1554.

276. *Amirnazmi*, 645 F.3d at 584-87; *Capital Cities/ABC*, 740 F. Supp. at 1012-14.

277. *See* discussion *supra* Section III.D.

President Trump issued two separate Executive Order under IEEPA and other authorities that, in conjunction with the Huawei Order, barred any transactions by U.S. persons with the Chinese company that owned the TikTok app and the WeChat app.[278] TikTok is an enormously popular video sharing service through which users submit short video clips, often involving jokes or funny dance moves.[279] WeChat is a video and text communication app.[280] The Executive Orders asserted that TikTok and WeChat are vectors for Chinese propaganda and information theft.[281]

In September 2020, a district court in California issued a preliminary injunction barring enforcement of the WeChat Executive Order.[282] In October and December, 2020, district courts in Pennsylvania and the District of Columbia issued preliminary injunctions against enforcement of Executive Orders issued by President Trump that would have shut down the TikTok video service because of its connections to China.[283] These cases suggest a possibly broader reading of the "information materials" exception. They appear distinguishable from the issues surrounding Huawei because they involve the use of an app by consumers to create original video content, which extends far beyond a ban on pieces of hardware for which there are available substitutes. Nevertheless, the TikTok cases raise interesting questions about the fluidity between the categories of "software" and "hardware" in relation to apps. The government has filed appeals in all these cases, which as of this writing remain pending.

E. Internet-Era Developments and the 2018 Export Control Reform Act

As previously noted President Trump's May 2019 Order is important because it relates to the future of Internet governance.[284] IEEPA is a pre-Internet-era statute, rooted in another statute, TWEA, that dates to World War I.[285] TWEA, in turn, relates to older principles in English and European law, from the Napoleonic age and before, about the Sovereign's power to restrict trade with the enemy.[286] For example, in *The Julia*, a prize case from 1814,

278. Exec. Order 13482 (August 6, 2020); Exec. Order 13483 (August 6, 2020).

279. *See* TikTok website, www.tiktok.com.

280. *See* WeChat website, https://www.wechat.com/en/.

281. Exec. Order 13482.

282. *U.S. v. WeChat Users Alliance v. Trump*, 2020 WL 5592848 (N.D. Cal. 2020).

283. *Marland v. Trump*, —- F. Supp.3d —-, 2020 WL 6381397 (E.D. Pa. 2020); *TikTok, Inc. v. Trump*, —- F. Supp.3d —-, 2020 WL 7233557 (D.D.C. 2020).

284. *See* Exec. Order No. 13,873.

285. CASEY, *supra* note 32, at 2-3.

286. The Rapid, Perry, Master, 12 U.S. (9 Cranch) 155, 161-62 (1814) (Stating that "[i]n the state of war, nation is known to nation only by their armed exterior; each threatening the other with conquest or annihilation. The individuals who compose the belligerent states, exist, as to each other, in a state of utter occlusion. If they meet, it is only in combat."); *Emergency Controls on International Economic Transactions: Hearing on H.R. 1560 and H.R. 2382 Before the Subcomm. on Int'l Econ. Policy and Trade*

Justice Story quoted the 17th Century Dutch Jurist Bynkershoek: "'*Ex natura belli, commercia inter hostes cessare, non est dubitandum. Quamvis nulla specialis sit commerciorum prohibitio, ipso tamen jure belli commercia esse vetita, ipsoe indictiones bellorum satis declarant*,'" which roughly translates to, "It cannot be doubted that it is part of the nature of war for trade between combatants to cease. Although there is no specific rule preventing trade, the law of war itself nevertheless makes sufficiently clear that trade has been forbidden."[287] Does the Internet's global, borderless community change this calculus?

As the Internet began to mature in the late 1990's and early 2000's, OFAC issued guidance letters under the informational materials exemption regarding Internet search and enhanced search listings in Iran.[288] Some of these letters seem to be related to the same group of inquiries, although the details, including the name of the inquiring entity, have been redacted.[289]

The first of these guidance letters, issued on April 30, 2003 in response to a request dated February 28, 2001, confirmed that a not-for-profit informational database available over the Internet, including a search function for the database, could be made accessible to entities in Iran.[290] The second, issued on June 3, 2003, concerned the provision of Internet connectivity services to Iran.[291] OFAC stated that such services could be approved on a case-by-case basis if the applicant shows that it will not export prohibited goods, technology, or software to Iran and would not "act as the provider of end-user Internet or telecommunications services" to Iran, the Iranian government, or any person in Iran.[292]

The third letter, issued on July 8, 2003, stated that a U.S. company could not provide paid enhanced Internet search listings to entities in Iran.[293] The fourth letter, issued on December 11, 2003, modified the July 8, 2003 letter.[294]

---

of the Comm. on Int'l Relations, 95th Cong. 81 (1977) (Statement of Peter Weiss, Vice President, Center for Constitutional Rights, New York, N.Y.) (Stating that "'trading with the enemy' was not a concept invented in 1917 to give American Presidents unlimited power to impose restrictions on the foreign and, in some cases, domestic commerce of this country. It is an old, venerable, and, when prudently applied, a necessary institution.").

287. The Julia, Luce, Master, 12 U.S. (8 Cranch) 181, 193 (1814).Translation provided by Carrie Opderbeck and Kevin Oriani.

288. *Interpretive Rulings on OFAC Policy*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/iran-sanctions/interpretative-rulings-on-ofac-policy (last visited Dec. 20, 2020).

289. *Id.*

290. Letter from R. Richard Newcomb, Director of OFAC, U.S. DEP'T OF THE TREASURY (April 30, 2003), https://home.treasury.gov/system/files/126/ia043003.pdf.

291. Letter from R. Richard Newcomb, Director of OFAC, (June 3, 2003), https://home.treasury.gov/system/files/126/ia060603.pdf [hereinafter Newcomb, June 3, 2003].

292. *Id.*

293. Letter from R. Richard Newcomb, Director of OFAC, U.S. DEP'T OF THE TREASURY (July 8, 2003), https://home.treasury.gov/system/files/126/ia070803.pdf.

294. *Id.*

In the December 11, 2003 letter, OFAC stated that although "[t]he listing of basic information on a website in a uniform format for companies around the world, including Iran," was not prohibited, "[t]he provision of marketing services to persons in Iran or the Government of Iran, above and beyond the mere dissemination of information in-being" is prohibited.[295] The December 11, 2003 letter stated that the provider could supply enhanced listings that included preexisting content supplied by the Iranian company, but could not create or modify such materials for the Iranian company.[296]

In 2010, OFAC issued a final rule that modified prior sanctions rules relating to Sudan and Iran relating to "the exportation of certain services and software incident to the exchange of personal communications over the Internet."[297] This followed a December 2009 Department of State determination that "this software is necessary to foster and support the free flow of information to individual Iranian citizens and, therefore, is essential to the national interest of the United States."[298] The sorts of activities covered by the new exemption included "instant messaging, chat and e-mail, social networking, sharing of photos and movies, web browsing, and blogging" software that is "publicly available at no cost to the user."[299] In 2012, OFAC issued an "Interpretive Guidance and Statement of Licensing Policy on Internet Freedom in Iran" under the resulting regulations.[300] The Interpretive Guidance included a list of permitted applications, including Yahoo Messenger, free Skype, Dropbox, Internet browsers, RSS feed readers, and free plug-ins such as Java.[301]

The trend from the Free Trade in Ideas Act through OFAC's early and more recent Internet-era guidance documents suggests that technology relating to basic Internet communication applications, which allow individuals from adverse countries to access ideas outside their borders, will not usually run afoul of sanctions regulations.[302] In contrast, bespoke software configured for a state-controlled entity such as an Iranian oil company will not qualify for an exemption under OFAC regulations and the courts will not likely disagree with OFAC's interpretation of TWEA or IEEPA despite its tenuous relationship to the actual statutory language.[303]

---

295. *Id.*

296. *Id.*

297. Cuban Assets Control Regulations; Sudanese Sanctions regulations; Iranian Transactions Regulations, 75 Fed. Reg. 10,997 (March 10, 2010) (to be codified at 31 C.F.R. §§ 515, 539, 560).

