Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233

COMMENTS OF CHINA TECH THREAT AND BLUEPATH LABS

Roslyn Layton, PhD
Founder, China Tech Threat

Peter Wood
Program Manager, BluePath Labs

September 20, 2021

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233

COMMENTS OF CHINA TECH THREAT AND BLUEPATH LABS

I. INTRODUCTION AND SUMMARY

The Commission seeks comment on a proposal to prohibit future authorizations communications equipment on entities that pose unacceptable risk to U.S. national security and whether approvals should be revoked from products and services from the Federal Communications Commission (FCC) Covered List pursuant to the Secure and Trusted Communications Networks Act of 2019.

Most Americans don't realize that they are at risk from intrusion by the People's Republic of China (PRC) when they use products and services like smartphones by Huawei and ZTE, video surveillance cameras by Hikvision and Dahua, and Hytera radios that are widely available on Amazon.com, Best Buy, and Walmart. Despite major policy enacted by the Congress and the Departments of Defense and Commerce to address risks posed by these entities as well as human rights violations, the FCC reports that some 3000 applications for equipment authorization from Huawei alone have been approved since 2018. This a serious and egregious

loophole which needs to be addressed.

The FCC proposes to close this gap by restricting, if not revoking, equipment authorizations from entities on the Covered List. The FCC has a unique, important authority granted by Congress to regulate commercial equipment which uses radio frequencies, including but not limited to the Communications Act (47 U.S. Code § 302a), Communications Assistance for Law Enforcement Act, and the Secure and Trusted Networks Act of 2019. Under this most recent Act, Congress has instructed the FCC to create a covered list of equipment and services that meet certain criteria and determinations of national security risk, to update this list periodically, and to add and remove entities accordingly.

The FCC has made a good start to propose prohibiting equipment authorizations from entities on the Covered List, presently the five Chinese military aligned companies Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company. However, there are many more similar entities operating in the US which pose an unacceptable national security risk. The FCC needs to apply these prohibitions to all equipment authorizations from Chinese government owned and military aligned entities which operate in the U.S. today which pose unacceptable national security risk.

By way of example, this comment suggests two firms among many which already fit the criteria defined by the 2019 Secure and Trusted Networks Act and should be added to the Covered List. It details the case to add Lenovo Group and Limited and Yangtze Memory Technologies Corp (YMTC) to the Covered List.

All information technology from the People's Republic of China (PRC) is vulnerable to

that government's intrusion, whether through technical means like control channels, backdoors or kill switches, or through government practices of surveillance, espionage, and sabotage. The only way to effectively mitigate the risk of PRC intrusion is to restrict the devices and equipment.

We offer our relevant knowledge and expertise in service to the FCC in this proceeding. And respond to the FCC's various questions with a series of policy points and observations relevant to this proceeding and to develop effective rules. **China Tech Threat** was founded by Roslyn Layton to study the problems of technology produced by the People's Republic of PRC and suggest policy solutions to protect the security, privacy, and prosperity of all Americans.[1] Layton is also Senior Vice President of Strand Consult, an independent research organization studying the global mobile telecom industry and has produced primary research reports on Huawei Technologies and the telecom industry in the People's Republic of China (PRC).[2] Layton earned a doctorate in international internet regulation at Aalborg University and continues to teach and research there.[3] She served on the Presidential Transition Team to the FCC, has testified in the Senate and House on various topics in the mobile telecom and technology industries and has participated in various FCC proceedings. She is the Program Chair of the Telecom Policy Research Conference, now in its 50th year.[4]

BluePath Labs (BPL) is a DC-based consulting company that focuses on research, analysis, disruptive technologies, and wargaming.[5] BPL has a team of Chinese-language enabled analysts

[1] "About Us," China Tech Threat, accessed September 17, 2021, https://chinatechthreat.com/about-us/.
[2] "China," *Strand Consult* (blog), accessed September 17, 2021, https://strandconsult.dk/category/china/.
[3] Roslyn Layton, *Which Open Internet Framework Is Best for Mobile App Innovation?: An Empirical Inquiry of Net Neutrality Rules around the World*, Ph.d.-Serien for Det Tekniske Fakultet for IT og Design, Aalborg Universitet (Aalborg Universitetsforlag, 2017), https://doi.org/10.5278/vbn.phd.engsci.00181.
[4] "TPRC," TPRC, accessed September 17, 2021, http://www.tprcweb.com.
[5] "Research," BluePath Labs, accessed September 17, 2021, https://www.bluepathlabs.com/research.html.

with expertise in PRC related to the People's Liberation Army, the Chinese R&D ecosystem and emerging technologies with defense applications. Peter Wood is defense analyst and expert in Chinese language and politics. He co-authored *China's Military-Civil Fusion Strategy: A View from Chinese Strategists* published by the China Aerospace Studies Institute.

II. DISCUSSION

A. The FCC Must Perform Its Duties Per the Secure and Trusted Networks Act of 2019

The opening paragraph of the Communications Act of 1934 notes its express purpose for the safety and security of communication, ensuring "adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communication. . ." The FCC conducts the authorization process for all equipment for non-federal communications. Current authorization parameters include compliance with interference regulation, hearing aid compatibility, and Environmental Protection Agency health requirements.

In recent years, the US government, in response to significant voter demand, has promulgated important laws and policies to address the growing threat and militarization of the People's Republic of China (PRC). Congress instructed the FCC to create the Covered List in as part of the 2019 Secure and Trusted Networks Act and to enact regulation to realize its goals and requirements. Congress recognized that certain policy instruments which enact security regulation among federal actors, do not necessary translate to protections and controls for equipment and services at the consumer or end-user level, and therefore Congress instructed the FCC to close the gap.

Section 2, a-d of the Act (27 USC 1601) requires the FCC to update the Covered List periodically or at least annually and instructs the agency to add or remove entities per the relevant criteria and determinations described as follows. To meet the relevant threshold of posing an" unacceptable risk of national security to safety and security the United States and/or United States persons", the communications equipment or service must fulfill technical and/or administrative criteria.

1. The technical criteria for communications equipment or services are those capable of
    - routing or redirecting data traffic
    - permitting visibility into user data or packets that the equipment or service transmits or handles or
    - causing the network of a provider of advanced communications to be disrupted remotely
2. The administrative criteria alone are sufficient to place an item on the Covered list. A communications equipment or service can be placed on the covered list through a determination made by one or more of the following
    - An Executive Brand interagency body with appropriate national security expertise including the Federal Acquisition Security Council (FASC) [The FASC includes representatives from seven executive branch agencies: the Department of Homeland Security, the Department of Defense, the Office of Management and Budget, the General Services Administration, the Office of the Director of National Intelligence (ODNI), the Department of Justice and the Department of Commerce.]
    - Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg.

22689; relating to securing the information and communications technology and services supply chain)

- As defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232; 132 Stat. 1918)
- An appropriate national security agency, e.g. Department of Defense

Notably Executive branch departments and agencies have already made determinations on entities which posed unacceptable national security risk. Here is a brief, but not comprehensive, overview.

Department of Defense

Per a statutory requirement of Section 1260H of the National Defense Authorization Act for Fiscal Year 2021, the Department of Defense (DoD) released the names of Communist Chinese Military Companies (CCMC) operating directly or indirectly in the United States.[6] While DoD must provide this list to Congress by law, and it provides value for the public interest, this list itself does not ensure security. DoD has also highlighted vulnerabilities with Lenovo and Lexmark, as a 2019 report for the DoD Inspector General noted some $33 million in purchasing of restricted laptops and printers.[7]

The key takeaway for the FCC is that equipment destined to apply for authorization could come from any of these Chinese military entities, though the brand names will not necessarily match the parent. For example the Aviation Industry Corporation of PRC (AVIC) owns the

[6] "DOD Releases List of Chinese Military Companies in Accordance With Section 1260H of the Na," U.S. Department of Defense, accessed September 17, 2021, https://www.defense.gov/Newsroom/Releases/Release/Article/2645126/dod-releases-list-of-chinese-military-companies-in-accordance-with-section-1260/.
[7] "(U) Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items" (Department of defense, July 26, 2019), https://media.defense.gov/2019/Jul/30/2002164272/-1/-1/1/DODIG-2019-106.PDF.

luxury Swiss watch maker Fiyta which makes a watch for outer space.[8] This adds complexity to the FCC's task.

Importantly the National Defense Authorization Act (NDAA) restricts *military* and *federal* procurement of products and services from vulnerable entities. It says nothing about the use of these products for consumers, and indeed smartphones by Huawei and ZTE, video surveillance cameras by Hikvision and Dahua, and Hytera radios proliferate on Amazon.com, Best Buy, and Walmart.

Moreover, the NDAA says nothing about state level government. The state and local governments of the 50 US states also conduct sensitive communications and collect valuable information related to the individuals and organizations of that state. Their devices are also vulnerable to malicious and foreign intrusion. Security practices vary significantly across states. To assess the level of risk taken by state government, China Tech Threat has performed a state-by-state analysis using DoD's criteria to compile and illustrate the purchase and installation of Lenovo and Lexmark.[9]

Department of Commerce Bureau of Industry and Security (BIS) Entity List and Military End User List

BIS is an agency in the Department of Commerce which conducts export control, treaty compliance system, and measures to ensure US strategic technology leadership. It charged with developing and enforcing controls so-called "dual-use" technologies with civil and military applications. In recent years, the US has entered into multilateral arrangements with other

[8] By Serge Maillard, "Fiyta: The Horological Side of Chinese Soft Power," accessed September 17, 2021, https://www.europastar.com/the-watch-files/watchmaking-in-china/1004091451-fiyta-the-horological-side-of-chinese-soft-power.html.

