National Security, Trade, and China: Risks and Responses in the Internet Age

By Ronald A. Cass

International & National Security Law Practice Group

About the Author:

Hon. Ronald A. Cass is Dean Emeritus, Boston University School of Law; former Commissioner and Vice-Chairman, U.S. International Trade Commission; former United States Representative Member, Panel of Mediators, International Center for Settlement of Investment Disputes, World Bank; Senior Fellow, International Centre for Economic Research. The views expressed in this paper are Dean Cass's alone, not those of any entity with which he is affiliated.

Note from the Editor:

The Federalist Society takes no positions on particular legal and public policy matters. Any expressions of opinion are those of the author. Whenever we publish an article that advocates for a particular position, we offer links to other perspectives on the issue, including ones opposed to the position taken in the article. We also invite responses from our readers. To join the debate, please email us at info@fedsoc.org.

Other Views:

• John Naughton, *Trump's Banning of Huawei Could Be the Beginning of the Biggest Trade War Ever*, The Guardian, June 2, 2019, *available at* https://www.theguardian.com/commentisfree/2019/jun/02/trump-banning-huawei-beginning-of-biggest-trade-war-ever-united-states.

• Russia — Measures Concerning Traffic in Transit (DS512), Summary of GATT Dispute Resolution Proceeding (May 8, 2019), *available at* https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm.

National security concerns cut across typical arguments about trade policy. Typical arguments concentrate on effects on domestic businesses, workers, and consumers from changes in import flows—flows that are determined by differences between national pay scales, regulatory regimes, and saving and consumption priorities. In contrast, national security concerns look to specific effects on national capacity to protect against perils with potential for broad, national impact.

One increasingly discussed security focus today concerns imports from China, notably imports of certain equipment in the information and communication technology (ICT) sector. News commentary has been mostly confined to one or two firms' products. Yet the combination of China's political system, economic structure, and export orientation poses broader threats, which are magnified in a world in which national security is inextricably connected to ICT, both because of its significance to a range of economic, financial, and ordinary daily functions and because of its integration with military hardware and operations. While some aspects of this threat may be controlled through decisions on government procurement and investment, other aspects require constraints on imports of a broader set of products. In addition to products from Huawei and ZTE (the Chinese firms most frequently discussed in connection with security risks), products of other commercially successful firms in the ICT sector—such as China Mobile, Lenovo, and Lexmark—would be on the list.[1]

This paper reviews the risks posed by Chinese imports, the conditions leading to these risks, the firms and products that could pose these risks, and ways in which those risks might best be addressed, particularly through invocation of Section 232 of the Trade Expansion Act of 1962.

I. Trade Basics: Economics and Security

Trade expands choices, enhances competition, raises standards of living, and increases wealth for both trading parties.[2] Anyone who recalls a time when people were limited to fruits and vegetables that were grown nearby appreciates the benefits of access to a worldwide market that can ship products from warmer climates to markets that are experiencing winter, and anyone who grows these products can appreciate having consumers in other markets eager to buy their goods. Having the broadest possible choice set of products that suit each person's tastes, interests, and budget is easy to like. That is why trade's overall effects are strongly positive, even though it undeniably can have negative

1 *See infra,* section III.

2 *See, e.g.*, Milton Friedman, Capitalism and Freedom 13 (1962) (making the general case for exchanges between willing participants). For explanations of the fundamentals of international trade, including the principal driving forces behind trade flows, see, e.g., Jagdish N. Bhagwati & T.N. Srinivasan, Lectures on International Trade chaps. 1–8 (1983).

effects on some businesses, workers, and communities. Over the past seventy-plus years, reductions in global trade barriers, largely associated with the General Agreement on Tariffs and Trade (GATT), have helped expand global trade at roughly half again the pace of global GDP and contributed to major increases in income and declines in poverty.[3]

Most arguments for trade restrictions rooted in concerns about economic dislocation elevate transient, concentrated effects associated with any change in economic factors—primarily changes in costs of production, technology, and consumer tastes—above broader, longer-term gains to society; such arguments have played out in different terms over more than two centuries. But careful scholars, including those known as proponents of managed trade in specific settings, recognize the strong, general case for open trade and reasons for caution in restricting it.[4]