298. *See id.*

299. *Id.*

300. OFFICE OF FOREIGN ASSETS CONTROL, INTERPRETIVE GUIDANCE AND STATEMENT OF LICENSING POLICY ON INTERNET FREEDOM IN IRAN (Mar. 20, 2012), https://home.treasury.gov/system/files/126/internet_freedom.pdf [hereinafter INTERNET FREEDOM IN IRAN].

301. *Id.*

302. *Id.*

303. Newcomb, June 3, 2003, *supra* note 292.

At the same time, with some degree of apparent contradiction, Congress recently seems to have significantly *expanded* the President's authority to restrict software and other technology exports under IEEPA.[304] Materials that were subject to export controls by Presidential action under 50 U.S.C. §§ 4604 or 4605 previously were not covered by the IEEPA information materials exclusion.[305] Section 4604 gave the President broad authority to "prohibit or curtail the export of any goods or technology subject to the jurisdiction of the United States or exported by any person subject to the jurisdiction of the United States" in order to restrict "the export of goods or technology . . . [which would] make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States."[306] Section 4605 gave the President broad authority to:

> [P]rohibit or curtail the exportation of any goods, technology, or other information subject to the jurisdiction of the United States or exported by any person subject to the jurisdiction of the United States, to the extent necessary to further significantly the foreign policy of the United States or to fulfill its declared international obligations,

including to protect against domestic inflation or shortages, to combat terrorism, and to protect public health.[307]

The authorities granted in 50 U.S.C. §§ 4604 and 4605 were repealed by the Export Control Reform Act of 2018 (ECRA), which was passed as part of the John S. McCain Defense Authorization Act for Fiscal Year 2019.[308] ECRA was passed as part of a package of trade measures including the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) and the Anti-Boycott Act of 2018.[309] Together, these statutes sought to clarify the role of the Committee on Foreign Investment in the United States (CFIUS), an interagency committee chaired by the Treasury Department, to update Presidential authority to enact export controls on certain products and technologies, and to limit foreign boycotts of U.S. technology companies.[310]

---

304. CASEY, *supra* note 32.

305. INTERNET FREEDOM IN IRAN, *supra* note 301.

306. 50 U.S.C. § 4604 (a)(1), (b)(1) (2015).

307. *Id.* § 4605 (2015).

308. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 2232.

309. *Id.* at §§ 1701-1728; 1771-1793.

310. *See* House Committee on Financial Services Report on Foreign Investment Risk Review Modernization Act of 2018, H.R. 115-784 (2018).

Although the President's authorities in ECRA were stated somewhat differently than in the repealed sections 4604 and 4605, their scope is no less extensive.[311] ECRA states that:

> The national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specific activities of United States persons, wherever located, be controlled for the following purposes:
>
> (A) To control the release of items for use in—
>
> (i) the proliferation of weapons of mass destruction or of conventional weapons;
>
> (ii) the acquisition of destabilizing numbers or types of conventional weapons;
>
> (iii) acts of terrorism;
>
> (iv) military programs that could pose a threat to the security of the United States or its allies; or
>
> (v) activities undertaken specifically to cause significant interference with or disruption of critical infrastructure.[312]

The President is authorized to control "the export, reexport, and in-country transfer of items subject to the jurisdiction of the United States" in order to facilitate these policies.[313] ECRA specifically authorizes the Entity List as a means for carrying out this authority.[314]

The authorities granted under ECRA are subject to some of the limitations of IEEPA.[315] ECRA states that "[t]he authority under this part may not be used to regulate or prohibit under this part the export, reexport, or in-country transfer of any item that may not be regulated or prohibited under section 203(b) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)), except to the extent the President has made a determination necessary to impose controls under subparagraph (A), (B), or (C) of paragraph (2) of such section."[316] This exclusion refers to IEEPA's exception for donations intended to be used to relieve human suffering, which the

311. 132 Stat. 2232at §§ 1753-1754.

312. House Committee on Financial Services Report on Foreign Investment Risk Review Modernization Act of 2018, H.R. 115-784, (2018).

313. 132 Stat. 2232 at § 1752 (a).

314. *Id.* at §1754(a)(2), (5).

315. *Id.* at § (b).

316. *Id.* at §1754(b).

President can restrict under IEEPA only if they impair U.S. response to an emergency, were given under coercion, or would endanger U.S. military operations.[317]

There is no similar exclusion in ECRA relating to the "information or information materials" provision of IEEPA.[318] Therefore, it appears that ECRA's repeal of sections 4604 and 4605, and the limited IEEPA carve-out in ECRA, means that in ECRA Congress has given the President *broader* power to restrict the export of "information or information materials" than previously existed under IEEPA.[319] This means the President now arguably has broader powers under IEEPA to place an entity that transacts in "information or information" materials on the Commerce Department's Entity List, as well as related powers under ECRA itself to list an entity alleged to cause "significant interference with or disruption of critical infrastructure," including Internet infrastructure.[320]

In addition to ECRA and other trade-related amendments, the John McCain Defense Authorization Act of 2019 also contained a provision that directed the Secretary of Defense to "develop a process and procedures for limiting foreign access to technology through contracts, grants, cooperative agreements, or other transactions, when such limitation is in the interest of national security."[321] The Act further prohibits any federal executive agency from entering into or extending any contract to procure or obtain certain "covered telecommunications equipment," or from entering into, extending, or renewing a contract "with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any such system."[322] Any equipment produced by Huawei, ZTE, and several other Chinese companies that provide video surveillance equipment, is defined as "covered telecommunications equipment."[323] Although these provisions relate only to government procurement and contracts, they further reflect the U.S. policy effort to exclude Huawei.[324]

IV. EVALUATION AND PROPOSALS FOR REFORM

Despite alarms raised by some observers, President Trump's May 2019 Order almost certainly would be upheld by a court if challenged under

317. 50 U.S.C. §1702.
318. *Id*. § (b)(3).
319. 50 U.S.C §§ 4604-4605.
320. 132 Stat. 2232 at §1754(b).
321. *Id.* at § 885(a).
322. *Id.* at § 889(a).
323. *Id.* at § (f)(3).
324. *Id.* at § (a)(A)-(B).

IEEPA.[325] IEEPA authorities have been invoked against countries, individuals, and general categories of activities for over 40 years by Presidents of both parties in circumstances that seem to fall far short of a literal reading of the statute's emergency language.[326] With very few exceptions, the courts have not been willing to pry into Executive decisions under IEEPA.[327] In this context, President Trump's invocation of IEEPA against leading Chinese suppliers of 5G equipment–companies that, like every large Chinese enterprise, are intertwined with the Chinese government–was not exceptional.[328] But the use of IEEPA as a blunt instrument in this case, as in many other prior cases, demonstrates a need for legislative reform.

There are two related concerns arising from President Trump's May 2019 Order, one relating to public policy and the other relating to the rule of law. The public policy concern is about whether and to what extent Huawei 5G equipment poses a threat, the effectiveness of a ban or other response, and how any U.S. response to that threat relates to Internet governance and the goal of a secure, open global Internet.[329] The rule of law concern relates to the vast and sweeping powers delegated by IEEPA, as it has been interpreted by the Executive branch and by the courts from its inception until now.[330] These concerns show that, at least as it relates to Internet governance, IEEPA is too broad and should be reformed. This reform should recognize the need for greater international coordination of standards and production for Internet hardware layer infrastructure.

A. Internet Governance and The Policy Question of Huawei 5G Equipment

From its beginning, the Internet was conceived of as a set of protocols that were agnostic about hardware.[331] In the 1990's, Internet "exceptionalists" argued that the network would usher in a borderless world, "a world that is both everywhere and nowhere," a "civilization of the Mind in Cyberspace."[332] A more moderate paradigm, realist but still hopeful for a

325. See discussion *supra* Part III.D.

326. Tom Hals & Brendan Pierson, *Trump's Mexican tariffs test limits of U.S. emergency powers: legal experts*, REUTERS (May 31, 2019, 3:06 PM), https://www.reuters.com/article/us-usa-trade-mexico-legal-analysis/trumps-mexican-tariffs-test-limits-of-u-s-emergency-powers-legal-experts-idUSKCN1T12AB.

327. *Id.*

328. Rollet, *supra* note 21.

329. David Shepardson & Karen Freifeld, *Trump extends U.S. telecom supply chain order aimed at Huawei, ZTE*, REUTERS (May 13, 2020), https://www.reuters.com/article/us-usa-trade-china-trump/trump-extends-u-s-telecom-supply-chain-order-aimed-at-huawei-zte-idUSKBN22P2KG.