[9] Roslyn Layton. "Stealing From the States: China's Power Play in IT Contracts US State Governments' Failure to Scrutinize the Purchase of Lenovo and Lexmark Equipment Jeopardizes Data Security." China Tech Threat. March 2020. https://chinatechthreat.com/special-report-state-contracts-with-banned-chinese-tech-manufacturers/

nations to improve the effectiveness of strategic trade control and to reduce abilities and incentives for seekers of sensitive items to evade rules.

BIS maintains the Lists of Parties of Concern including the Entity List and the Military End User List.[10] It uses the Entity List to controls the ability of US firms to license strategic technology to foreign parties. [11] US firms wishing to transact business with a listed entity will typically be denied a license.

The Entity List is used to keep sensitive US technology out of adversaries' hands. This is an important tool to restrict US firms from working with vulnerable foreign entities. Some 420 PRC firms have been added to the Entity List in years for various practices that endanger US national security and violate human rights. Over 900 entities from the PRC appear in the Consolidated Screening List, including Panda Electronics and drone maker Shenzhen DJI Sciences and Technologies Ltd.[12] However many PRC equipment manufacturing maintain their own research, development, and production which do not necessarily need to access US technology. Hence they may be out of the purview of the Entity List. As such, it is not sufficient for the FCC to rely only on the Consolidated List of Actors of Concern to identify entities which pose safety and security risks.

B. Understanding the Information Technology (IT) Threats Posed by the PRC

A *threat* is an expression of intent to inflict injury or damage. Relatedly, a *vulnerability* is the quality or state of being exposed to the possibility of being attacked or harmed. All information technology goods and services produced by entities owned or affiliated with the PRC are

[10] "Lists of Parties of Concern," accessed September 17, 2021, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern.
[11] "Entity List," accessed September 17, 2021, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.
[12] https://www.trade.gov/consolidated-screening-list

vulnerable to PRC threats. There are three categories of threats associated with the PRC information technology. These are:

- Malicious hardware, software, and components
- Data theft and exfiltration
- Unethical and illegal business practices

Malicious hardware, software, and components

Many PRC information technology inputs are designed with the intention to infiltrate, disrupt, damage, or otherwise compromise the integrity of the product. For example, a backdoor is a malicious hardware or software that bypasses or negates the regular process to authenticate access a computer system, product, software service, or device. Backdoors enable unauthorized remote access to elements within a system (files or databases) and/or empower an unauthorized user or use to execute commands in the network. It is a covert method to bypass authentication and encryption. It can be a hidden part of a program, code within the firmware of hardware, or exist in another part of the electronic technology. The presence of backdoors and other tech threats prompted Congress to restrict the use of Huawei in the US. Similarly, devices from Lenovo, Lexmark, and Hikvision have been restricted for purchase by the military.

A cyberattack is an aggressive action involving the misuse of technology to infiltrate, exfiltrate, tamper, or disrupt computer networks. These attacks are escalating in sophistication, severity, and frequency, and until recently few US policymakers were willing to investigate the link between the problem of intrusion with the preponderance of PRC information technology embedded throughout the US.

The case of Supermicro, still unresolved, demonstrates the risk of hardware manufacture in and by the PRC. The story illustrates that even products from U.S. firms can be compromised by third-party suppliers in the PRC. Reporting from Bloomberg in 2018[13] and 2021[14] includes corroboration from multiple U.S. intelligence and security officials who allege that the People's Liberation Army (PLA) in concert with a Chinese subcontractor attached a tiny chip into thousands of motherboards intended for U.S. companies.

Once installed in servers, these stealth backdoors could open networks to hackers. The attack was reported to have impacted at least 30 companies, including a major bank, Apple, and Amazon Web Services. Apple subsequently ripped and replaced 7,000 servers, and Amazon terminated a related supplier in PRC. "Hardware hacks are more difficult to pull off and potentially more devastating, promising the kind of long-term, stealth access that spy agencies are willing to invest millions of dollars and many years to get," the 2018 Bloomberg article states. "In Supermicro, PRC's spies appear to have found a perfect conduit for what U.S. officials now describe as the most significant supply chain attack known to have been carried out against American companies." Jay Tabb, who served as Executive Assistant Director of the FBI's national security branch from 2018 to 2020, observes:

> "Supermicro is the perfect illustration of how susceptible American companies are to potential nefarious tampering of any products they choose to have manufactured in PRC. It's an example of the worst-case scenario if you don't have complete supervision over where your devices are manufactured. The

[13] USA v. Ehab Ashoor. | [2010] | U.S. District Court, Southern District of Text, Houston Division | No. H-09-CR-307| https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/r9dKMMM0Gi5I/v0

[14] Jordan Robertson and Michael Riley. "The Big Hack: How PRC Used a Tiny Chip to Infiltrate U.S. Companies." Bloomberg. October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/ the-big-hack-how-PRC-used-a-tiny-chip-to-infiltrate-america-s-top-companies

> Chinese government has been doing this for a long time, and companies need to be aware that PRC is doing this… And Silicon Valley in particular needs to quit pretending that this isn't happening."[15]

The PRC has an IT industry that sells hardware, software, and other applications to US organizations and individuals. Many of these technologies are gaining market share, whether through competitive pricing, partnering, or other means. Major U.S. action has restricted Huawei, ZTE, Hikvision and others, but there is nothing to stop other state-owned and state-affiliated companies from installing backdoors on any piece of Chinese hardware and/or manipulating the equipment's' control channel to other constituent devices which handle data streams. In fact, the Chinese government may require it.

Consequently, the PRC's enormous global market position in the IT manufacturing market gives it many long-term advantages to conduct infiltration (it has the knowledge and blueprints of its products), supply chain attacks (embedding malware in products), human intelligence (learning about customers, participating in U.S. trade associations), and social engineering. Supply chains are vulnerable to threats that may turn out to be more significant in the long term: Chips could be intentionally compromised during the design process *before* they are even manufactured. If placed into the design with sufficient skill, these built-in vulnerabilities would be extremely difficult to detect during testing. And they could be exploited months or years later to disrupt or exfiltrate data from a system containing the compromised chip. Such a scenario was detailed in *Ghost Fleet: A Novel of the Next World War*, which describes the grounding of all U.S. fighter jets because of compromised circuits produced in the

[15] Jordan Robertson and Michael Riley. "The Long Hack: How PRC Exploited a U.S. Tech Supplier." Bloomberg. February 12, 2021. https://www.bloomberg.com/features/2021-supermicro/

PRC.[16]

Relatedly a kill switch is a force operation designed to shut down network, device, or piece of software. Circuits can be enabled with a kill switch which can trigger a shutdown of the device in which they are embedded or in other parts of the equipment.[17]

Data theft and exfiltration

Data theft or exfiltration is the unauthorized or malicious transfer of data from a computer, device, program, or system. This is frequently done through hacking or the exploitation of a weakness in a system to gain access to personal or enterprise data. PRC hackers include an ever-changing mix of official, military, civilian and even robot actors, which may engage in state-sponsored, freelance, or independent intrusions. One example is the hack of the Office of Personnel Management, the US government's human resource department for federal employees, which the PRC conducted to capture millions of individuals' records including fingerprints and security clearances.

However, hacking is not necessarily the leading problem. PRC companies themselves may provide user or enterprise data to the government. The PRC's 2016 Internet Security Law asserts the country's sovereignty over cyberspace, authority over all internet products and services made in the PRC, and obligations of Chinese producers of internet products and services to the Chinese state. The PRC's 2017 National Intelligence Law compels any Chinese subject to

[16] Singer, Peter Warren, and August Cole. *Ghost fleet: A novel of the next World War*. Houghton Mifflin Harcourt, 2015.
[17]"Now May Be the One Chance for Safer IoT Cyber Security," *Verdict* (blog), May 21, 2021, https://www.verdict.co.uk/now-may-be-chance-for-safer-iot/.,
U. F. Editors, "Hardware Trojan: Kill Switch within the Circuitry of an Integrated Circuit," Unrevealed Files, accessed September 17, 2021, https://www.unrevealedfiles.com/hardware-trojan-kill-switch-within-the-circuitry-of-an-integrated-circuit/.
"The Hunt for the Kill Switch," IEEE Spectrum, May 1, 2008, https://spectrum.ieee.org/the-hunt-for-the-kill-switch.

spy on behalf of the state. As such, the PRC's information communication technology firms can be compelled to collect data or conduct surveillance on any piece of technology at any time for any reason anywhere. Customer information collected on Chinese devices anywhere can also brought to PRC. Indeed, many contracts with Chinese IT providers stipulate as much. However, data need not be taken out of the United States to be available to the Chinese government. The PRC does not honor US, United Kingdom, or European Union privacy and data protection laws. Users by accessing PRC technology providers like TikTok, WeChat, or AliPay expose themselves to the PRC's Social Credit System and other PRC data processing. The PRC keeps a database on foreign nationals for a variety of purposes.

There is little to no ability to challenge the PRC in Chinese court. There is no warrant for the request to intrude or due process should a plaintiff seek damage for an intrusion.

Unethical and illegal business practices

Many PRC technologies are developed in unethical conditions, for example the development of facial recognition technologies through coercion and surveillance of Uighur Muslims and the production of IT products and service with child or slave labor. Additional illegal practices include predatory pricing, dumping, and lack of financial, regulatory, or other disclosure per relevant laws. A related issue is the development of artificial intelligence, facial recognition, and other technologies in unethical situations which are subsequently integrated in products and services consumed by Americans.