One set of concerns, however, is different and has been recognized as a special ground for setting aside normal trade rules. Article XXI of the GATT (brought forward into the World Trade Organization (WTO) framework) provides:

> Nothing in this Agreement shall be construed . . . . (b) to prevent any [member country] from taking any action *which it considers necessary for the protection of its essential security interests* . . . (iii) taken in time of war or other emergency in international relations . . .[5]

The precise meaning of the GATT language is debated, especially the degree to which the italicized phrase precludes WTO dispute resolution bodies from second-guessing a member state's judgment of its security needs. But the point of the provision is clearly to mark out a special limitation on interference with a nation's protection of its security, including self-protection through otherwise prohibited restrictions on trade.

II. Risks to U.S. National Security

Communications among government personnel engaged with national security issues always have been sensitive, high-priority targets for infiltration by actual and potential opponents. They have also been high-priority for protection through encryption and other steps to reduce opportunity for interception, translation, and defensive or retaliatory maneuvers. For example, breaking the German military's codes used in its Enigma machines often is credited as contributing significantly to Allied forces' success in defeating Nazi Germany in World War II.[6]

In today's world, communications are even more important and far more numerous and constant. Their importance is partly tied to the vast increase in use of electronic transactions—including, but not limited to, in the domain of finance—in place of what formerly required physical operations. Further, much of what still takes place in the physical realm—such as driving a car or a tank, piloting a plane, or sending missiles toward targets—is governed by instructions that are communicated at a distance or by processes taking place within physically separate equipment pursuant to integrated circuits' memory and computing processes.[7]

Any process that incorporates computer chips and any process that occurs at the direction of an electronically transmitted instruction is potentially vulnerable to cyber-espionage and cyber-warfare.[8] In the age of the internet, that covers virtually all of our important, our everyday, and our highly sensitive functions. Diplomatic, strategic, and tactical communications and operations necessary to national security are vulnerable to concentrated hacking efforts, potential sources of leakage of communications, and possible weaknesses in the internal instruction sets that govern computing functions.[9] Every nation's protection depends on the robustness of the insulation around these electronic operations.

All of us are familiar with weaknesses in the way that data are collected, stored, and transmitted. When one of our credit cards is hijacked, it could be because of a major leak of data from a company we've done business with, or a thief could have stolen the information necessary to access our accounts from a single transaction at a terminal in a store. Even though we are notified that our data may have been taken and cancel the card, we are left to wonder when the theft occurred and what damage may have been done that will not surface right away. Our nation's secret communications and the security of critical equipment may be subject to even greater risks, as the resources trained on intercepting or disrupting those functions may be far greater and far more focused than those deployed in the commercial realm.

In addition to the risks to national security from efforts to exploit weaknesses in government equipment, software, and communications, serious security risks attach to equipment, software, and communications of government contractors and others with whom the government does business. The risks include not only those associated with direct efforts to exploit weaknesses in communicating and computing, but also those from latent or even unknown weaknesses in communicating and computing resources that interface with government directly or as links in a larger chain. A "backdoor" may be built into commercially successful software or embedded in equipment that is widely

3 *See, e.g.*, Mark Dean, *Why Has World Trade Grown Faster than World Output*, Bank of England Q. Bull. 310–17 (Autumn 2004).

4 *See, e.g.*, Jagdish Bhagwati, Protectionism 24–42 (1988); Paul R. Krugman, *Is Free Trade Passé?*, 1 J. Econ. Perspectives 131, 138–43 (1987).

5 General Agreement on Tariffs and Trade art. XXI, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194 [hereinafter GATT] (italics added).

6 *See, e.g.*, Jack Copeland, *Alan Turing: The Codebreaker Who Saved "Millions of Lives,"* BBC, Jun. 19, 2012, *available at* https://www.bbc.com/news/technology-18419691.

7 *See, e.g.*, United States Government Accountability Office, Report GAO-16-350: *Vehicle Cybersecurity* (March 2016), *available at* https://www.gao.gov/assets/680/676064.pdf.