330. Casey, *supra* note 32, at 3.

331. *See* discussion *supra* Part III.A.

332. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

transnational future, then began to emerge. This paradigm focused on the three basic layers of the Internet: hardware, code, and content. The code layer was conceived of as a form of "law": the code protocols determined what kind of hardware could be used and what kind of content could be communicated.[333] If the code remained "open"–controlled by the community and not by any one government or private interest–the broadest possible range of devices could communicate with each other, and even more importantly, the broadest possible range of content would be permissible.[334]

Both the exceptionalist and moderate realist views of the Internet agreed with pioneers such as Robert Kahn that the hardware layer should be "dumb."[335] The routers and switches that implemented the internet protocols were not supposed to remember anything about the content they carried.[336] The "brains" of the network were the code protocols that enabled ideas to flow across the hardware.[337]

Other, more skeptical critics of this "exceptionalist" view of the Internet however, soon emerged.[338] Tim Wu and Jack Goldsmith noted that the hardware layer was not merely dumb or neutral because hardware is physically embedded in national territories.[339] As they suggested in 2008,

> It is not just that nations have the power to shape the Internet's architecture in different ways. It is that the United States, China, and Europe are using their coercive powers to establish different visions of what the Internet might be. In so doing, they will attract other nations to choose among models of control ranging from the United States' relatively free and open model to China's model of political control. The result is the beginning of a technological version of the cold war, with each side pushing its own vision of the Internet's future.[340]

Recent developments have proven Goldsmith and Wu largely correct.[341] Repressive regimes control Internet hardware infrastructure in order to

---

333. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999).

334. *See id.* at 107.

335. *See e.g.*, Kahn & Cerf, *supra* note 96, at 255.

336. *See e.g.*, *id.*

337. Keith Townsend*, As the 'brains' of SDN, network controllers enable agility,* TECHTARGET (Nov. 19, 2015), https://searchservervirtualization.techtarget.com/feature/As-the-brains-of-SDN-network-controllers-enable-agility.

338. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 184 (2008).

339. *Id.*

340. *Id.*

341. Adam Segal, *The Coming Tech Cold War With China Foreign Affairs,* FOREIGN AFFAIRS (Sept. 9, 2020), https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china.

control the content layer.[342] One common means by which this occurs is through control over Internet Exchange Points (IXPs).[343] An IXP is a hub through which a large amount of Internet traffic into and out of a city or region can be routed.[344] IXPs are common around the world and can boost network efficiency.[345] They can be run by governments, nonprofits, consortia of telecommunications companies, or some combination thereof.[346] For example, Linx is the London Internet Exchange, a not-for-profit organization that provides fast and accurate connections to its members through peering and other services.[347] But IXPs can also be used as a checkpoint for deep packet inspection and traffic throttling.[348] State-controlled IXPs in Iran, Saudi Arabia, and Russia, which generally must be used for broadband Internet traffic in those countries, afford those governments significant control over the content layer.[349]

There is no doubt that the hardware layer is not "dumb" and that it is fundamental to Internet freedom and security. If Huawei is intertwined with the Chinese government and/or military, the large-scale installation of its hardware in the 5G backbone is a significant problem. The problem is compounded because, as Nicholas Weaver has noted, "[s]abotage can be really, really subtle . . . [a] single microscopic difference: the addition of a small sabotage chip, and now you lose all your assurances."[350]

But is Huawei's equipment compromised? The answer to that question is frustratingly hard to pin down.[351] It is difficult to know with any certainty

342. Eda Keremoglu & Nils B Weidmann, *How Dictators Control the Internet: A Review Essay*, 53 COMP. POLITICAL STUD. 1690 (2020).

343. Keith Collins & Nikhil Sonnad, *How countries like China and Russia are able to control the internet*, QUARTZ (2016), https://qz.com/780675/how-do-internet-censorship-and-surveillance-actually-work/.

344. *What is an Internet Exchange Point? How do IXP's Work?*, CLOUDFARE, https://www.cloudflare.com/learning/cdn/glossary/internet-exchange-point-ixp/ (last visited Dec. 20, 2020) [hereinafter *What is an Internet Exchange Point?*].

345. *See id.*

346. *What is an IXP - Internet Exchange Point*, THOUSANDEYES, https://www.thousandeyes.com/learning/techtorials/internet-exchange-point (last visited Dec. 20, 2020).

347. *About the London Internet Exchange,* LINX, https://www.linx.net/about/ (last visited Dec. 20, 2020).

348. *See* What is an Internet Exchange Point?, *supra* note 345.

349. *See Freedom in the World 2020: Iran*, FREEDOM HOUSE, https://freedomhouse.org/country/iran/freedom-world/2020 (last visited Dec. 20, 2020); *Freedom in the World 2020: Russia*, FREEDOM HOUSE, https://freedomhouse.org/country/russia/freedom-world/2020 (last visited Dec. 20, 2020); *Freedom in the World 2020: Saudi Arabia Report*, FREEDOM HOUSE, https://freedomhouse.org/country/saudi-arabia/freedom-world/2020 (last visited Dec. 20, 2020). Freedom House is a government-funded non-profit, non-governmental organization.

350. *Is Huawei a Security Threat? Seven Experts Weigh In*, VERGE (Mar. 17, 2019) https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g.

351. *See, e.g.,* Tim Rühlig, *Who Controls Huawei? Implications for Europe*, UI Paper No. 5, May 2020, https://perma.cc/27GJ-PSAP; Curtis J. Milhaupt & Wentong Zheng, *Beyond Ownership: State Capitalism and the Chinese Firm*, 103 GEORGETOWN L. J. 665, 670 (2015); Margaret K. Lewis, *Who*

whether, or to what extent, Huawei is an arm of the Chinese State.[352] Huawei's founder, Ren Zhengfei, was a former officer of the People's Liberation Army, but Huawei claims it is 98.6% owned by its employees and is not directly linked to the government or the military.[353] However, the precise ownership structure of Huawei is opaque to Western observers.[354]

Likewise, the Chinese state exercises substantial regulatory control over all private Chinese companies, and some general Chinese national security laws might obligate private companies to cooperate with the state on national security matters.[355] The precise relationship between Huawei and the Chinese state, however, is also opaque.[356]

The U.S. Justice Department has attempted to demonstrate Huawei's ill intent through a series of criminal indictments, although none of these cases relate to compromised 5G equipment.[357] On December 1, 2018, Huawei's CFO Meng Wanzhou, who is also Ren Zhengfei's daughter, was arrested in Canada based on U.S. charges of financial fraud relating to evasion of U.S. sanctions against Iran by a U.S. Huawei subsidiary.[358] In January 2019, Huawei was indicted by the U.S. Justice Department in the Western District of Washington State for alleged theft of trade secrets from American telecommunications company T-Mobile and related charges.[359] In the context of the broader debate about Huawei 5G equipment, the trade secret theft charges sound almost comical: Huawei allegedly used consulting agreements and relationships with T-Mobile employees to obtain confidential information about "Tappy the Robot," a testing system that touches

---

Controls China, August 25, 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3600580.

352. *Id.*

353. *See* U.K. INTELLIGENCE & SEC. COMM., FOREIGN INVOLVEMENT IN THE CRITICAL NATIONAL INFRASTRUCTURE: THE IMPLICATIONS FOR NATIONAL SECURITY 4 (June 2013) (U.K), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Inf rastructure.pdf.

354. *See* Lindsay Maizland & Andrew Chatzky, *Huawei: China's Controversial Tech Giant*, COUNCIL ON FOREIGN RELATIONS (Feb. 12, 2020), https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

355. *See id.;* Christopher Ashley Ford, U.S. Asst. Sec'y of State, Remarks at the Multilateral Action on Sensitive Technologies (MAST) Conference (Sep. 11, 2019), *in* Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications, U.S. DEP'T OF STATE, https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/ (last visited Dec. 20, 2020).

356. Maizland & Chatzky, *supra* note 355.

357. *See e.g*., Indictment, *Huawei Device*, Cr. No. 19-010 at 5, 15; *Wanzhou Meng Charged*, *supra* note 11.