C. The PRC's Military Civil Fusion Strategy and Threats to Equipment Using Radio Frequencies

The People's Republic of PRC (PRC) is the leading manufacturer of equipment using radio

frequencies devices. Its headquarters thousands of state-owned and military-aligned firms which produce products destined for the US market. Moreover, many US firms manufacture in PRC, whether in their own facilities or with contractors. No other country comes close to the breadth and scale of the security threat of the PRC. While intruders may come from any location on earth, PRC is engaged in a committed, long-term plan to displace the US in military and economic leadership, and information technology is a key front for this offensive.[18]

The PRC regards itself as engaged in a long-term 'systems confrontation' with the United States, pitting states' respective defense strategies, economic systems and degree of civil-military synergy against one another.[19] Maintaining a technological edge is crucial for PRC to achieve a decisive lead. More broadly, the PRC's strategy is to "displace" the US as the preeminent global leader economically, politically, and militarily. Doshi describes displacement as *blunting* the exercise of US control; *building* control over US; and expanding control globally.

This can be observed in many IT industries in which PRC has gained large if not total market share: computers, smartphones, communications equipment, solar panels, flat panel displays, and light emitting diodes (LED). While the US may have willingly divested assets to PRC actors and offshored/outsourced manufacturing which have empowered the PRC, many PRC advances were facilitated by intellectual property theft and/or forced technology transfer, not merit or market competition. It can be observed in PRC's comeuppance in global governance and technology standards. It can be observed in the growth of PRC's military which now exceeds the US on many levels. Notably America's piecemeal strategy which focuses on individual target

[18] Doshi, Rush. *The Long Game: PRC's Grand Strategy to Displace American Order*. Oxford University Press, 2021.
[19] Alex Stone and Peter Wood, *PRC's Military-Civil Fusion Strategy*, 12 June 2020. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/CASI_China_Military_Civil_Fusion_Strategy.pdf, 4, 12.

companies rather than the systemic, organizing forces which drive PRC's ambition has enabled the PRC to circumvent many U.S. restrictions.

The PRC industrial policy strategy, Made in China 2025 [中国制造 2025], and the Dual Circulation [国内国际双循环] policy, launched in 2015 and 2020 respectively complement its Five Year plans, and are intended to bolster the PRC's overall economic strength while promoting technological innovation and reducing reliance on foreign technology.[20] In doing so it seeks to displace the U.S.'s and other countries' leading position. These policies have come into even sharper focus as the PRC continues to rely on semiconductors to an outsize degree--making breakthroughs in that technology by any and all means a major priority.

Information technology is a pillar of the displacement strategy, as described as techno nationalization or techno globalization. The PRC is the only threat actor which has an IT industry which rivals America's. Chinese computers, devices, software, and other information technologies are ubiquitous and embedded with PRC government practices and laws which may facilitate intrusion, theft, espionage, surveillance, sabotage, or other compromise of integrity. These practices can also be described as a form of cyberwarfare.

In "A World Divided: The Conflict with Chinese Techno-Nationalism Isn't Coming – It's Already Here,"[21] [22] leading military intelligence expert James Mulvenon attributes the reign of technological globalism[23] to the "Davos set" and the gurus of the Fourth Industrial

[20] Alicia García Herrero, "What is Behind PRC's Dual Circulation Strategy" *PRC Leadership Monitor*, Fall 2021 Issue 69 1 September 2021. https://3c8314d6-0996-4a21-9f8a-a63a59b09269.filesusr.com/ugd/af1ede_23bce3e803574025848156e2ba8ca776.pdf

[21] James Mulvenon. A World Divided: The Conflict with Chinese Techno-Nationalism Isn't Coming – It's Already Here War on the Rocks. January 28, 2021. https://warontherocks.com/2021/01/a-world- divided-the-conflict-with-chinese-techno-nationalism-isnt-coming-its-already-here/

[22] Rodrik, Dani. The globalization paradox: democracy and the future of the world economy. WW Norton & Company, 2011.

[23] Ostry, Sylvia, and Richard R. Nelson. Techno-nationalism and techno-globalism: Conflict and cooperation.

Revolution, who want a borderless world organized by transnational social media platforms and supply chains.[24] However "global" this regime claims to be, its supply chain and IT actors are increasingly national, located in and controlled in a single place: the PRC (albeit with some product assembly in Taiwan).

Mulvenon characterizes today's world as two different technological ecosystems—one dominated by PRC firms, either implicitly or explicitly controlled by the mercantilist Chinese state,[25] and the other an "amorphous technological environment" comprising the Organization for Economic Co-operation and Development countries and their associated firms (yet, increasingly penetrated by PRC actors). Notably, the PRC model is increasingly authoritarian, while the other evolves policy and regulation to accommodate democratic norms and expectations. "The edges where these two spheres meet are now in a persistent site of conflict, with the demands of global interconnectivity and supply chains chafing against a range of trade and export security concerns," Mulvenon observes.

The PRC is actively working to improve the efficiencies of its research and infrastructure investments in both the civilian and military spheres, what it describes as its Military-Civil Fusion Strategy [军民融合战略], hereafter MCFS. This has obvious implications for technological transfer of even ostensibly civilian technologies to the Chinese military, but the strategy has additional meaning for the PRC. In their study of the Military-Civil Fusion Strategy, Alex Stone and Peter Wood note that Chinese military strategists regard MCFS as a state governance approach that could directly support PRC's ability to prevail in a long-term strategic

Brookings Institution Press, 2000.
[24] Klaus Schwab. Fourth Industrial Revolution: What is means, how to respond. World Economic Forum. January 14, 2016. https://www.weforum.org/focus/fourth-industrial-revolution
[25] Jude Blanchette. "From "PRC Inc." to "CCP Inc.": A New Paradigm for Chinese State Capitalism." PRC Leadership Monitor. December 1, 2020. https://www.prcleader.org/blanchette

competition. MCFS seeks to acquire, exploit and weaponize American-made technologies and, ultimately, usurp the United States' economic and military leadership. The PRC is engaged in a sustained, whole-of-nation campaign of cyber-warfare against the United States that seeks to disrupt U.S. networks and acquire sensitive technologies that can be used against American national security and economic interests. For a detailed discussion of MCFSS, see the referenced report.[26] As of 2018, at least 3000 PRC enterprises participate in MCFS, with 70 percent coming from the IT industry.[27]

D. PRC Laws and Practices Compel Its Firms to Participate in MCFS, formally and informally

Even if PRC device manufacturers are not explicitly part of PRC's MCFS strategy, PRC law and practice compels them to participate. The rise of General Secretary Xi Jingping is associated with an acceleration of PRC's military advancement and an associated set of laws and policies to organize all PRC enterprise and the role of internet.[28] Through a series of actions codified in laws for Counterespionage (2014), National Security (2015), Counterterrorism (2015), Cybersecurity (2016), Foreign NGO Management (2016), National Intelligence (2017), and Data Security (2021).[29] Essentially through these laws, the PRC asserts sovereignty over the internet and its right and ability to acquire any data on any PRC made device anywhere in the world at any time. Similarly any Chinese subject can be enjoined to conduct espionage on behalf of the state.

---

[26] Stone, Alex, and Peter Wood. "PRC's Military-Civil Fusion Strategy: A View from Chinese Strategists." (2020). https://www.bluepathlabs.com/uploads/1/1/9/0/119002711/PRCs_military_civil_fusion_strategy-_full_final.pdf

[27] "Roughly 3,000 Private Chinese Enterprises Have Entered the Front Line of Military Industrial Procurement" [我国大约3000家民企已进入军工采购一线], Xinhua, 14 March 2018, http://m.xinhuanet.com/mil/2018-03/14/c_129829001.htm.

[28] Murray Scott Tanner. "Beijing's New National Intelligence Law: From Defense to Offense." Lawfare.com July 20, 2017. https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

[29] Ibid.

The FCC itself has recognized PRC authority to enjoin Chinese companies in the Huawei order.[30] The FCC also recognized in its license proceedings for PRC Telecom, PRC Unicom, and PRC Mobile that these PRC firms cannot separate themselves from the PRC government.[31] Essentially PRC firms have no ability to push back against a PRC demand, much less protect their users. There is no rule of law instrument such as warrant, due process, or judicial remedy that a PRC firm could access to stop, deter, or mitigate a PRC demand.

If anything, PRC device manufacturers support PRC goals. Increasingly, PRC device manufacturers publicize and promote their ties to the Chinese Communist Party.[32] It is not uncommon for leading technology CEOs in China to highlight their support and leadership in the Chinese Communist Party as a demonstration of national pride and solidarity.

MCFS is antithetical to US law, practice, and values. While it is true that the US military has been an important actor in certain technological innovations, US practice differs from the PRC for key reasons. For one, the US Constitution separates the government and military, and it guarantees civilian control over the armed forces. This is an important standard of liberal democracy versus authoritarian dictatorship. In the PRC, the government and military are a single entity.

US firms have a choice of whether to contract with the military. Moreover, US firms and other actors can challenge the practices of the military in court. MCFS firms in the PRC are frequently established as de facto military companies or national champions which are run at the

[30] "Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation" (FCC, June 30, 2020), https://docs.fcc.gov/public/attachments/DA-20-690A1.pdf.
[31] Ibid
[32] Emily Feng, "Chinese Tech Groups Display Closer Ties with Communist Party," *Financial Times*, October 10, 2017, https://www.ft.com/content/6bc839c0-ace6-11e7-aab9-abaa44b1e130.

behest of the government.