8 *See, e.g.*, *id.* (This message was emphasized throughout the GAO report, explaining GAO's decision to subtitle its report "DOT and Industry Have Efforts Under Way, But DOT Needs to Define Its Role in Responding to a Real-World Attack.").

9 *See, e.g.*, Center for Strategic & International Studies, *Significant Cyber Incidents*, *available at* https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents; Natalian Drozdiak, *EU Investigating Report of Massive Hacking of Diplomatic Cables*, Bloomberg, Dec. 19, 2018, *available at* https://www.bloomberg.com/news/articles/2018-12-19/eu-investigating-report-of-massive-hacking-on-diplomatic-cables.

available in ordinary consumer markets, allowing access to highly sensitive information stored on computing or communications equipment directly or remotely, or possibly providing a key to opening other connections leading to such information.[10] Given the number of governments and other entities around the world with interest in discovering information held by the United States or in restricting U.S. military, diplomatic, or other operational options, it is entirely appropriate for the U.S. government to adopt a highly protective stance toward reducing these risks.

III. China Trade's Security Risks

Many nations and many entities pose risks. China and Chinese-origin products, however, pose special risks because a combination of several factors increases the possibility of the products' use for purposes harmful to U.S. security.[11]

The first factor is China's announced goal of dominance in numerous fields, including ICT, that are critical to security, intra-government communications, and military effectiveness.[12] China has made no secret of its intentions in this respect and has made extensive investments in support of these goals.

Second, China has made broad and intense investments in espionage, both in China and abroad, notably including cyber-espionage.[13] It has extensive networks of espionage assets, human and technical, deployed in China and increasingly overseas.[14] This underlies cautions issued by the U.S. government to officials and business executives traveling in China and having on-going communications with Chinese citizens.[15]

Third, China's economy, although still evolving, is not driven by large numbers of small, independent, privately-run firms. Instead, unlike most of the major world economies, it depends to a very large degree on state-owned enterprises (SOEs) and firms that, while not formally state-owned, rely for funding on major (often controlling) investments from the Chinese government. There are estimated to be more than 150,000 SOEs in China, including in some of China's largest enterprises, apart from government investments in many if not most nominally private enterprises that are engaged in substantial economic activity.[16] These enterprises often are led by former government functionaries, including high-ranking members of China's communist party and former military officers.[17] While these officials may no longer have direct roles in government, there is at the least reasonable suspicion of their continuing ties to and responsiveness to the government.[18]

Fourth, also in contrast to most successful and almost all advanced national economies, China's political regime is both openly authoritarian and insulated against formal democratic checks on its exercise of government power.[19] Although for at least a quarter-century China loosened controls over various economic decisions and activities, China's government under President Xi has been reasserting control over many aspects of China's economic activity. As one observer reported, "Since 2012, private, market-driven growth has given way to a resurgence in the role of the state."[20] The reassertion of control over the economic sector has gone hand-in-hand with assertion of greater control over other activity, including renewed restraints on public speech

10 *See, e.g.*, Bob Flores, *The Dangers of Backdoor Software Vulnerability and How to Mitigate Them*, Cyber Defense (May 7, 2019), *available at* https://www.cyberdefensemagazine.com/the-dangers-of-backdoor-software-vulnerabilities-and-how-to-mitigate-them/ (observing that "as the complexity and scale of application development has advanced, and the components and dependencies have expanded . . . the attack surface [for backdoors] is significantly broader" and the decreasing cost of computing and storage dramatically facilitate cyber-attack options).

11 *See, e.g.*, U.S. House of Representatives Permanent Select Comm. on Intelligence, Investigative Report: The U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Cong., 2d Sess. (Oct. 8, 2012) (House Select Comm.).

12 *See, e.g.*, David J. Lynch & Danielle Paquette, "China to Revise Plan for Global Technology Dominance," Wash. Post, Dec. 12, 2018, *available at* https://www.washingtonpost.com/business/economy/china-to-revise-global-technology-dominance-plan/2018/12/12/6942cb78-fe22-11e8-83c0-b06139e540e5_story.html.