358. *Wanzhou Meng Charged*, *supra* note 11; Anna Fifield, *Huawei executive Meng Wanzhou seen as successor to father's tech empire*, WASH. POST (Dec. 6, 2018), https://www.washingtonpost.com/world/asia_pacific/huawei-executive-meng-wanzhou-seen-as-successor-to-fathers-tech-empire/2018/12/06/bd9f2e04-f969-11e8-8d64-4e79db3 3382f_story.html.

359. Indictment, *Huawei Device*, Cr. No. 19-010 at 5, 15.

smartphone screens.[360] The Justice Department also indicted Huawei in January 2019 for alleged wire fraud, money laundering, and violations of IEEPA.[361] Those charges relate to funds Huawei allegedly diverted to an Iranian subsidiary in violation of U.S. sanctions against Iran.[362]

As noted in Part I, effective May 16, 2019, Huawei was added to the Department of Commerce's "Entity List," which requires a finding that there is "reasonable cause to believe . . . that the entity has been involved, is involved, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States."[363] Companies on the Entity List require a special license for certain transactions.[364] The U.S. State Department has said Huawei's addition to the Entity List was prompted by the January 2019 cases filed by the Justice Department, but given the nature of those cases and the timing of the listing–one day after the May 15, 2019 Executive Order–that claim is risible.[365]

Notwithstanding incidents like the attempt to steal Tappy, or, more seriously, China's strategic relationship with Iran, no public sources have identified any specific malware, backdoors, or flaws in Huawei 5G equipment that could be traced to Chinese government or military involvement.[366] The most well-publicized alleged security incident that involved Huawei and the African Union has become a muddle.[367] The Western country that has given Huawei the most scrutiny, the UK, has been unable to develop a repeatable process to test Huawei's code, but has allowed limited Huawei 5G equipment.[368] Some private consultancies have identified

360. *See id.*

361. Superseding Indictment, *Huawei Technologies*, Cr. No. 18-457 at 5, 15.

362. *See id.*

363. 84 Fed. Reg. 43,493.

364. 15 C.F.R. § 744.11(a) (2020).

365. *See* Ford, *supra* note 356, (Part I, stating that "Huawei was nominated to be put on the Entity List by my bureau early this year, after it was indicted by the U.S. Justice Department in January 2019 for theft of trade secrets, attempted theft of trade secrets, conspiracy wire fraud, and obstruction of justice . . . . The first tranche of the Huawei parent and its affiliates (69 entities) were duly placed on the Entity List in May 2019.") Ashley Ford makes no mention in that speech of the May 15, 2019 Executive Order. But Ashley Ford does assert that "it seems to some of us to be nothing less than madness to allow Huawei to worm its way into one's next-generation telecommunications networks – just as it seems nothing less than madness to allow other Chinese technology giants to vacuum up and expatriate personal and consumer data and to control electronic commerce in free sovereign nations. . . . The world surely cannot afford to turn such critical capabilities over to technologists who are subject to control and manipulation by the Chinese Communist Party." *Id.,* Part VII.

366. Maizland & Chatzky, *supra* note 355.

367. Joan Tilouine & Ghalia Kadiri, *A Addis-Abeba, le siège de l'Union africaine espionné par Pékin*, LE MONDE (Fr.) (Jan. 26, 2018), https://www.lemonde.fr/208uawei208/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

368. HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD, ANNUAL REPORT, 2019, § 3.19 (UK) [hereinafter HCSEC 2019 ANNUAL REPORT].

flaws in Huawei equipment, but on their face, these seem due to sloppy manufacturing practices rather than cunning malice.[369]

1. The African Union Incident

In 2018, the French newspaper *Le Monde* reported that Huawei exfiltrated data over a period of five years from the African Union's new headquarters.[370] The AU headquarters' construction was funded and built by China as "China's gift to Africa."[371] The U.S. seized on this alleged incident as a prime example of Huawei's duplicity.[372]

The AU initially neither confirmed nor denied the data exfiltration but at first took some steps to limit Chinese access to its systems.[373] Huawei denied that any data theft occurred and stated that, "[o]ur involvement in the data center infrastructure for the AU headquarters in Ethiopia included two solutions, neither of which accessed customer or business data. The solutions provided to the AU was controlled, managed and operated by the organization's IT staff and Huawei had no access to AU data."[374] In May 2019, Huawei signed a new deal with the African Union to build 5G networks and other Internet infrastructure.[375] The African Union now denies that there was any data theft.[376]

Were the African Union allegations manufactured or exaggerated by the U.S. as part of an effort to tarnish Huawei's reputation and to justify hawkish policies towards Huawei and China? Is the African Union's renewed coziness with Huawei a deal with the devil for cheaper equipment? Do governments across Africa want to use Huawei gear, assisted by Huawei technicians, to spy on their citizens and political rivals?[377] Is the African Union's ongoing agreeable relationship with Huawei the result of corruption? Are parts of all these narratives true at the same time? We may never know.

---

369. *Id.*

370. Tilouine & Kadiri, *supra* note 368.

371. *See* Justin Sherman, *What's the Deal with Huawei and This African Union Headquarters Hack?*, NEW AMERICA (May 28, 2019), https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/whats-the-deal-with-huawei-and-this-african-union-headquarters-hack/; Erin Conway-Smith, *African Union's new Chinese-built headquarters opens in Addis-Ababa, Ethiopia*, WORLD FROM PRX (Jan. 28, 2012, 1:13 PM), https://www.pri.org/stories/2012-01-28/209uawei209-unions-new-chinese-built-hedquaters-opens-addis-ababa-ethiopia.

372. *See* Ford, *supra* note 356.

373. Sherman, *supra* note 372.

374. *Statement on Huawei's Work with the African Union*, HUAWEI (2020), https://www.huawei.com/us/facts/voices-of-huawei/statement-on-huaweis-work-with-the-african-union.

375. Tom Wilson, *Huawei and African Union boost relationship with deal*, FINANCIAL TIMES (May 21, 2019), https://www.ft.com/content/30ec5c54-83aa-11e9-b592-5fe435b57a3b.

376. *Id.*

377. *See* Joe Parkinson, et al., *Huawei Technicians Helped African Governments Spy on Political Opponents*, WALL STREET JOURNAL (Aug. 15, 2019), https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

2. The EU and the U.K.

Most EU countries have not followed the U.S.'s lead in banning or restricting Huawei 5G equipment.[378] The EU's "Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures," published in January 2020, notes the risk of "State interference through 5G supply chain" arising from "Third part[ies]," but concludes that the effectiveness of mitigation measures against this risk is "very high."[379] Proposed mitigation measures include certification and audit requirements, robust patch management, and access controls.[380] A regulatory authority could oversee and limit or exclude some suppliers or equipment that cannot meet these requirements, as well as promote diversification of third party equipment suppliers.[381] The COVID-19 crisis only weakened European sentiment against Huawei, and against China generally, because of the need to build out Internet capacity and because of a soft-power campaign by China to provide pandemic relief aid to Europe.[382]

The U.K. allowed Huawei equipment in its networks but, both pre- and post-Brexit, took steps to mitigate its risk.[383] In July 2020, however, under pressure from the Trump Administration, the UK reversed course and issued ban and rip-and-replace orders for Huawei 5G equipment.[384]

Even before the build out of 5G infrastructure, in 2010, the UK established the Huawei Cyber Security Evaluation Centre (HCSEC), a partnership between the UK government and Huawei to monitor the cybersecurity of Huawei Internet infrastructure equipment.[385] The HCSEC is

---

378. *See* Carisa Nietsche & Martijn Rasser, *Washington's Anti-Huawei Tactics Need a Reboot In Europe*, FOREIGN POLICY (Apr. 30, 2020, 12:19 PM), https://foreignpolicy.com/2020/04/30/210uawei-5g-europe-united-states-china/.

379. *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, EUROPEAN UNION NIS COOPERATION GRP. (2020), https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

380. *Id.*

381. *See id.* at 11-12, 21, Annex 1, tbl. 2.

382. *See id.*; *see* Philip Wen & Drew Hinshaw, *China Asserts Claim to Global Leadership, Mask by Mask*, WALL STREET JOURNAL (Apr. 1, 2020, 10:41 AM), https://www.wsj.com/articles/china-asserts-claim-to-global-leadership-mask-by-mask-11585752077?mod=searchresults&page=1&pos=1.