Information Technology and Innovation Foundation (ITIF) President Rob Atkinson described these key differences in a recent article titled Useful Idiots for the CCP" observing,

> "The U.S. government never forced foreign companies to invest in America to get market access. It never required technology transfer. It never encouraged and engaged in intellectual property theft. It seldom, if ever, engaged in massive late-stage production subsidies to national champions. It didn't use its regulatory state to coerce foreign companies into compliance, providing PRC with technology advantages.
>
> To be sure, like most nations, the United States invested in science and a STEM workforce, encouraged tech transfer from universities through effective measures like the Bayh-Dole Act, and put in place a research and development tax credit. If that is all PRC was doing, there'd be no problem and no case for complaints.
>
> But of course, that is not the principal way that PRC is trying to gain global dominance in advanced technology industries. They are cheating and violating the spirit, and usually the letter of the WTO." [33]

The equivalence argument has brandished by many US actors which wish to continue business with the PRC while downplaying if not ignoring the security concerns. The points by ITIF offer valuable counterpoint because it is an organization which supports enterprise but describes how bright lines can be drawn for national security and rule of law reasons, particularly as the PRCs practices violate the World Trade Organization requirements.

[33] Robert D. Atkinson, "Today's 'Useful Idiots' for the CCP" (Information Technology and Innovation Foundation, September 7, 2021), https://itif.org/publications/2021/09/07/todays-useful-idiots-ccp.

E. Technical and Supply Chain Considerations

Importantly the FCC recognizes that the equipment authorization responsibility may be held by more than the equipment manufacturer. It recognizes, "…. the assembler (if the equipment is assembled from individual component parts and the resulting system is subject to authorization), or the importer (if the equipment by itself or the assembled system is subject to authorization) and could also include retailers and parties performing modification under certain circumstances." As such, the FCC is mindful that regulating the brand name on the package is not sufficient to ensure security. Indeed this realization likely underscores that the adoption of a mere five PRC firms on the FCC's Covered List is insufficient to address the threats posed by some 2100 PRC firms involved with MCFS which operate in the US today. More largely the FCC likely understands that there are a variety of ways, actors, and points which make equipment vulnerable and require that the FCC perform a thorough inquiry and rulemaking as it undertakes today.

The PRC has a critical role in the electronics supply chain as an assembler and manufacturer. Given the PRC's significant military capabilities, the 'internet of things' could become a global attack surface for denial-of-service (DoS) intrusions, command and control nodes installation, surveillance (via poorly secured internet-connected security cameras), and so on. The ubiquity of these devices also means that they may be placed behind cyber devices without thinking or otherwise make their way into supply chains without end users' knowledge.

Indeed PRC equipment manufacturers themselves acknowledge that equipment can route and redirect user traffic and permit visibility into user data and/or packets transmitted and/or handled by the piece of equipment. This fact is noted in Section 889 of the 2019 NDAA and

reiterated in the filing by Hytera.[34] Challenges by Huawei and other covered companies against various rules restricting this equipment have been rejected in US courts, for example Huawei's petition to rescind the USF subsidy rule. Indeed the courts have also observed that the companies have been accorded substantial due process by the federal agencies themselves as well as the US court system which allows for formal complaint. Separately, it can be noted that US firms are not afforded the same opportunity when operating in PRC.

The FCC's operating licensing process shares similarity with equipment authorization. The FCC has found through its proceedings with China Unicom, China Telecom, and China Mobile that even partially owned PRC government enterprises are indirectly, if not directly and ultimately, controlled by the PRC government.[35] This is also reflected in corporate governance documents giving the PRC ultimate control of US-based based daughter companies. Despite the substantial due process afforded to these companies, they failed to address or mitigate the FCC's security concerns. The FCC found that PRC entities are vulnerable to exploitation, influence, and control by the PRC government and that "in the current security environment, there is a significant risk that the Chinese government would use the grant of such authority to conduct activities that would seriously jeopardize the national security and law enforcement interests of the United States." Notably the granting of licenses to PRC Mobile was denied because "due to a number of factors related to China Mobile USA's ownership and control by the Chinese government, grant of the application would raise substantial and serious national security and law enforcement risks that cannot be addressed through a mitigation agreement [and] grant of

[34] "ECFS Filing Detail," accessed September 17, 2021, https://www.fcc.gov/ecfs/filing/108171542312534. See attached PowerPoint on p. 6
[35] "FCC Launches Proceeding on Revoking China Telecom's Authorizations," Federal Communications Commission, December 10, 2020, https://www.fcc.gov/document/fcc-launches-proceeding-revoking-china-telecoms-authorizations.

this application would not be in the public interest."

Importantly, the companies on the FCC's Covered List do not dispute that they are under the power and influence of the PRC government and can be made to spy and surveille. Devices from these firms could be used to advance the PRC's goals, for example through the illicit acquisition of information where these PRC devices are connected in the USA. These methods include but are not limited to hacking, espionage, surveillance, sabotage, and other means to compromise integrity. It was for these reasons that Congress, based upon the insight of the Director of National Intelligence, identified the five companies now on the FCC's Covered List.[36] The following case studies on Lenovo and YMTC demonstrate how PRC government and military influence is integrated within the firm and presents security risk for equipment.

F. Case Study: Lenovo

As the following case study details, Lenovo should be added to the FCC's Covered List for technical and administrative reasons. As noted in the following case study, multiple US agencies have noted how traffic has been re-routed and redirected from Lenovo laptops to the PRC (see discussions from the State Department, US Marines, and Department of Defense). From the administrative side, the Department of Defense has a de fact "no Lenovo" policy. Moreover, the company has an exceedingly close proximity to the PRC government and military which makes it a candidate for the Department of Defense's CCMC list.

The U.S.-China Economic and Security Review Commission (USCC) is a bipartisan body was created by Congress under the National Defense Authorization Act of 2000. Its legislative mandate is to monitor, investigate, and submit to Congress an annual report on the

[36] "NCSC Briefs Agencies across the U.S. Government on Supply Chain Threats Posed by Five Specified Chinese Companies," accessed September 17, 2021, https://www.dni.gov/index.php/ncsc-newsroom/item/2141-ncsc-briefs-agencies-across-the-u-s-government-on-supply-chain-threats-posed-by-five-specified-chinese-companies.

national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, to Congress for legislative and administrative action. It issues special and annual reports to Congress on a variety of critical topics. For example, its 2018 "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology" report concluded that Lenovo is in the same class as Huawei and ZTE for its proximity to the PRC government.[37] The report explains,

> "Government support can take many forms, but it often includes preferential financing rates, preference in government contract bidding, and sometimes oligarchy or monopoly status in protected industries. In the case of Chinese national champions, the support also appears to include officially sanctioned or officially conducted corporate espionage designed to improve the competitiveness of Chinese firms while potentially advancing other government interests. Huawei, Zhongxing Telecommunications Corporation (ZTE), and Lenovo are three Chinese ICT companies that exhibit some of these characteristics…Lenovo's growth has been attributed to the economic and political support it receives from the Chinese government, including the use of state-owned intellectual property resources. Lenovo has been linked to Chinese state-led cyberespionage efforts. Lenovo products have been banned by intelligence agencies in Australia, Canada, New Zealand, the United Kingdom, and the United States (Five Eyes Countries) since the mid-2000s, when laboratories of the British intelligence agencies Military Intelligence, Section 5 and Government Communications Headquarters

[37] "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology." USCC April 19, 2018. https://www.uscc.gov/research/supply-chain-vulnerabilities-china-us-federal-information-and-communications-technology.

discovered “backdoors” and vulnerable firmware in Lenovo products.”[38]

Indeed Lenovo may be a graver concern because it facilitates the process and storage of data on laptops and servers, unlike Huawei and ZTE which enable primarily transmission, frequently of encrypted data.

As the USCC report describes, Lenovo originally formed in 1984 as the New Technology Development Company, a component of the state-run Chinese Academy of Sciences (CAS) Institute of Computing Technology[39] established to develop military technology.[40] The founder of Lenovo was educated at the Xi’an Military Communications Engineering Institution of the PLA, now Xidian University. The university has close connections with the PLA and is considered to be a link between PRC’s civilian and military research on cybersecurity.[41] Additionally, Lenovo’s CEO, who succeeded its founder, was educated at PRC’s University of Science and Technology, which was established and resourced by the CAS.[42] The CAS and its individual members have a history of coordinating with the Chinese military, including its cyber and electronic warfare operations.[43] The Chinese government, through Legend Holdings Limited, is the largest shareholder of Lenovo stock.

The company’s official government purpose was to “resolve problems relating the Sinification of IBM-system computers and IBM compatibles,” which it did by inserting a “Han-

[38] Ibid.
[39] Nathaniel Ahrens and Yu Zhou, PRC’s Competitiveness: Myth, Reality, and Lessons for the United States and Japan, CASE STUDY: Lenovo (Washington, DC: Center for Strategic and International Studies, January 2013), https://www.csis.org/analysis/PRC%E2%80%99s-competitiveness-lenovo.
[40] Zhijun, Ling. *The Lenovo affair: the growth of PRC's computer giant and its takeover of IBM-PC*. John Wiley & Sons, 2006.
[41] Edward Wong, “University in Xi’an Opens School of Cyberengineering,” Sinosphere: Dispatches from China (blog), The New York Times, January 6, 2015, https://sinosphere.blogs.nytimes.com/2015/01/06/university-in-xian-opens-school-of-cyberengineering/.
[42] 113 “USTC Introduction,” University of Science and Technology of China, About, October 14, 2016, http://en.ustc.edu.cn/about/201101/t 20110113 _87798.html.
[43] John Costello, “Testimony before the U.S.-PRC Economic and Security Review Commission: Chinese Intelligence Agencies: Reform and Future,” June 9, 2016, http://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony060916.pdf.

card" component into the computer to enable the input of Chinese characters, a system called Lian-Xiang or "linked thought", Lenovo's original Chinese name.[44] CAS provided the building, housing, and salaries for the startup and served as loan guarantor and customer to the fledgling firm. Lenovo grew as a reseller of IBM and HP computers which it outfitted with its "Han-card" and later in computer assembly, studying the components of imported computers and HP's distribution model. Lenovo developed strong domestic brand (in part by using its government connection to reverse judges' decision from 2nd to 1st place in a prestigious Chinese technology award[45]) and distribution with government help.