13 *See, e.g.*, Magnus Hjortal, *China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence*, 4 J. Strategic Security 1 (issue no. 2, summer 2011); U.S. Department of Defense Inspector General, *Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items*, Jul. 26, 2019 (non-classified [redacted] version), *available at* https://media.defense.gov/2019/Jul/30/2002164272/-1/-1/1/DODIG-2019-106.PDF.

14 *See, e.g.*, Mike Giglio, *China's Spies Are on the Offensive: China's Spies Are Waging an Intensifying Espionage Offensive Against the United States*, The Atlantic, Aug. 26, 2019, *available at* https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/; House Select Comm., *supra* note 11, at 2–4.

15 *See, e.g.*, Ellen Nakashima & William Wan, *In China, Business Travelers Take Extreme Precautions to Avoid Cyber-Espionage*, Wash. Post, Sep. 16, 2011, *available at* https://www.washingtonpost.com/world/national-security/2011/09/20/gIQAM6cR0K_story.html.

16 *See, e.g.*, *China's State Enterprises Are Not Retreating, But Advancing*, The Economist, Jul. 20, 2017, *available at* https://www.economist.com/leaders/2017/07/20/chinas-state-enterprises-are-not-retreating-but-advancing.

17 *See, e.g.*, *China's State Enterprises Are Not Retreating, But Advancing*, *supra* note 16; Lindsay Maizland & Andrew Chatzky, *Huawei: China's Controversial Tech Giant*, Council on Foreign Relations (Jun. 12, 2019), *available at* https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

18 *See, e.g.*, Maizland & Chatzky, *supra* note 17 (observing that the "government has considerable sway over all Chinese private companies" because of heavy regulation and government-connected executive appointments). *See also* Wendy Leutert, *Firm Control: Governing the State-Owned Economy Under Xi Jinping*," 2018 China Perspective 27 (issue 1-2, 2018) (exploring the relationship between consolidation of personal power and greater state control over economic activity).

19 *See*, *e.g.*, Ted Galen Carpenter, *Prepare for a More Authoritarian China: China May Be Getting Richer, But That's Not Making It Freer*, Nat'l Interest, Aug. 3, 2019, *available at* https://nationalinterest.org/feature/prepare-more-authoritarian-china-70861; Cheng Li, *The End of the CCP's Resilient Authoritarianism? A Tripartite Assessment of Shifting Power in China*, 211 China Q. 595 (Sep. 2012), *available at* https://www.cambridge.org/core/journals/china-quarterly/article/end-of-the-ccps-resilient-authoritarianism-a-tripartite-assessment-of-shifting-power-in-china/FFF9FFE49772D9FF702150AF9CA7799E; James Kynge, *China and Hong Kong: The Ultimate Test of Authoritarian Rule*, Fin. Times, Oct. 4, 2019, *available at* https://www.ft.com/content/75b391b6-e699-11e9-b112-9624ec9edc59.

20 *See* Richard McGregor, *How the State Runs Business in China*, The Guardian (Jul. 25, 2019) (quoting Nicholas Lardy), *available at* https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei.

and publicly available information.[21] Recent events in Hong Kong are merely the most widely observed evidence of these changes.[22]

Part of the framework in place in China under the current regime is the legal requirement that private firms cooperate in government security initiatives, including by granting access to private communications and fully cooperating with China's Cyberspace Administration.[23] This creates special risk for anyone using telecommunications, computing, or related equipment from a broad array of well-known Chinese firms including Huawei, ZTE, China Mobile, Lenovo, and Lexmark, among others.[24] All of these firms have considerable investment from or control by China's government, leadership that is intimately connected to China's government or military, and evidence of product or service features that raise specific questions regarding intended or coincidental security risks.[25]

A final factor in the riskiness of Chinese ICT imports is that these firms' products typically are complex, sophisticated, and technologically advanced—characteristics that increase opportunities for inclusion of features that can be exploited with or without the firms' active cooperation.[26] The risks posed by such products are considerably greater, and less easily evaluated, than risks associated with ordinary commercial purchases of less complex products, such as the glass used to make mobile phone screens. Even such highly sophisticated products can pose relatively low security risks, as it is much more difficult to manipulate features to permit state espionage or related intrusions.