383. Annabelle Dickson & Laurens Cerulus, *Boris Johnson allows Huawei to build parts of UK 5G Network*, POLITICO (Jan. 28, 2020, 1:26 P.M.), https://www.politico.eu/article/boris-johnson-allows-huawei-to-build-parts-of-uk-5g-network/; Ian Levy, *Security, complexity, and Huawei; protecting the UK's telecoms networks*, National Cyber Security Centre (Feb. 22, 2019), https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uk s-telecoms-networks.

384. UK Press Release, "Huawei to be Removed from UK 5G Networks by 2027," July 14, 2020, available at https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027#:~:text=Following%20US%20sanctions%20against%20Huawei,by%20the%20end%20of%202027 [hereinafter UK Press Release].

385. *See* Amit Katwala, *Here's how GCHQ scours Huawei hardware for malicious code*, WIRED UK (Feb. 22, 2019), https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk; Levy, *supra* note 384.

reviewed by an Oversight Board that conducts annual reviews of the HCSEC's work.[386]

The HCSEC Oversight Board has published five annual reports on its work, running from 2015 through 2019.[387] The reports from 2015 through 2017 were generally positive.[388] In each of those years, the Oversight Board reported that "HCSEC fulfilled its obligations in respect of the provision of assurance that any risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated."[389]

The 2018 report, however, stated that, "[d]ue to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated."[390]

Although the 2017 report had offered a positive recommendation, it required Huawei to correct deficiencies in some product builds.[391] The recommendation particularly related to HCSEC's ability to certify that the source code of built products did not vary from the code in sample products provided for evaluation, a process the Oversight Board called "binary equivalence."[392] The 2018 report expressed concern that these deficiencies had not yet been resolved.[393]

The HCSEC's March 2019 report was much more negative than the 2018 report. It concluded that "the Oversight Board can only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term."[394] The March 2019 Report suggested that Huawei might never be able to establish binary equivalence:

> Without a process to show that the source code and build environments examined by HCSEC uniquely produce the binary deployed in the UK's networks, it is impossible to provide end-to-

386. HCSEC 2019 ANNUAL REPORT, *supra* note 369, at App. A; Levy, *supra* note 384.

387. HCSEC 2019 ANNUAL REPORT, *supra* note 369, at § 3.19.

388. *See generally*, HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD, ANNUAL REPORT, 2017, Summary (UK) [hereinafter HCSEC 2017 ANNUAL REPORT]; HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD, ANNUAL REPORT, 2016, Summary (UK) [hereinafter HCSEC 2016 ANNUAL REPORT]; HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD, ANNUAL REPORT, 2015, Summary (UK) [hereinafter HCSEC 2015 ANNUAL REPORT].

389. *Id.*

390. HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD, ANNUAL REPORT, 2018, Summary (UK) [hereinafter HCSEC 2018 ANNUAL REPORT].

391. HCSEC 2017 ANNUAL REPORT, *supra* note 389, at Summary.

392. HCSEC 2018 ANNUAL REPORT, *supra* note 391, at §§ 3.9, 3.16.

393. *Id.* at §§ 3.9-3.23.

394. HCSEC 2019 ANNUAL REPORT, *supra* note 369, at Summary, Part I.

> end assurance in the security and integrity of the products in use. Binary equivalence was seen to be an interim step to gaining that assurance in the face of Huawei's extremely complex build process.[395]

The Oversight Board stated in its 2019 Report that HCSEC had not yet been able to develop and deploy a process that could demonstrate binary equivalence.[396] The Board also noted that the effort to audit Huawei equipment was complicated because Huawei's build process "provides no end-to-end integrity, no good configuration management, no lifecycle management of software components across versions, use of deprecated and out of support tool chains (some of which are non-deterministic) and poor hygiene in the build environments, many of which cannot be easily recreated . . . "[397]

The Board also identified other typical cybersecurity and software engineering problems such as "unprotected stack overflows in publicly accessible protocols, protocol robustness errors leading to denial of service, logic errors, cryptographic weaknesses, default credentials and many other basic vulnerability types."[398]

Despite the HCSEC's March 2019 Report, along with pressure from the Trump Administration, the UK did immediately not ban all Huawei 5G equipment.[399] Before permitting the use of Huawei equipment, the House of Commons Science and Technology Committee conducted an evaluation of security risks, and "found no evidence . . . to suggest that the complete exclusion of Huawei from the UK's telecommunications network would, from a technical point of view, constitute a proportionate response to the potential security threats posed by foreign suppliers."[400] Nevertheless, the Science and Technology Committee recommended that Huawei equipment be excluded from the "core" of the UK telecommunications network, and Prime Minister Boris Johnson adopted that recommendation, along with a recommended cap limiting equipment of "high risk" vendors, including Huawei, to more than thirty-five percent of the periphery of the network.[401]

---

395. *Id.* at § 3.19.
396. *Id.*
397. *Id.* at § 3.21.
398. *Id.* at § 3.12.
399. Dickson & Cerulus, *supra* note 384.
400. Letter from Rt. Hon. Norman Lamb MP, Secretary of State for Digital, Cultural, Media, and Sport, to Rt. Hon. Jeremy Wright MP, Secretary of State for Digital, Culture, Media and Sport (July 10, 2019), https://www.parliament.uk/globalassets/documents/commons-committees/science-technology/Correspondence/190710-Chair-to-Jeremy-Wright-re-Huawei.pdf.
401. *Id.*; *New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity*, DEP'T FOR DIGITAL, CULTURE, MEDIA & SPORT (Jan. 28, 2020) (U.K.),

On July 14, 2020, however, the UK decided to prohibit the purchase of any new Huawei 5G equipment after December 31, 2020, and to require that all Huawei equipment be removed from UK 5G networks by the end of 2027.[402] The July 2020 decision also continued the ban on Huawei equipment in the core of the UK network. This abrupt change of course was attributed by the UK government to the effect of US sanctions against Huawei.[403] The UK National Cyber Security Centre determined that the US sanctions could disrupt Huawei's global supply chain, thereby damaging Huawei's ability to support its commitments in the UK and, in turn, endangering UK cybersecurity.[404] Many observers suggest the move was more about appeasing the Trump Administration than about increased supply chain or security risks.[405]

3. Private Consultancies

There are few publicly available technical reports from private consultancies about the security of Huawei 5G equipment.[406] A recent report by one such consultancy, Finite State, found that Huawei devices had more firmware vulnerabilities than other devices, including possible backdoor access points, "primarily due to the use of vulnerable open-source and third-party components."[407] Some Huawei devices also contained "hard-coded default credentials and hard-coded default cryptographic keys."[408] It is unclear from the Finite State report whether these vulnerabilities were intentionally created for nefarious purposes or merely the result of sloppy engineering.[409] The Finite State report notes that "[m]ost of the time, these backdoors are created unintentionally—they are engineering tools used during the development process," but that "intent is hard to discern."[410]

---

https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity.

402. UK Press Release, *supra* note 385.

403. *Id.*

404. *Id.*; *see also* NCSC Report, *Summary of the NCSC Analysis of May 2020 US Sanction* (July 14, 2020), available at https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction.

405. *See, e.g.,* Toby Helm, *Pressure from Trump Led to 5G Ban, Britain Tells Huawei*, THE GUARDIAN (July 18, 2020), available at https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei; Stephen Fidler and Max Colchester, *U.K. to Ban Huawei from its 5G Networks Amid China-U.S. Tensions* (July 14, 2020), available at https://www.wsj.com/articles/u-k-makes-u-turn-on-huawei-after-u-s-pressure-11594727179.

406. *Finite State Supply Chain Assessment*: *Huawei Technologies Co., Ltd.*, FINITE STATE, https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf (last visited Dec. 20, 2020).

407. *Id.* at 3.

408. *Id.* at 4.

409. *Id.* at 29.

410. *Id.*

B. Proposals for Reform

1. Policy and Internet Governance

As the discussion in Part IV.A above shows, the public policy concern about Huawei equipment in the 5G infrastructure are real but difficult to quantify.[411] It is reasonable to assume Huawei is intertwined in some ways with the Chinese state, particularly since its ownership structure is opaque and not subject to external audit.[412] The Chinese state maintains active cyber espionage and cyber war capabilities.[413] The U.K.'s experience shows that Huawei's coding and manufacturing processes open its products to vulnerabilities and that compliance is hard to verify.[414] There is thus no doubt that the U.S. is right to be concerned about large amounts of Huawei hardware in its 5G infrastructure.