After becoming the top retailer in the Chinese market, Lenovo acquired IBM's personal computer and laptop division in 2005, IBM's and HP's Chinese operations, and in 2014, IBM's x86 server division and Motorola Mobility. Close association with the Chinese government has been instrumental for the company to be deemed a "national champion" for state support and promotion,[46] to list on the Stock Exchange of Hong Kong as a "Red Chip" stock to obtain international capital (and obscure its Chinese government ownership),[47] and to lessen, if not avoid, prosecution for import profiteering and other crimes which brought down its competitors.[48]

Lenovo's government ownership share has been reduced from 55 percent to 29 percent, the revenue and dividends of which are realized by PRC's Ministry of Finance and State-Owned Assets Management Bureau, which is used to further PRC's military industrial projects such as the Belt & Road Initiative and the antisatellite program, and other projects PRC government

[44] Ling p. 50
[45] Ling p. 77
[46] Ling p. 203
[47] Ling p. 160
[48] Ling p. 87

officials serve on Lenovo's board, some with double voting rights.[49]

In 2006, after congressional inquiries into the purchase of 16,000 Lenovo computers, the U.S. Department of State said the purchased computers would not be used.[50] In 2015, the U.S. Navy announced it would replace servers for its guided missile cruisers and destroyers after Lenovo acquired certain IBM server and software product lines, due to concerns that the equipment could be compromised during maintenance or remotely accessed by the Chinese government.[51]

In 2010, Lee Chieffalo, a United States Marine who managed the operations center in Iraq testified in court, "A large amount of Lenovo laptops were sold to the U.S. military that had a chip encrypted on the motherboard that would record all the data that was being inputted into that laptop and send it back to PRC. That was a huge security breach. We don't have any idea how much data they got, but we had to take all those systems off the network."[52]

In 2016, several incidents suggested the DoD internally banned Lenovo products owing to concerns about cyber spying against Pentagon networks and concerns that the company is installing backdoors in its products for the purposes of espionage. In April 2016, an Air Force email appeared to order that Lenovo products be removed from DoD networks.[53] In October 2016, the Washington Free Beacon reported that the Pentagon's Joint Staff had produced an

[49] Ibid p. 207
[50] "US Government Restricts PRC PCs," BBC News, May 19, 2006, http://news.bbc.co.uk/2/hi/americas/4997288.stm.
[51] Phil Muncaster, "US Navy Looks to Dump Lenovo Servers on Security Concerns—Report," Infosecurity Magazine, May 7, 2015, https://www.infosecurity-magazine.com/news/us-navy-dumps-lenovo-servers/; Megan Eckstein, "Navy Needs New Servers for Aegis Cruisers and Destroyers after Chinese Purchase of IBM Line," USNI News, May 5, 2015, https://news.usni.org/2015/05/05/navy-needs-new-servers-for-aegis-cruisers-and-destroyers-after-chinese-purchase-of-ibm-line.
[52] USA v. Ehab Ashoor. | [2010] | U.S. District Court, Southern District of Text, Houston Division | No. H-09-CR-307| https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/r9dKMMM0Gi5I/v0
[53] Hayley Tsukayama and Dan Lamothe, "How an Email Sparked a Squabble over Chinese-Owned Lenovo's Role at Pentagon," The Washington Post, April 22, 2016, https://www.washingtonpost.com/business/economy/how-an-email-sparked-a-squabble-over-chinese-owned-lenovos-role-at-pentagon/2016/04/22/b1cd43d8-07ca-11e6-a12f-ea5aed7958dc_story.html.

internal report warning against using Lenovo equipment.[54]

Lenovo is believed to have been complicit in installing Superfish spyware and potentially a BIOS backdoor on many of its computer products.[55] Superfish is a preloaded software shipped with Lenovo computers that ostensibly monitored internet browser traffic to improve advertisements, but also allowed hackers to read all encrypted browser traffic, including banking transactions, passwords, emails, and instant messages. The DHS U.S. Computer Emergency Readiness Team issued an alert and mitigation details in response.[56] Users later discovered that Lenovo computers shipped with a rootkit-style covert installer that would reinstall unwanted software on computers after users had deleted it. In September 2017, Lenovo reached a settlement with the Federal Trade Commission over charges that the company harmed consumers. As part of the settlement, Lenovo is required to implement a comprehensive software security program for consumer software.[57] The security program is subject to third-party audits.

Lenovo's acquisitions in the US were highly controversial, subject to significant pushback for national security concerns, and catalyzed major legislation to overhaul the review and approval for foreign direct investment by the Committee on Foreign Investment in the United States (CFIUS).[58] Major political and military shifts in PRC in recent years have increased national security threats, promoting US policymakers to revoke and unwind US licenses and acquisitions by Chinese state-owned and affiliated entities. Today CFIUS imposes a

[54] Bill Gertz, "Military Warns Chinese Computer Gear Poses Cyber Spy Threat," The Washington Free Beacon, October 24, 2016, http://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/.
[55] Vijay, "Lenovo PCs and Laptops Seem to Have a BIOS Level Backdoor," TechWorm, August 12, 2015, http://www.techworm.net/2015/08/lenovo-pcs-and-laptops-seem-to-have-a-bios-level-backdoor.html.
[56] Department of Homeland Security, "Lenovo Superfish Adware Vulnerable to HTTPS Spoofing," February 20, 2015, https://www.us-cer t.gov/ncas/aler ts/TA15 - 051A.127
[57] Federal Trade Commission, "Lenovo Settles FTC Charges It Harmed Consumers with Preinstalled Software on Its Laptops That Compromised Online Security," September 5, 2017, https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.
[58] "CFIUS' Growing Power to Protect American Security from China Tech Threats: Examining TikTok and Lenovo" (China Tech Threat, June 26, 2020), https://chinatechthreat.com/wp-content/uploads/2020/06/CFIUS-Paper-062420_.pdf.

much higher standard of data protection than in 2014, and it is likely that Lenovo's acquisition of IBM and Motorola assets would not be allowed under today's standards.

The externalities of these acquisition still have reverberations, as taxpayers are on the hook for $378 million of replacement cost as part of the US Space Force deployment and removal of an IBM server related to the Lenovo deal.[59] Indeed IBM servers were deployed in sensitive military installation across the armed forces. For example the Aegis Combat System is an American integrated naval weapons system produced by Lockheed Martin which uses powerful computer and radar technology to track and guide weapons to destroy enemy targets.[60] In addition to the US Navy, Aegis is deployed by navies in Japan, Spain, Norway, South Korea, Australia, and in NATO's missile defense. The IBM server is also a part of Raytheon's GPS Next-Generation Operational Control System, known as GPS OCX.[61] Global Positioning System (GPS) has 4.5 million commercial installations and over 1 million federal installations.

In recent years, Lenovo's role in the development of unethical facial recognition has come to light. In December 2020, the Washington Post described a chilling patent application by Huawei, the Chinese Academy of Sciences, and Megvii for the identification of Uighur Muslims at large in Western PRC and automatically reporting them to the police.[62] Megvii was censured

[59] Theresa Hitchens, "Raytheon Gets OK, $378M To Replace Risky OCX Hardware," *Breaking Defense* (blog), March 27, 2020, https://breakingdefense.com/2020/03/raytheon-gets-ok-378m-to-replace-risky-ocx-hardware/.
[60] "Aegis Combat System," Lockheed Martin, accessed July 28, 2020, https://www.lockheedmartin.com/en-us/products/aegis-combat-system.html.
[61] "GPS Next-Generation Operational Control System | Raytheon Intelligence & Space," Raytheon Intelligenve and Space, accessed July 28, 2020, https://www.raytheonintelligenceandspace.com/capabilities/products/gps-ocx.
[62] Drew Harwell and Eva Dou, "Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says," Washington Post (blog), December 8, 2020. https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-softwa re-that-could-recognize-uighur-minorities-alert-police-report-says/. See also IPVM Team. "Huawei/Megvii Uyghur Alarms" December 8, 2020. https://ipvm.com/reports/huawei-megvii-uygur

by the Department of Commerce in 2019 for the use of its flagship product Face++, an open-source facial recognition platform, in repression of Uighur Muslims in Western PRC.[63]

Lenovo has long been an early/stage investor in biometric technologies including Face++ and uses the technology in its laptops.[64] Lenovo also develops proprietary facial recognition technologies like LeFace and Veriface which are purported to be more accurate than Face++.[65] A recent academic paper highlights that LeFace is more "racially fair" than Face++, suggesting that it does a better job to detect Uighur Muslims.[66]