It is important to recognize the possibility that any of the above factors could be overstated due to a lack of sufficient credible information. Overstatement also can occur because personal interests may be served by exaggeration of risks or manipulation of factual information.[27] With respect to risks associated with ICT products from China, however, there is at least as great a prospect that the risks are *under*stated rather than *over*stated. There are obvious interests for the government of China, entities associated with the government, firms that produce and export ICT products from China to the United States, and entities that currently sell or use such products (or wish to) to minimize any estimation of the security risks associated with commercially viable and often low-priced China-sourced products.

Attention to error rates and error costs is essential to critical analysis, and caution before taking a complaint about imports as gospel is sensible. Yet the nature and importance of national security risks, the manifest connection of complex ICT products to such risks, and the complex of factors that make China-sourced ICT products especially likely to pose such risks together provide strong basis for setting aside the usual reservations about pleas for limiting imports or for regulating their use.

IV. Potential Remedies

There are several possible remedies to the risks posed by China-sourced ICT products. While not an exhaustive listing, some of the major candidates are described below.

One obvious remedy is to make changes to U.S. government procurement rules to guard against inclusion of such products in departments and operations of special sensitivity.[28] But such changes are unlikely to be availing. Security lapses often have been traced to government officials' personal equipment—not to their work-purchased equipment and services—or to the equipment and networks of non-government personnel (particularly government contractors). These lapses can be addressed by strengthening enforcement of rules respecting government personnel's use of equipment or services even for strictly personal communications. But highly publicized lapses in security by officials at the highest levels—lapses that occurred despite security personnel's cautions about the activities that led to them—suggest the difficulty of reliance on such rules. Moreover, there simply are too many points of interaction between government and non-government actors in respect of even very sensitive security-related functions to gain much traction through limits on government purchasing and government personnel alone.

Another potential remedy that addresses part of the problem just noted is to amend rules governing government contractors

21 *See*, *e.g.*, Jude Blanchett, *5 Bad Things in China's Future (and 3 Good Things)*, Foreign Pol'y, Oct. 2, 2019, *available at* https://foreignpolicy.com/2019/10/02/five-bad-things-in-chinas-future-and-three-good-ones/; Elizabeth C. Economy, *The Problem with Xi's China Model: Why Its Successes Are Becoming Liabilities*, Foreign Affairs, March 6, 2019, *available at* https://www.foreignaffairs.com/articles/china/2019-03-06/problem-xis-china-model.

22 *See*, *e.g.*, Kynge, *supra* note 19; Daniel Victor & Mike Ives, *What's Happening with the Hong Kong Protests?*, N.Y. Times, Oct. 15, 2019, *available at* https://www.nytimes.com/2019/10/15/world/asia/what-are-hong-kong-protests-about.html?.

23 *See, e.g.*, Paul Rosenzweig & Kathryn Waldron, Broadening the Lens on Supply Chain Security in the Cyber Domain 3 (R Street Policy Study No. 170, Apr. 2019), *available at* https://www.rstreet.org/2019/04/15/r-street-policy-study-no-170-broadening-the-lens-on-supply-chain-security-in-the-cyber-domain/.

24 *See, e.g.*, Tara Beeny, et al., Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology 14-18 (Apr. 2018), *available at* https://www.uscc.gov/Research/supply-chain-vulnerabilities-china-us-federal-information-and-communications-technology (Interos Solutions, Inc., document prepared for U.S.-China Economic & Security Review Commission); Andy Keiser & Bryan Smith, *Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat*, Nat'l Security Inst. (Jan. 24, 2019), *available at* https://nationalsecurity.gmu.edu/chinese-telecommunications/; Rosenzweig & Waldron, *supra* note 23, at 6–8; U.S. Department of Defense Inspector General, *supra* note 13, at 6–7.

25 *See, e.g.*, Beeny, et al., *supra* note 24, at 24–27; Rosenzweig & Waldron, *supra* note 23, at 6–8; U.S. Department of Defense Inspector General, *supra* note 13, at 6–9.