Given the public policy concerns involving the use of Huawei equipment, the provisions in the McCain Defense Authorization Act of 2019, which restrict federal government agencies from acquiring such equipment or from using service providers that rely on Huawei equipment, are not unreasonable.[415] The question is whether, or under what circumstances, the U.S. federal government should have authority to determine whether *private* telecommunications providers can acquire and use Huawei equipment in networks that will comprise part of the *global* Internet backbone. This question is especially difficult to answer since Huawei equipment is already part of the global Internet, including in the EU and the UK.[416]

Some bipartisan proposals have been presented in Congress to address this concern, but unfortunately, they are both too narrow and too blunt.[417] The "Secure and Trusted Communication Network Act of 2019," sponsored by Representatives Pallone (D), Walden (R), Matsui (D), and Guthrie (R), would prohibit the use of federal funds to acquire telecommunications equipment from companies on a list to be maintained by the Federal Communications Commission.[418] The list would include any equipment produced or provided by Huawei that is:

---

411. *See* discussion *supra* Part IV.A.

412. *See supra* Part IV.A.

413. *See, eg.*, Kenneth Lieberthal & Peter W. Singer, *Cybersecurity and U.S.-China Relations*, BROOKINGS INST. (Feb. 2012), https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.

414. HCSEC 2019 ANNUAL REPORT, *supra* note 369, at § 3.12.

415. Pub. L. No. 115-232, §885(a), §888(f)(3)(A).

416. *See* Rita Liao, *Huawei says two-thirds of 5G networks outside China now use its gear*, TECHCRUNCH (June 25, 2019, 10:01 PM), https://techcrunch.com/2019/06/25/huawei-wins-5g-contracts/.

417. *See e.g.*, H.R. 4459; S. 1625.

418. H.R. 4459.

> capable of – (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; or (B) causing the network of a provider of advanced communications service to be disrupted remotely.[419] This definition covers all core virtualized routing equipment, but it might also include radio access network equipment at the network periphery that is controlled by software.[420]

The bill is therefore a blunt instrument, because it effectively would ban the use of federal funds on any Huawei 5G equipment.[421] At the same time, it is narrow, because it only relates to the use of federal funds.[422] "Federal funds" is defined in the bill to include the USF, other federal grants, subsidies, or loans, and any federally backed private loans for the deployment of communications networks.[423] The USF and the federal grant and loan programs referenced in the bill support broadband and wireless coverage in rural and low-income areas, schools, and libraries.[424] The bill would establish a reimbursement fund for small carriers that would be required to replace Huawei or other listed equipment.[425]

The "United States 5G Leadership Act of 2019," sponsored by Senators Wicker (R), Cotton (R), Warner (D), and Markey (D), is similar to the House "Secure and Trusted Communication Network" bill.[426] It lists Huawei, ZTE, and any other Chinese telecommunications provider as covered companies.[427] It includes a policy statement that the federal government should "support but not build or operate 5G networks" but that "communications networks deployed in the United States should not incorporate any hardware or software produced by . . . a covered company."[428] Additionally, the Senate bill would bar the use of the USF to purchase equipment from covered companies and would establish a replacement grant program, but it does not purport to bar the use of Huawei equipment in the U.S. 5G network outright.[429] Similar to the House bill, then, this Senate bill is both blunt and narrow.

---

419. *Id.* § 2(b)(2)(A-B).

420. *See* Leo Kelion, *Huawei: What is 5G's core and why protect it?*, BBC NEWS (Jan. 28, 2020), https://www.bbc.com/news/technology-51178376.

421. *See* H.R. 4459 § 2(b)(1)(A).

422. *Id.* § 3(1).

423. *Id.* § 7(7).

424. *See Universal Service Fund*, FED. COMMC'NS COMM'N, https://www.fcc.gov/general/universal-service-fund (last visited Dec. 20, 2020).

425. H.R. 4459 § 4.

426. S. 1625.

427. *Id.*, § 2(9).

428. *Id.*, § 3(3), (4).

429. *Id.*, §§ 4-5.

As the limits of these two bills demonstrate, the current U.S. policy of complete exclusion of Huawei seems Quixotic or Sisyphean—or maybe both at the same time.[430] This exclusion is difficult to accomplish through the law unless the federal government effectively controls a significant part of an important market and severely limits the property and contract rights of private companies—one reason why the most extensive effort to date is an "emergency" measure and not an ordinary legislative or regulatory action.[431] Further, the current policy can only affect parts of the Internet infrastructure within the U.S., rather than with the rest of the world, including our allies.[432] As a recent article in The Economist puts it,

> The problem with America's strategy is that it is trying to win today's 'tech cold war', as some call it, with yesterday's arsenal. In effect it is trying to build an impenetrable wall around Huawei by any means necessary. This is a fool's errand in a hyper-connected world in which technology and talent can flow freely. It only provides extra incentives for Huawei—and China—to become technologically self-sufficient.[433]

The bigger governance issue here concerns how industry-led technical standards bodies could interface with an internationally-coordinated legal regime concerning cybersecurity.[434] 5G technical standards are set by the 3rd Generation Partnership Project (3GPP).[435] 3GPP is comprised of seven "Organizational Partners" and twenty "Market Representation Partners."[436] The Organizational Partners are trade associations from Japan, the U.S., China, Europe, India, and South Korea, mostly comprised of private companies, but also in some cases including government and university representation.[437] The Market Representation Partners are trade associations

430. Thomas D. Lairson, et al., *Why the US Campaign Against Huawei Backfired*, THE DIPLOMAT (May 13, 2020), https://thediplomat.com/2020/05/why-the-us-campaign-against-huawei-backfired/.

431. Rosie Perper, *Huawai slams Trump's 'unreasonable' ban, saying that the move will only harm US interests in its own 5G rollout*, BUSINESS INSIDER (May 16, 2019, 12:06 AM), https://www.businessinsider.com/huawei-responds-trump-china-tech-national-emergency-ban-2019-5.

432. Lairson, et al., *supra* note 431.

433. *Open Standards, not sanctions, are America's best weapon against Huawei*, ECONOMIST (Apr. 8, 2020), https://www.economist.com/leaders/2020/04/08/open-standards-not-sanctions-are-americas-best-weapon-against-huawei (authors for The Economist are anonymous).

434. *Id.*

435. *See About 3GPP*, 3GPP, https://www.3gpp.org/about-3gpp/about-3gpp (last visited Dec. 20, 2020).

436. *See Partners*, 3GPP, https://www.3gpp.org/about-3gpp/partners (last visited Dec. 20, 2020).

437. *Id.*

in particular sectors, such as the 5G Infrastructure Public Private Partnership.[438]

This kind of industry-led, ground-up standards setting method is vital to communications and Internet infrastructure. It keeps standards open so that the network core can integrate seamlessly, while allowing for competition and innovation in standard-compliant core devices as well as in network edge devices and services.[439] But it is not a process with much public accountability, nor can it effectively manage concerns relating to national and international security. These accountability and security governance gaps leave room for the kinds of gamesmanship we now see involving China, Huawei, and the United States.[440]

One very positive aspect of the "United States 5G Leadership" bill in the Senate is a provision that would increase U.S. participation "at international forums that set standards for 5G networks and for future generations of wireless communications networks," including 3GPP, the ISO, and the ITU.[441] Not only is it wise for the U.S. to participate more fully in standard-setting, it is also long past time for the U.S. to take the lead in developing an international treaty regime relating to cybersecurity and cyber war.[442] Such a treaty, of course, cannot, and should not, replace the national security and cybersecurity apparatus of nation states. But like the U.N. Charter section relating to traditional war, it can provide a layer of diplomacy and dispute resolution that can help mitigate catastrophic events, and a public forum for

---

438. *See Market Representatives,* ETSI, https://webapp.etsi.org/3gppmembership/Results.asp?SortMember=Name&DirMember=ASC&SortPartner=Name&DirPartner=ASC&Market=on&SortMarket=Name&DirMarket=ASC&SortObserver=Name&DirObserver=ASC&SortGuest=Name&DirGuest=ASC&Name=&search=Search (last visited Dec. 20, 2020); *5G Public Private Partnership Website*, 5GPPP: THE 5G PUBLIC PRIVATE PARTNERSHIP, https://5g-ppp.eu/5g-infrastructure-association/ (last visited Dec. 20, 2020).