Lenovo partnered with CAS Institute of Automation to develop facial recognition technologies, as Lenovo identified the weakness of software and wanted to move to biometric identification.[67] Lenovo is a founding member of the FIDO Alliance based in Mountain View, CA.[68] It is documented that Lenovo was a lead investor in Megvii which produces Face++. Lenovo is also listed as a key customer and the Face++ is used in many of its laptops.[69] It is considered one the key stars in the Lenovo portfolio.[70]

The widespread deployment of Megvii's Face++ technology in consumer products such as smartphones made by Huawei, Xiaomi and Vivo; "smile-to-pay" terminals by Alibaba; and laptops made by Lenovo (in addition to Lenovo seeding Face++ development[71]) have caused

[63] "Addition of Certain Entities to the Entity List," Federal Register, October 9, 2019, https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.
[64] "Lenovo Capital and Incubator Group Created to Advance Core Technology Investments," *Lenovo StoryHub* (blog), accessed September 17, 2021, https://news.lenovo.com/pressroom/press-releases/lenovo-capital-and-incubator-group-created-to-advance-core-technology-investments/.
[65] "Lenovo Research," accessed September 17, 2021, http://research.lenovo.com/webapp/view_English/ResearchNews.html?id=404&type=1.
[66] Sheng Shi et al., "Algorithm Bias Detection and Mitigation in Lenovo Face Recognition Engine," in *Natural Language Processing and Chinese Computing*, ed. Xiaodan Zhu et al., Lecture Notes in Computer Science (Cham: Springer International Publishing, 2020), 442–53, https://doi.org/10.1007/978-3-030-60457-8_36.
[67] "Institute of Automation," accessed September 17, 2021, http://english.ia.cas.cn/.
[68] "History of FIDO Alliance," *FIDO Alliance* (blog), accessed September 17, 2021, https://fidoalliance.org/overview/history/.
[69] "China's AI Start-up Megvii Raising $500 Million at $3.5 Billion Valuation: Sources," *Reuters*, December 10, 2018, sec. Technology Photos, https://www.reuters.com/article/us-megvii-fundraising-idINKBN1O90AV.
[70] "Lenovo Leads $10M Investment in 6-Legged Robot Maker Vincross," *TechCrunch* (blog), accessed September 17, 2021, https://social.techcrunch.com/2019/02/19/vincross-raises-10-million/.
[71] "Lenovo Capital and Incubator Group Created to Advance Core Technology Investments," *Lenovo StoryHub*

understandable concern.[72] The PRC's development and use of surveillance technology for repression of human rights has sparked a global backlash from the Department of Commerce Entity List with its designation of Megvii for use of the technology on Uighur Muslims in Western PRC[73]; condemnation by Human Rights Watch,[74] and variety of bans and regulations proposed by Council of Europe on the development of facial recognition.[75]

In acquiring IBM's laptop division, which employed some 15,000 workers in North Carolina's Research Triangle Park in 2004, Lenovo promised[76] to grow employment in the region. But today, less than 2000 of Lenovo's 63,000 employees are located in the United States. Today, Lenovo is the world's leading maker of laptops and a leading maker of servers.[77] Lenovo's acquisitions of key US computer and mobile brands were critical parts of PRC's strategy of "techno-nationalism", the use of technology to shape the culture and politics of the nation.[78] Its Chairman and CEO Yang Yuanqing is one of the richest people in the PRC. He is known as much for his leadership in the company and the Chinese Communist Party (CCP), having led the National Committee of the Chinese People's Political Consultative Conference, a

(blog), May 6, 2016, https://news.lenovo.com/pressroom/press-releases/lenovo-capital-and-incubator-group-created-to-advance-core-technology-investments/.

[72] "Facial Recognition Specialist Megvii Plans Share Sale," *BBC News*, August 26, 2019, sec. Technology, https://www.bbc.com/news/technology-49473583.

[73] "Addition of Certain Entities to the Entity List," Federal Register, October 9, 2019, https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.

[74] Maya Wang, "The Robots Are Watching Us," Human Rights Watch, April 6, 2020, https://www.hrw.org/news/2020/04/06/robots-are-watching-us.

[75] "Consultative Commiittee of the Convention for the Protection Og Individuals with Regard to the Automatic Processing" (Convention 108, January 28, 2021), https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

[76] "Exclusive: 20 Minutes with Yuanqing Yang, CEO of Lenovo," Triangle Business Journal, accessed September 17, 2021, https://www.bizjournals.com/triangle/blog/techflash/2014/03/exclusive-20-minutes-with-yuanqing-yang-ceo-of.html.

[77] "Report: Worldwide PC Market Rises 13% in Q2 2021, Lenovo and HP Take the Top Two Spots," GSMArena.com, accessed September 17, 2021, https://www.gsmarena.com/report_worldwide_pc_market_rises_13_in_q2_2021_lenovo_and_hp_take_the_top_two_spots-news-50005.php.

[78] "Research | U.S.- CHINA | ECONOMIC and SECURITY REVIEW COMMISSION," accessed September 17, 2021, https://www.uscc.gov/research/PRCs-technonationalism-toolbox-primer.

group of elites that includes more than 50 Chinese billionaires who advise the Politburo.[79]

On a related point, Hytera noted in its filing in this proceeding that its "founder and majority shareholder is not associated with and has never been a member of the Chinese Communist Party ("CCP")." This is a significant admission and demonstrates the reality and perception that being a CCP member is associated with underhanded PRC government practice. Notably, Hytera wants to demonstrate distance from the PRC government and took great pains to make this point in its meeting with the FCC.

Given the preponderance of critical factors as defined by the Secure and Trusted Networks Act, the FCC should add Lenovo to its Covered List.

G. Case Study: Yangtze Memory Technologies Company (YMTC)

YMTC provides an important example of a producer of key component in electronic equipment (semiconductors) which presents national security risk. Among other dangers, YMTC chips can be enabled with kill switches which can cause a device and/or network shutdown. The national security dangers posed by YMTC have been detailed by the Biden White House. Given that BIS placed Fujian Jinhua on the Entity List and designated Semiconductor Manufacturing International Corporation (SMIC) as a Military End User, it was widely expected in 2020 that YMTC would be next. BIS' delay in taking this needed action has resulted in censure by Congress.[80] It has been suggested that given their growing and record profits in the PRC, US semiconductor manufacturing equipment makers Applied Materials, KLA, and Lam Research

[79] "Top Lenovo Exec Keeps Key Chinese Government Advisory Post | WRAL TechWire," February 4, 2013, https://www.wraltechwire.com/2013/02/04/top-lenovo-exec-keeps-key-chinese-government-advisory-post/./

[80] "McCaul, Hagerty Urge Raimondo to Include the CCP's YMTC on Commerce Department Entity List". Press Release, GOP Foreign Affairs Committee. July 12, 2021. https://gop-foreignaffairs.house.gov/press-release/mccaul-hagerty-urge-raimondo-to-include-the-ccps-ymtc-on-commerce-department-entity-list/

have succeeded to deter BIS from designating YMTC for its national security risks.[81]

Without flash memory integrated circuits, the data on a smartphone or electronic device would be erased every time it ran out of power and could not be transferred between devices. Today the companies which produce the machinery to make these specialized chips reside primarily in US and a handful of democratic countries. The PRC would like to dominate and is pulling out the stops to do so, especially with YMTC. A report by Chinese military expert James Mulvenon at SOS International details YMTC and the PRC's use of subsidy, espionage, and anticompetitive and illegal practices to support it.[82] Moreover, US, EU and Asian firms accelerate this trend by actively selling and sharing advanced technology with PRC-affiliated actors like YMTC. From the FCC's perspective, it should be mindful of the fabs which produce the chips embedded into equipment which it authorizes, particularly military fabs like YMTC which could enable a kill switch on the chip.

YMTC is owned by Tsinghua Unigroup, which also controls Tsinghua University, one of PRC's most esteemed and celebrated universities, and a long-time collaborator with the Chinese Academy of Sciences and the People's Liberation Army (PLA). Tsinghua Unigroup tried to purchase US semiconductor manufacturers but was blocked by Committee on Foreign Investment of the United States.[83] [84] Tsinghua University has 9 defense laboratories.[85] YMTC

[81] Robert Castellano. "Applied Materials And Lam Research: Little Impact From Possible Demise Of China's NAND Industry." Seeking Alpha. July 19, 2021. https://seekingalpha.com/article/4439969-applied-materials-and-lam-research-little-impact-from-possible-demise-of-chinas-nand-industry
[82] Roslyn Layton, "China Aims To Dominate Flash Memory," Forbes, accessed September 17, 2021, https://www.forbes.com/sites/roslynlayton/2021/01/04/china-aims-to-dominate-flash-memory/.
[83] Eliza Gkritsi, "A Chinese Firm Made a Memory Chip that Can Compete with Samsung. What's Next?," TECHNODE (Apr. 23, 2020), https://technode.com/2020/04/23/ymtc-memory-chip
[84] *See* Eva Dou and Robert McMillan, "PRC's Tsinghua Unigroup Buy Small Stake in U.S. Chip Maker Lattice," Wall St. J. (Apr. 14, 2016), www.wsj.com/articles/PRCs-tsinghua-unigroup-buys-small-stake-in-u-s-chip-maker-lattice-1460654877
[85] Tsinghua University. (2019, November 21). Retrieved from https://unitracker.aspi.org.au/universities/tsinghua-university/?_sm_au_=iVVnpNHbKsVZHL6q01TfKK3Qv3fc4

produces a 3D NAND 64-layer device, and now has set its sights on the ambitious goal of increasing its global supply of the NAND market from 0 to 8% in just two years.[86] Huawei was identified "among the first wave of buyers" for chips produced by YMTC.[87]