26 *See, e.g.*, Ronald A. Cass, *Lessons from the Smartphone Wars: Patent Litigants, Patent Quality, and Software*, 16 Minn. J.L. Sci. & Tech. 1, 13–16 (2015) (discussing complexity of smartphones in relation to number of patented components and processes, as well as commercial value), *available at* http://scholarship.law.umn.edu/mjlst/vol16/iss1/3; House Select Comm., *supra* note 11, at 1–6 (discussing difficulties of addressing security threats from complex equipment that interconnects with communications networks).

27 *See generally, e.g.*, Anne O. Krueger, *The Political Economy of the Rent-Seeking Society*, 64 Amer. Econ. Rev. 291 (1974).

28 Some have already called for such changes. *See, e.g.*, Beeny, et al., *supra* note 24; Keiser & Smith, *supra* note 24, at 15, 26; U.S. Department of Defense Inspector General, *supra* note 13.

as well as government personnel.[29] Here, too, some gains may be had, but the same enforcement problems that attach to attempts to enforce security regulation through rules addressed to government officials stand in the way of effective control of security risks through regulations aimed at government contractors. Asking a broad swath of entities and individuals who work for private firms that do business with the U.S. government to appreciate the risks from use of widely available commercial ICT products is apt to be insufficient protection of national security. The breaches of security that have been traced back to officials' privately owned products, to equipment and services of government contractors, and to the personnel who work for those contractors are sufficiently numerous to highlight the difficulty of directing others what products to use and how to assure their security.

A different and broader possible remedy would rely on imposing restrictions on importation and sale in the United States of certain China-sourced ICT products that are deemed to pose significant risks to the security of the United States. The most likely vehicle for effecting such restrictions would be Section 232 of the Trade Act of 1962.[30] The provision, as amended, requires the Secretary of Commerce, in consultation with the Secretary of Defense and other appropriate government officials, to conduct an investigation of the possible national security effects of particular imports (when requested by particular parties or on his own initiative). The Secretary evaluates the effects of the imports on national security and recommends to the President whether and what action is appropriate to eliminate or reduce adverse security effects. The President is given broad discretion to determine whether the imports threaten U.S. national security. He also is granted expansive authority to determine the appropriate action if he decides those imports do threaten national security, including negotiating limits on imports but also extending to an unspecified wider range of options.

On its face, Section 232 seems to offer a clear option for the U.S. to investigate Chinese ICT imports and their impact on U.S. security interests and, if necessary, to address the threats through import restraints or other means. While the U.S. law's plain text would cover actions restricting importation and sale of ICT products that could compromise U.S. security by virtue of their potential susceptibility to espionage from China, some arguments about the law reach back to the underlying international trade provision that determines whether Section 232's implementation would be consistent with U.S. obligations under the GATT and WTO.[31] The provision at issue states that the GATT does not prevent any member country "from taking any action which it considers necessary for the protection of its essential security interests."[32] That provision is followed directly by three clauses listing reasons a nation might conclude that its interests are threatened. The third clause covers actions deemed necessary to protect security that are "taken in time of war or other emergency in international relations."[33] The United States takes the position that what a nation "considers necessary for the protection of its essential security interests" is up to each nation, as the phrase's emphasis not on what *is* necessary but on what a nation *considers* necessary strongly suggests.[34] A recent decision of a WTO dispute resolution panel rejected that reading, but there is considerable doubt whether that particular ruling will be upheld.[35] Moreover, even if the WTO decides that it is authorized to decide the necessity of actions to respond to an "emergency in international relations," there certainly is a strong argument that national security threats tied to escalating cyber-espionage and prospects for cyber-espionage satisfy Article XXI's conditions.