439. *See About 3GPP*, *supra* note 436.

440. *See infra* Part IV.A.

441. S. 1625 § 9(a).

442. *See* U.N. General Assembly Resolution, *Developments in the Field of Information and Telecommunications in the Context of International Security*, G.A. Res. 27/32 (Dec. 5, 2018). The details of such a possible treaty regime are beyond the scope of this paper, but it can be outlined as follows. The treaty regime should not relate to specific technological or code standards, except to set high-level policy goals relating to security. *See* U.N. OEWG, *Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*, §(C), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf. The job of defining detailed standards belongs with the kinds of ground-up standards-setting bodies where that work now resides. *Id*. at §(B)(19). Rather, the treaty body should develop principles for transparency and accountability, common protocols for security testing, a forum for dispute resolution, and mechanisms for sanctions. *Id*. at §(C)(32). Some steps in this direction are already being taken by the United Nations Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, although the current focus of discussion remains on existing international law instruments combined with voluntary, non-binding norms. *Id.* at §(A)(6).

discussing seemingly intractable problems such as whether Huawei 5G network components can be trusted.[443]

2. IEEPA and Export Control Reform

As noted in Part I, in response to different concerns and in tension with policy choices regarding Huawei, some lawmakers have advanced proposals to amend IEEPA.[444] The ARTICLE ONE Act, proposed by a bipartisan group of Senators, would automatically terminate any emergency declaration made under the National Emergencies Act after 30 days unless Congress affirmatively votes to extend the emergency.[445] The ARTICLE ONE Act also would adopt a similar provision to the Democrat-sponsored bills that would exclude the authority to impose duties or quotas on articles entering the United States from the President's IEEPA powers.[446] However, the ARTICLE ONE Act would allow the President to exclude imports from a given country entirely, consistent with historic trading with the enemy authorities.[447]

In February 2020, Representative Ilhan Omar introduced a package of bills she titled the Pathway to PEACE (Progressive, Equitable, and Constructive Engagement) that included the "Congressional Oversight of Sanctions Act" (COSA).[448] Rep. Omar's proposed COSA bill states that "successive Presidents from both parties have used the authority granted by the International Emergency Economic Powers Act . . . and the National Emergencies Act . . . to declare national emergencies that do not meet the threshold of 'unusual and extraordinary threat[s] to the national security and foreign policy of the United States.'"[449] The bill would require a joint resolution of Congress to approve IEEPA sanctions within sixty days of being in session after sanctions are announced.[450] The bill was praised by groups ranging from Human Rights Watch to the Cato Institute.[451]

Bills such as the ARTICLE ONE Act and COSA would provide additional Congressional oversight of emergency declarations in general, which is good policy.[452] The provisions in those bills that would require Congressional action to extend a state of emergency declared by the

443. *See* U.N. Charter art. 33, ¶ 1.
444. S. 2413.
445. S. 764 § 202(a)(2).
446. *Id.* § 4.
447. *Id.* § (2).
448. H.R. 5879; *Pathway to PEACE*, *supra* note 29.
449. H.R. 5879 § 3.
450. *Id.* § 4(a)(6).
451. *See Pathway to PEACE*, *supra* note 29.
452. *See* S. 764 § 202(a)(2); H.R. 5879.

President, however, might constitute an improper legislative veto.[453] In *INS v. Chadha*,[454] the Supreme Court held that a legislative veto violates Constitutional separation of powers.[455] The statutory provision in *Chadha* allowed either branch of Congress to pass a resolution revoking the Attorney General's decision to suspend deportation of a deportable alien.[456] This is different than the provisions in the ARTICLE ONE and COSA bills, by which the Executive's declaration of a state of emergency would expire after a set period without further Congressional action.[457] The reasoning in *Chadha* could suggest, however, that the kind of "Legislative pocket veto" reflected in the ARTICLE ONE and COSA bills also violates the separation of powers.[458] Having delegated discretion to the President to declare a state of emergency, Congress might not be Constitutionally empowered to assert further control over that declaration through a veto by inaction.[459]

This kind of question suggests that, whatever broader reform over emergency declarations in general Congress might enact, the specific authorities available to the President under IEEPA, and relatedly under ECRA, should be narrowed. At the same time, Congress should develop a more rational and regular approach to the potential threats posed by compromised Internet backbone equipment. My proposals for IEEPA reform, and for related export control reform, favor an open, global Internet with a loose layer of formal international governance relating to cybersecurity.[460] IEEPA gives the American President alone too much control over U.S. national Internet infrastructure, which contributes to the prospect of fractured regional networks. The large and important policy decisions inherent in the build and maintenance of U.S. Internet infrastructure should not be decided by Executive Order without more control by the Legislative and Judicial branches.

This checks and balances problem for the rule of law is compounded exponentially by the need to invoke a "national emergency" that poses an

453. *See* S. 764 § 2; H.R. 5879 § 4.
454. INS v. Chadha, 462 U.S. 919 (1983).
455. *Id.* at 959.
456. *Id.* at 994.
457. *See* S. 764 § 202(a)(2); H.R. 5879.
458. A similar issue has been raised in connection with the War Powers Resolution of 1973, 50 U.S.C. § 1541 (the "WPR"). The WPR requires that U.S. forces be removed from hostilities within sixty days if Congress does not declare war, issued an authorization for the use of military force, or extended the time period, unless Congress is physically unable to meet as a result of armed attack. WPR, *supra* note 139, at 1544(b). The WPR also allows Congress to direct the President to remove armed forces from hostilities absent a declaration of war or specific statutory authorization by concurrent resolution. WPR, *supra* note 139, at § 1544(c). Many scholars believe these provisions are unconstitutional under *Chadha*. *See* James A. Baker III and Warren Christopher, *The War Powers Commission Report* 23, University of Virginia Miller Center for Public Affairs (2008).
459. *See* 50 U.S.C. § 1701(a).
460. *See infra* Part IV.B.2.

"unusual and extraordinary threat" to the United States to trigger IEEPA.[461] A state of emergency is a condition that suspends the ordinary operation of the law and gives the government more control over the people.[462] Emergency declarations should be rare and limited. Ordinary policy decisions, taken in the context of ordinary risks and threats, should be arrived at by ordinary means.

In particular, the "informational materials" exclusion in IEEPA should be expanded to cover Internet and other telecommunications infrastructure.[463] The exception for EAR exclusions should also be clarified to state that IEEPA cannot be used as a basis for excluding transactions in Internet and other telecommunications infrastructure equipment through the Entity List without a more robust technical review process.[464] Finally, the export control statute should be amended to clarify that basic Internet infrastructure components should be evaluated separately before any action is taken under the "critical infrastructure" provision in ECRA.[465] These changes would not prevent the U.S. from placing Huawei on the Entity List or from excluding some or all Huawei components from the U.S. 5G infrastructure. They would, however, require a more robust review process, under conditions of the ordinary rule of law, rather than the kind of expedited, shoot-a-blunderbuss-from-the-hip approach that suffices under a state of emergency.

To implement these reforms, Congress should establish a U.S. standards body that could provide a way to certify Internet equipment on measures relating to performance, privacy, security, and reliability. Equipment that comprises critical Internet infrastructure would only be available for sale and use in the United States if it is certified as reasonably secure and reliable.[466] The "reasonably secure and reliable" standard could be developed through administrative rules and guidance based on scientific testing, as is the case, for example, with the FDA's standards for the sale of medical devices.[467] Medical devices are subject to different degrees of rigor in safety and efficacy testing depending on the level of risk a class of device might pose to human

461. *See* 50 U.S.C. § 1701(a).

462. *See, e.g.,* GIORGIO AGAMBEN, THE STATE OF EXCEPTION 1 (Kevin Attell trans., 2005); GIORGIO AGAMBEN, HOMO SACER: SOVEREIGN POWER AND BARE LIFE 15 (Daniel Heller-Roazen trans., 1998); CARL SCHMITT, POLITICAL THEOLOGY: FOUR CHAPTERS ON THE CONCEPT OF SOVEREIGNTY 12 (George Schwab trans., 1985); Evan J. Criddle & Evan Fox-Decent, *Human Rights, Emergencies, and the Rule of Law*, 34 HUM. RTS. Q. 39, 40 (2012); Bruce Ackerman, *The Emergency Constitution*, 113 YALE L.J. 1029, 1030 (2004).