The White House also called out YMTC in its June 2021 Supply Chain report noting,

> "PRC's memory projects are the most mature of all its efforts across the semiconductor spectrum. YMTC, a subsidiary of Tsinghua Unigroup, is emerging as PRC's national champion memory chip producer. Even though YMTC's 3D-NAND memory technology is untested and significantly less advanced than global leaders, it still represents a watershed moment in PRC's semiconductor ambitions, especially because YMTC was only founded in July 2016. YMTC has received an estimated $24 billion in subsidies from Chinese government sources, which was essential to the firm's rapid development."[88]

There is a repeated pattern of strategic US advantage in technology being whittled away by the PRC. Next generation flash or so-called 3-dimenional NAND represents an improvement in chip design such that the circuits are organized in a vertical 3D skyscraper fashion rather than planar 2D, like the improvement resulting from putting books on a shelf rather than laying them side by side on a table. Leading SME manufacturers produce 3D NAND circuitry approaching 200 layers—all within the space of a few nanometers or the width of a few atoms. "YMTC is focused on 128-layer and 196-layer chips, leapfrogging over earlier generations. …It plans to start

[86] Ben Yeh, "Competition in NAND Flash Market to Intensify in 2021 as YMTC Unveils 128L Products on Schedule, Says TrendForce" TRENDFORCE (Apr. 20, 2020), www.trendforce.com/presscenter/news/20200420-10280.html.
[87] Cheng Ting-Fang and Lauli Li, "How PRC's Chip Industry Defied the Coronavirus Lockdown," NIKKEI ASIAN REV. (Mar. 19, 2020), https://asia.nikkei.com/Spotlight/The-Big-Story/How-PRC-s-chip-industry-defied-the-coronavirus-lockdown
[88] "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth" (The White House, June 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

volume production of the 128-layer products later this year and targets having half of its available capacity utilized for 128-layer products by 2021 with estimates ranging of capturing 7% to 15% of global production by 2024," notes the new report by Mulvenon who specializes in strategic intelligence for US defense and government and runs a team of some 30 linguists and intelligence analysts. In 2020, he published the definitive report on Semiconductor Manufacturing International Corporation (SMIC) which demonstrated its ties to the Chinese military, a finding which was reportedly critical to the US Department of Commerce adding SMIC as a Military End User.

Commerce cited the PRC's express strategy for Civil Military Fusion in restricting SMIC, a process by which any economic input in the PRC can be commandeered for military purposes.[89] Given such a strategy, some policy experts advocate that the US needs to restrict and "decouple" its entire semiconductor industry from the PRC to avoid the displacement of US preeminence and loss of high-paying jobs.[90] They note that the PRC can game what they describe as Commerce's piecemeal efforts to restrict one or two semiconductors firms, as production can be shifted to other vulnerable entities.[91]

In any event, Mulvenon's new report details YMTC ownership by Tsinghua Unigroup which supplies the PRC military. YMTC executives and board members have participated in the PRC's military modernization efforts. YMTC is also funded by the country's Integrated Circuit Industry Investment Fund, government support explicitly designed to evade World Trade

[89] "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List." Federal Register, December 12, 2020. https://www.federalregister.gov/documents/2020/12/22/2020-28031/addition-of-entities-to-the-entity-list-revision-of-entry-on-the-entity-list-and-removal-of-entities
[90] Scissors, Derek. "Partial Decoupling From China: A Brief Guide." American Enterprise Institute. July 7, 2020. https://www.aei.org/research-products/report/partial-decoupling-from-china-a-brief-guide/
[91] Ibid.

Organization restrictions on government subsidies. As it does not trade publicly, YMTC avoids investor and analyst scrutiny. “This development model precisely mirrors the rise of Huawei, which used similar “national champion” advantages, along with the benefit of state-sponsored cyber espionage, to steal the intellectual property of its competitors, driving competitors out of the market, and assuming a dominant market position,” notes Mulvenon. He adds that YMTC’s recent provision of chips for Huawei’s Mate40 phones, likely violates of the Commerce Department’s Foreign Direct Product Rule prohibitions.

It is not only the PRC’s practices which accelerate the decline of firms in democratic countries in favor of PRC supremacy. Foreign firms themselves vigorously supply YMTC. Many note that Commerce’s restrictions have not slowed their business. Mulvenon’s report details YMTC’s reliance on key foreign suppliers including Applied Materials for Wafer Fab Equipment, Dutch ASML for high-end lithography, LAM Research for high aperture etching (the unit has a dedicated Vice President for the YMTC account), KLA-Tencor, and Korea-based Nextin for metrology and inspection tools, and the California-based firm ACMR for cleaning systems.

PRC semiconductors executives appear to enjoy a revolving door between elite US institutions and the PRC government. YMTC CEO Simon Yang earned his masters and PhD at Rensselear Polytechnic Institute in New York, worked at Intel in Oregon, and was previously CEO at the now banned SMIC. More largely, US engineers and academics regularly share their semiconductor advancements perhaps unwittingly with PRC operatives at conferences and professional organizations. This underscores that some of the most important exchanges are between individuals and that PRC operatives can gain valuable human intelligence through

academic and scientific proceedings.

With YMTC, the PRC has rolled out the same playbook used successfully to displace foreign firms in the smartphone, solar panel, telecommunications equipment, flat panel displays, and LED domains. Policymakers and consumers failing to learn these lessons are doomed to repeat them.

James A. Lewis of the Center for Strategic & International Studies wrote a critical discussion of semiconductor manufacturing equipment (SME) to YMTC.[92] His starting point in that given that PRC is a hostile power, attempting to address its actions through negotiation is ineffective; the PRC will only respond to realpolitik, or consequential action. Author James Lewis notes that US policies to date have worked to slow the PRC's development of a home-grown semiconductor industry. However, he wants a policy that does not punish the American industry for the strict measures which need to be imposed. As such, he suggests that that no SME be licensed to PRC firms. Only US firms operating in the PRC should be allowed to import SME. Indeed, this would be the important measure to ensure that firms continue to realize existing revenue, the industry's key concern. Notably the measure would preclude new sales to PRC firms.

Lewis notes that careful restrictions on SME exports to PRC would slow PRC's semiconductor growth. Though the PRC has lagged in semiconductors, it is competitive with some memory chips and is moving in the logic and specialized chip domains. The PRC buys most chips from US companies, many which have fabs in the PRC. As discussed YMTC has

[92] James Andrew Lewis**. "**Managing Semiconductor Exports to PRC." Center for Strategic & International Studies. May 2020. https://www.csis.org/analysis/managing-semiconductor-exports-PRC

PLA ties. The US should restrict equipment to this company. Lewis observes,

> "Restrictions on [semiconductor manufacturing equipment] exports to PRC, if used carefully, would slow PRC's semiconductor growth. A straightforward approach would block export to Chinese companies while allowing sales to U.S. and Japanese firms, even if they are located in PRC…. If YMTC or other Chinese companies succeed in making commercially viable memory chips, a new source of supply will be introduced and shrink market share and revenue for the other producers. However, if YMTC no longer had access to Western SME or materials, this would slow the company's competitiveness, growth, and its ability to produce more advanced chips."[93]

Lewis recognizes that YMTC needs to be added to the Entity list in addition to SMIC. This measure requires effective coordination with US allies and other semiconductor countries Japan, South Korea, Netherlands, and Taiwan to avoid workarounds and defections. However, there is evidence to suggest that the governments of these countries are already aligned with the Balanced Approach.

Lewis and CSIS partnered with the State Department to develop principles for the 5G Clean Path effort to which more than 30 major telecommunications providers from 20 nations representing more than half of the world's economy have joined.[94] A similar Clean Path could be developed for the semiconductor supply chain by starting with the SME itself. Moreover, the US firms in the PRC should be encouraged to transition their operations to other countries to reduce the proximity and probability of PRC predation. Over time, US semiconductors firms will realize

[93] Lewis, J. A. (2020). Managing Semiconductor Exports to PRC (Publication). Washington, DC: Center for Strategic and International Studies.
[94] Layton, R. (2020, September 07). State Department's 5G Clean Network Club Gains Members Quickly. Retrieved September 18, 2020, from https://www.forbes.com/sites/roslynlayton/2020/09/04/state-departments-5g-clean-network-club-gains-members-quickly/

new revenue in safer, more sustainable environments.

H. Voluntary and Best Practice Measures

FTC and NIST

The Commission rightly observes the important work to promote security by the Federal Trade Commission (FTC) and the National Institute of Standards & Technology (NIST). The FTC not only maintains an important portal on IoT Security, it makes enforcements against actors for poor cybersecurity practices. This is important to discipline bad behavior when it happens, and potentially to recover damages for consumers. Indeed Executive Order 14028 tasked the two agencies to collaborate on a labeling scheme for security practices. However, as this comment will demonstrate, labels fall short because a device can be compliant with official rules but still be vulnerable to intrusion.

NIST has considerable materials on best practices and frameworks for IoT Security. It offers important tools such as the National Vulnerabilities Database and the Cybersecurity framework. Notably the publishing of vulnerabilities is an important means of transparency and facilities the resolution of shortcomings in information technology. NIST also has specific recommended practices for manufacturers including identifying expected customers and users and defining expected use cases; researching customer cybersecurity needs and goals; determining how to address customer needs and goals; planning for adequate support of customer needs and goals; defining approaches for communicating to customers; and deciding what to communicate to customers and how to communicate it. While guidance and best practices are helpful, there is no guarantee they will be implemented. NIST has no authority to force compliance or to punish bad actors.