If the U.S. initiates a proceeding under Section 232, finds a national security threat, and undertakes actions designed to restrict imports of Chinese ICT products that might present security risks, political pushback from China is almost inevitable. Chinese officials have been vocally opposed to restrictions on products from Huawei and ZTE which have been identified by several nations, including the United States, as conducive to Chinese cyber-espionage.[36] If limitations are imposed on a wider array of items from a larger group of firms, the level of complaints from China certainly would rise. In response, China would likely impose sanctions against U.S.-sourced exports to China and increase efforts to persuade U.S. firms dependent on China trade to vocally oppose the government's actions. Given China's recent willingness to wield its economic muscle and its political control of the law and markets within China to secure favorable results, there is substantial reason to expect some U.S. firms to voice support for China's position in any trade conflict.[37] While there are reasons for skepticism about many claimed needs for

29 *See, e.g.*, Beeny, et al., *supra* note 24, at 33; Keiser & Smith, *supra* note 24, at 15.

30 19 U.S.C. § 1862.

31 *See*, *e.g.*, Brandon J. Murrill, *The "National Security Exception" and the World Trade Organization*, Cong. Research Serv. (Nov. 28, 2018), *available at* https://fas.org/sgp/crs/row/LSB10223.pdf.

32 GATT art. XXI, sec. b, *supra* note 5.

33 *Id.* at sec. b, cl. iii.

34 *See*, *e.g.*, Russia — Measures Concerning Traffic in Transit (DS512), Responses of the United States of America to Questions from the Panel and Russia to Third Parties (GATT Dispute Resolution Proceeding), Feb. 20, 2018, at 1–5, *available at* https://ustr.gov/sites/default/files/enforcement/DS/US.3d.Pty.As.Pnl.and.Rus.Qs.fin.%28public%29.pdf.

35 *See*, *e.g.*, William A. Reinsch, *The WTO's First Ruling on National Security: What Does It Mean for the United States?*, Center for Strategic & Int'l Studies (Apr. 5, 2019), *available at* https://www.csis.org/analysis/wtos-first-ruling-national-security-what-does-it-mean-united-states.

36 *See, e.g.*, Keiser & Smith, *supra* note 24; Maizland & Chatzky, *supra* note 17; *Five Eyes Will Not Use Huawei in Sensitive Networks*, Reuters, Apr. 24, 2019, *available at* https://www.reuters.com/article/us-britain-huawei-ncsc-usa/five-eyes-will-not-use-huawei-in-sensitive-networks-senior-us-official-idUSKCN1S01CZ; *Czech Cyber Watchdog Calls Huawei, ZTE Products a Security Threat*, Reuters, Dec. 17, 2018, *available at* https://www.reuters.com/article/us-czech-huawei/czech-cyber-watchdog-calls-huawei-zte-products-a-security-threat-idUSKBN1OG1Z3.

37 Apart from the self-interest of firms seeking to advance their own prospects of favorable treatment in China, there is ample reason to expect China to use its economic clout outside China as a source of advantage. *See, e.g.*, Center for Strategic and International Studies, *China Power: How Will the Belt and Road Initiative Advance China's Interests?*, *available at* https://chinapower.csis.org/china-belt-and-road-initiative/; Andrew Chatzky & James McBride, *China's Massive Belt and Road Initiative*, Council on Foreign Relations (May 21, 2019), *available at* https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

protection of domestic producers, there also is special reason for wariness about the arguments certain to be made on the other side of this debate.

V. Conclusion

Given the paramount importance of national security, it is critical to examine complaints about the threats posed by China-sourced products in the ICT sector. The combination of factors—political, economic, military, and practical—that make such products especially likely to pose security threats provides strong reasons to consider U.S. actions that could counter such threats before there is significant damage to U.S. national security.

In particular, the Department of Commerce should view an investigation under Section 232 of the Trade Expansion Act as an appropriate vehicle for gathering the necessary information on the scope and shape of security threats posed by particular firms, products, or product classes and for formulating responses to those threats. Although Chinese officials would oppose an investigation and responses that it might generate, that opposition might say more about their interest in continued maintenance of conditions conducive to espionage (or at least to facilitating it when that would most serve China's perceived national interests) than it does about the factual predicates for U.S. action. This paper does not purport to give a final answer to the question whether particular actions ultimately are the right responses, but it does support serious inquiry into threats to U.S. security from a broader set of firms and products than has been the focus of public scrutiny.