463. *See* 50 U.S.C. § 1702(b)(3).

464. *See id.*

465. Export Control Reform Act, H.R. 5040, 115th Congr., § 102(1)(A)(v) (2018).

466. *See generally* H.R. 4459.

467. *See Overview of Device Regulation*, U.S. FOOD AND DRUG ADMIN., https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation (last visited Dec. 20, 2020).

health and safety.[468] Internet infrastructure devices likewise could be classified by potential risk and subject to different levels of certification.[469] Perhaps some devices would require the kind of "binary equivalence" tests the UK HCSEC tried to obtain from Huawei, and perhaps if Huawei could not pass such tests some of its equipment could be excluded from U.S. networks.[470] In any event, the process would be subject to ordinary rulemaking procedures, with accountability to Congress and with judicial oversight at least of the responsible agency's interpretation of and adherence to the statute.[471]

V. CONCLUSION

President Trump's May 2019 Executive Order aimed at Huawei 5G equipment likely was within the authority delegated to him by Congress under IEEPA, in conjunction with the changes made to export controls in 2018 by ECRA.[472] This action, however, illustrates an ongoing problem with IEEPA. IEEPA undermines the rule of law because it has for decades been used as a tool of "ordinary" policy making rather than for its intended purpose as a rare and limited emergency power.[473] The problem is compounded in relation to global Internet governance.

The U.S. President alone should not hold so much control over the future shape of the Internet. Existing proposals to reform IEEPA are well-intentioned but likely contain unconstitutional legislative veto provisions.[474] Meanwhile, Congress is moving aggressively to target Huawei and some other Chinese telecommunications companies in ways that are blunt and counterproductive.[475] Both IEEPA and U.S. export control law should be amended to establish a vigorous process for testing the security and reliability of Internet infrastructure components against a backdrop of U.S. leadership in coordinated international Internet governance. Such a framework can help address reasonable concerns about Huawei and other Chinese influence in the U.S. and international Internet backbone through the operation of the ordinary rule of law and in pursuit of the policy goal of a secure, open, global Internet.[476]

---

468. For a description of this process, *see ID.*

469. *See id.* (whereby devices are classified as Class I, II, or III depending on the regulatory requirements needed to be met).

470. *See* HSSEC 2018 ANNUAL REPORT, *supra* note 391, at §§ 3.9, 3.16.

471. *See*, *A Guide to the Rulemaking Process*, OFFICE OF THE FED. REGISTER, https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf (last visited Dec. 20, 2020).

472. H.R. 5040.

473. *See infra* Part III.B.

474. *See infra* Part IV.B.2.

475. *See infra* Part I (noting specifically the ARTICLE ONE Act and COSA Act).

476. *See infra* Part IV.B.1.

APPENDIX A: ORIGINAL EXECUTIVE ORDERS AND OTHER PRESIDENTIAL ACTIONS UNDER IEEPA

Date	Order	President	Country/ Topic
11/14/1979	12170	Carter	Iran / hostage crisis / Iranian government assets
10/14/1983	12444	Reagan	Countries and Persons Threatening United States Export Regulation Upon Expiration of the Export Administration Act of 1979 / Export Control Act expired, continues those authorities by ExOrd
5/1/1985	12513	Reagan	Nicaragua / all imports and exports
9/9/1985	12532	Reagan	South Africa / apartheid / loans to government of South Africa, goods or technology to South Africa government agencies (police); no assistance to firms that don't adhere to apartheid

Date	**Order**	**President**	**Country/ Topic**
1/7/1986	12543	Reagan	Libya / goods of Libyan origin, exports to Libya,
4/8/1988	12635	Reagan	Panama / Noriega / Panama government property
8/2/1990	12722	George H.W. Bush	Iraq / all goods and services of Iraqi origin
8/2/1990	12723	George H.W. Bush	Kuwait / invasion of Kuwait / Kuwait government property
11/16/1990	12735	George H.W. Bush	Countries and Persons Proliferating Weapons of Mass Destruction / export controls
10/4/1991	12775	George H.W. Bush	Haiti / Haitian government assets

Date	**Order**	**President**	**Country/ Topic**
5/30/1992	12808	George H.W. Bush	Western Balkans (Serbia and Montenegro) / government property
9/26/1993	12865	Clinton	Angola / war / arms
1/23/1995	12947	Clinton	Countries and Persons Committing or Supporting Terrorism / property, transactions of certain persons and organizations
10/21/1995	12978	Clinton	Colombia / narcotics trafficking, violence / property, transactions of certain persons
5/20/1997	13047	Clinton	Burma / repression of democratic opposition / new investment
11/3/1997	13067	Clinton	Sudan / human rights violations / Import, export Sudan
7/4/1999	13129	Clinton	Afghanistan

Date	**Order**	**President**	**Country/ Topic**
6/21/2000	13159	Clinton	Russia / nuclear proliferation /
1/18/2001	13194	George W. Bush	Sierra Leone / rough diamonds
5/22/2001	13213	George W. Bush	Liberia / United Revolutionary Front diamond trade from Sierra Leone through Liberia / rough diamonds
3/6/2003	13288	George W. Bush	Zimbabwe / democratic process / specific persons
5/11/2004	13338	George W. Bush	Syria / terrorism, occupation of Lebanon, WMD / munitions, air carriers, persons designated by SecTreas and SecState
2/7/2006	13396	George W. Bush	Cote d'Ivoire / civilian killings, human rights abuses / property, transactions of certain persons
6/16/2006	13405	George W. Bush	Belarus / elections / human rights abuses / contributions, donations

Date	**Order**	**President**	**Country/ Topic**
10/27/2006	13413	George W. Bush	Democratic Republic of the Congo / violence and atrocities / property, transactions of certain persons
8/1/2007	13441	George W. Bush	Lebanon / persons endangering Lebanon's democratic government / property, transactions of certain persons
6/26/2008	13466	George W. Bush	North Korea / weapons grade nuclear material
4/12/2010	13536	Obama	Somalia / piracy / property, transactions of specific persons
7/24/2011	13581	Obama	Transnational Criminal Organizations / specifically designated or determined by SecTreas and SecDef
5/16/2012	13611	Obama	Yemen / persons who threaten peaceful transition of power
3/6/2014	13660	Obama	Ukraine / persons interfering with democratic process in Ukraine

Date	Order	President	Country/ Topic
4/3/2014	13664	Obama	South Sudan / violence, child soldiers / persons designated by Sec Treas, SecState
5/12/2014	13667	Obama	Central African Republic / breakdown of law and order / child soldiers / property of certain persons / donations, contributions / immigration of certain persons
3/8/2015	13692	Obama	Venezuela / human rights / specific persons
4/1/2015	13694	Obama	Persons Engaging in Significant Malicious Cyber-Enabled Activities / property, transactions of persons engaged in cyber attacks as determined by SecTres, AG, SecState / immigration of such persons
11/22/2015	13712	Obama	Burundi / killing civilians, political repression / immigration of certain persons / property or interests of certain persons / donations, contributions

Date	**Order**	**President**	**Country/ Topic**
1/13/2017	13761	Obama	Sudan; Revoking / waiving sanctions
8/24/2017	13808	Trump	Venezuela; human rights; financial transactions
9/20/2017	13810	Trump	North Korea; nuclear tests; air and sea traffic, funds; immigration
12/20/2017	13818	Trump	Persons Involved in Serious Human Rights Abuse or Corruption / property, transactions of specific persons
8/6/2018	13846	Trump	Iran; re-imposing old sanctions, issuing new sanctions, weapons proliferation
9/12/2018	13848	Trump	Unspecified; election interference
11/27/2018	13851	Trump	Nicaragua human rights abuses; Economic transactions, immigration
5/15/2019	13873	Trump	Foreign Technology

Date	**Order**	**President**	**Country/ Topic**
8/6/2020	13942	Trump	TikTok
6/6/2020	13943	Trump	WeChat
1/5/2021		Trump	Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, WPS Office