The FCC also recognizes important materials and frameworks developed by CTIA-The Wireless Association, GSMA, the ioXt Alliance, and TIA. These are all to the good and should continue. The FCC can encourage manufacturers to implement best practices, but these are not sufficient to ensure security.

These institutions, however needed and important, cannot address fully the challenge of end user security. Notably they are valuable for US-based and trusted manufacturers, but they are not sufficient to address threats and intrusions from PRC manufacturers. Simply put, PRC intrusion can override established controls. Even if a PRC manufacturer implemented all the recommendations from FTC and NIST, a PRC actor or affiliate could intrude on the device, even though superficially lawful. This risk cannot be mitigated effectively other than not using PRC devices. As such, the FCC may be the only backstop to protect end users on their devices and has the statutory authority develop and enforce rules.

Certifications

Theoretically certification and labeling improve information and consumer choice. The consumer would see the certification and label noting a secure product and purchase accordingly. However it is possible that PRC devices could end up being able to take advantage of the US labeling scheme to demonstrate its adherence to best practices, but not disclosing that its products are vulnerable to PRC intrusion. Labels and certifications can also make a false sense of security, leading a consumer to believe she is secured from intrusion when she is not.

International standard setting bodies

The PRC has increased its presence in international standard setting bodies and in some cases has attempted to impose standards and methods of security and protocol which would further the

adoption of PRC style surveillance. The PRC has been a key promoter of new internet protocols which would be embedded in Chinese made devices.

Under General Secretary Xi, the PRC has entered a period of consolidation of its domestic internet controls and has pursued internationalizing those norms on the world stage.[95] Significantly, this includes a new design for the Internet presented to the United Nations, which includes embedded backdoors already incorporated into existing technology by Huawei and others.[96] Importantly, this includes replacing the notion of an open, borderless Internet in which information can flow freely with "internet sovereignty"--computer systems designed for social control and government surveillance. Notably, these controls and protocols are embedded in the smart and safe cities solutions offered by Chinese firms. [97][98]

To set agendas and drive technological discussions, the PRC has secured leadership positions in U.N. agencies like the International Telecommunication Union, World Summit on the Information Society, and the Internet Governance Forum and related events, like the World Summit on Information Technology. As meticulously detailed in *Hidden Hand: Exposing how the Chinese Communist Party Is Reshaping the World,* when the PRC talks of making global organizations more "inclusive," it means increasing their acceptance of authoritarian regimes and giving Chinese Communist Party (CCP) values equal weight as democratic ones.[99]

Authors Clive Hamilton and Mareike Ohlberg detail how the PRC has succeeded in

[95] Negro, Gianluigi. Internet in PRC: From Infrastructure to a Nascent Civil Society. Palgrave Macmillan, 2017.
[96] Madhumita Murgia and Anna Gross, "PRC and Huawei Propose Reinvention of the Internet," March 27, 2020, https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2.
[97] Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," August 7, 2019, https://thediplomat. com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/.
[98] Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," October 14, 2019, https://www.aspi.org.au/report/engineering-global-consent-chinese- communist-partys-data-driven-power-expansion
[99] Hamilton, Clive, and Mareike Ohlberg. Hidden hand: exposing how the Chinese Communist Party is reshaping the world. Simon and Schuster, 2020.

"Sinicizing" the U.N. by building up support for third world nations to gain a seat on the U.N. Human Rights Council, with the goal of subsequently perverting the notion of universal human rights to one that accepts "human rights with Chinese characteristics." The PRC consistently scores as one of the worst violators of human rights and "makes technology central to repression" according to Human Rights Watch.[100]

University of Virginia PRC Internet policy expert Aynne Kokas describes how the PRC influences standard-setting through national regulation, industrial dominance, and multi-stakeholder organization.[101] Notably, Chinese law requires many IT firms to insource data to the PRC, storing it on government-run servers. Meanwhile the PRC exports its laws through the practices deployed by Chinese companies abroad. A type of "cyber- sovereignty,"[102] the PRC's policy is an extension of asserted territorial rights, like those to the South PRC Sea and Taiwan Straits, to the digital domain. Literally hundreds of PRC government and military affiliated organizations are part of technology standards organizations and trade associations, such as the International Standards Organization, the International Electronic Commission, 3GPP, IEEE, Wi-Fi Alliance, the ORAN Alliance and others. The presence of PRC at these meetings also creates opportunities for PRC to conduct espionage, illicit human intelligence gathering etc. Indeed Huawei's lead role in the Wi-Fi Alliance and the development of Wi-Fi 6 is problematic.

Many companies and countries practice industrial espionage, but the PRC takes it to the next level with the integration of diplomatic, academic and military intelligence, as well as

[100] "World Report 2021: Rights Trends in PRC," Human Rights Watch, January 13, 2021, https://www.hrw. org/world-report/2021/country-chapters/PRC-and-tibet. "World Report 2020: Rights Trends in PRC's Global Threat to Human Rights," Human Rights Watch, January 3, 2020, https://www.hrw.org/world- report/2020/country-chapters/global.
[101] Kokas, Aynne, Cloud Control: PRC's 2017 Cybersecurity Law and its Role in US Data Standardization (July 26, 2019). Available at SSRN: https://ssrn.com/abstract=3427372
[102] Schneier, Bruce (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company

seemingly ordinary professionals, students and tourists, which enable the theft of intellectual property and valuable information.[103] A cursory review of the cases brought by the U.S. Department of Justice's China Initiative demonstrates many common and banal situations in which one would never suspect major IP theft to take place.[104] As such, the salespeople, account and product managers, and technicians of Chinese government-owned IT firms are uniquely placed to gather information when they service their customers.

Essentially the PRC goal is to reach the point in which hacking is no longer needed. Instead government access is built-in from the start. This means that all PRC made products and services will be designed for the purpose of government surveillance and data exfiltration.

I. FCC's Legal Authority to Conduct These Proceedings

The Communications Act is explicit about the FCC's authority to regulate devices. The FCC has jurisdiction to regulate any device used for non-federal communications under 47 USC sec. 151, which provides that the FCC's purpose is to ensure nationwide wire and radio communication service "with adequate facilities . . . for the purpose of national defense." Historically the FCC regulated end-user telephones and other devices for national security purposes, though with the advent of greater complexity and computerization, the FCC has forborne from exercising some of its authority on the national security front. Notably the FCC has adopted the equipment authorization process today which outsources some of the work to certified labs.[105] However, the FCC has this capability as it demonstrated with the actions taken

[103] Peter Mattis and Matthew Brazil, Chinese Communist Espionage: An Intelligence Primer (Naval Institute Press, 2019).
[104] "Information About the Department of Justice's PRC Initiative and a Compilation of PRC-Related Prosecutions Since 2018." Department of Justice. https://www.justice.gov/nsd/information-about- department-justice-s-PRC-initiative-and-compilation-PRC-related Accessed February 17, 2021.
[105] "Equipment Authorization," Federal Communications Commission, October 21, 2015, https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

with Huawei and ZTE on Universal Service Fund subsidies, and the Secure and Trusted Networks Act requires as much.

The Courts have affirmed the FCC's authority to engage in these restrictions for national security purposes. This was affirmed in Huawei v. FCC, denying Huawei's petition to rescind Order 19-211 denying USF funds for purchases to covered companies.[106] Indeed the judges admonished Huawei for its characterization that the FCC in making the rule was acting outside its national security jurisdiction, as if it was a "junior varsity State Department." The court observed, "Assessing security risks to telecom networks falls in the FCC's wheelhouse. And the agency's judgments about national security receive robust input from other expert agencies and officials. We are therefore persuaded that, in crafting the rule, the agency reasonably acted within the broad authority Congress gave it to regulate communications."

The information technology threats posed by the PRC cannot be mitigated other than restricting the equipment.

III. CONCLUSION

With this proceeding, the FCC has taken an important step to improve security. The Commission recognizes that its rules for equipment authorization need to be updated. We support the FCC to deny all future equipment authorizations from the five entities of the FCC's Covered List as well as to revoke past authorizations.

While the five entities on the FCC's Covered List are important to restrict, the list is not reflective of the systemic threats and vulnerabilities posed by PRC information technology and

[106] "On Petition for Review of an Order of the Federal Communications Commission, No. 19-121" (US Court, June 18, 2021), https://www.ca5.uscourts.gov/opinions/pub/19/19-60896-CV0.pdf.

how it impacts US networks. The FCC must expand the Covered List per the requirements of the Secure and Trusted Networks Acts. At the very least, this must include Lenovo and YMTC. Both these entities meet the technical and administrative criteria established by the Secure and Trusted Networks Act. Multiple US agencies have reported that traffic has been re-routed and re-directed on Lenovo equipment; DoD describes the security risk of the using the equipment and has restricted it internally. As a semiconductor fabricator, YMTC can enable kill switches on chips which can cause remote disruption if not shutdown of a piece of equipment, if not a network. YMTC has been described by the White House itself.

Given the current state of DoD and BIS lists which collectively note hundreds of RRC entities which pose unacceptable national security risks, it is possible that the FCC's Covered List could grow significantly. With this substantive inquiry and rulemaking including many pages of questions and analysis, the Commission illustrates that the Commission has made a serious and bona fide attempt to grapple with a difficult, complex subject. While some answers to the FCC's questions are not necessarily clear, the FCC has attempted to scope the boundaries of its authority and note its limitations. It is reasonable to regulate within these circumstances.

Respectfully submitted,

Roslyn Layton, PhD
Founder, China Tech Threat

Peter Wood
Program Manager, BluePath Labs

September 20, 2021