National Defense Authorization Act Section 889: Contextual Analysis of the Restriction of Certain "Covered Technologies" from the People's Republic of China

Julius Moye
Strategic Export Controls (NPTG 8526 B)
Professor Robert Shaw
Middlebury Institute of International Studies at Monterey

May 15, 2020

In the last few years there has been a greatly increased importance given to strategic trade controls (STCs) and supply chain security. The National Security Strategy of 2017 pointed to resilient supply chains as a "national priority"[1] and a Federal Acquisition Security Council was established within the executive branch via Senate Bill 3085 in December of the following year.[2] However, strategic trade controls garnered theretofore unseen public attention with the passing of the National Defense Authorization Act for Fiscal Year 2019 (NDAA FY19)[3]. The major tenets of NDAA 2019 with regard to strategic trade controls were the Export Control Reform Act (ECRA) and the Foreign Investment Risk Management Modernization Act (FIRMAA)[4]. Yet there is one piece of NDAA FY19 which has been at play for almost a year that warrants attention. Section 889 of the NDAA has caused a significant stir in legal circles and amongst industry, as its scope is still continuing to be hashed out by policymakers. Given the provisions within it, there certainly is ample reason to focus attention on this recent regulation. The following article, while brief, will seek to examine this piece of legislation in its broader context. In doing so, it will conduct the analysis through three lenses: legal, national security and international trade. This three-pronged conceptual framework for analyzing STCs may prove valuable in a time when their value as foreign policy tools appears to be on the rise.

The Legislation: Legal Perspective

Assessing Section 889 through a legal lens is essential to better understand the scope of the impact. National Defense Authorization Act Section 889 (hereinafter "Section 889" or "889") is designed as a foreign acquisition regulation (FAR) that places stipulations on the sale and use of certain "covered" technologies in the process of selling a product or providing a service to the U.S. government. It also imposes strict reporting requirements on such contractors.[5] The covered technologies are in reference to those supplied by five specified Chinese telecommunications firms: Huawei Technologies Company , ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries.

The legislation itself can be divided into two distinct sections, often referred to as Parts A and B respectively. Part A went into effect in August 2019 and covers the sale of "any equipment, system or

[1] The White House, "National Security Strategy of the United States of America", pg. 29. December 2017. <whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
[2] Federal Acquisition Supply Chain Security Act of 2018, S.3085. June 19, 2018. <https://www.congress.gov/bill/115th-congress/senate-bill/3085>
[3] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515. <https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf> [hereinafter NDAA FY19]
[4] Leiter, Michael & Gerkin, Daniel." Tightened Restrictions on Technology Transfer Under the Export Control Reform Act". Skadden, Arps, Slate, Meagher & Flom, LLP. Sept. 11, 2018. <https://www.skadden.com/insights/publications/2018/09/tightened-restrictions-on-technology-transfer>
[5] NDAA FY19, Sec. 889 [hereinafter Sec. 889]

service" that uses the abovementioned covered technologies as a "substantial or essential component."[6] The National Defense Industrial Association (NDIA) stated that many contractors have already reconfigured supply chains to weed out known products from the covered entities, while others have had issues with identification.[7] However, things become much more complex when Part B is taken into account.

Part B will go into effect in August 2020. Pursuant to the language of the NDAA, the government is prohibited from contracting "with an entity that *uses* any equipment, system, or service that uses covered telecommunications equipment."[8] This is often referred to as the "use" provision. As law firm Sheppard Mullin wrote:

> *"Think about how many things in your office might contain covered components. Obviously, your computers, phones, printers, surveillance systems, and security systems might, but the list goes well beyond those items. As written, the rule could cover your thermostat, the cars in your fleet, your copiers."*[9]

Perhaps it is unlikely that the use provision will have such a large scope. Nevertheless, it has instilled deep uncertainty among industry. Another key component of Part B is its focus on grants and loans, which extends to the health care and higher education sectors. As Jonathan Aronie notes, "the inclusion of grants within the scope of Section 889 brings within the rule's reach a number of entities that often pay little attention to Congress' annual NDAAs."[10]

The Rationale: National Security Perspective

Section 889 was preluded by Sections 1634 and Sections 1656 of NDAA FY18[11], which prohibited the use of Kaspersky's Lab products and equipment from Russian- or Chinese-connected companies in certain Department of Defense systems.[12] This is a glimpse into the rationale behind the current telecommunications provisions, for the reasoning then was to enhance cybersecurity and prevent malicious use of "backdoors" by foreign state actors. It is also informative to view 889 in the context of the FIRMMA, from which it took many of the same definitions. As Akin Gump notes, "in its explanation

---

[6] Sec. 889(a)(1)(A)

[7] Hallman, Wes. "Sec. 889 Prohibition on Certain Telecommunications and Video Surveillance Services of Equipment: The Impact on the Defense Industrial Base". Public Meeting. March 2, 2020. National Defense Industrial Association. <https://www.acq.osd.mil/dpap/dars/section889.html>

[8] Sec. 889(a)(1)(B)

[9] 2019 National Defense Authorization Act, Section 889 Q&A. Sheppard Mullin. <https://www.governmentcontractslawblog.com/wp-content/uploads/sites/108/2019/11/QA-Attachment.pdf>

[10] Aronie, Jonathan, Paddock, Michael, McCarty, Keeley. "Why the Health Care Industry Should Be Concerned About Section 889 of the 2019 National Defense Authorization Act", The National Law Review. May 13, 2020 <https://www.natlawreview.com/article/why-health-care-industry-should-be-concerned-about-section-889-2019-national-defense>

[11] National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, Sec. 1634 & 1656. <https://www.congress.gov/115/crpt/hrpt404/CRPT-115hrpt404.pdf>

[12] Wiley Law, "Update on NDAA FY18 Cyber Provisions". Feb. 2018. <https://www.wiley.law/newsletter-Update-on-NDAA-FY18-Cyber-Provisions>

for adopting the FIRRMA definition, the agencies note that Section 889 and FIRRMA have similar objectives… and that consistency in effectuating those objectives is crucial."[13]

However, there exists a much broader context within which Section 889 was developed. This measure has been proclaimed to be a step towards increasing interoperability between the United States and its allies. It may also prove to be one of several key approaches in forcibly decreasing market access for Chinese companies on a global scale. It is informative to turn to some provisions of the most recent NDAA to further understand this broader context. Section 1260(I) strictly conditionalizes the ability of the Department of Commerce to remove Huawei from the BIS Entity List, while the Supply Chain and Counterintelligence Risk Management Task Force was created via Section 6306.[14] These and many other steps are working to address the potential threat of foreign technological industry on both the supply and demand sides of the coin. As Hdeel Abdelhady succinctly put it, "the race to dominate future technologies like artificial intelligence and 5G underpins the most complex legal and policy issues between the two nations [U.S. and China]."[15] The reality of trade controls moving from merely restrictive mechanisms to something much wider in scope appears evident.

The notion of "unrestricted warfare"[16] by China has been circulating amongst foreign policy circles for some time now and, whatever its objective veracity, it seems to have mobilized a swift and comprehensive response by the U.S. in recent years. Thus, perhaps strategic trade controls should be viewed as not merely a set of defensive regulations (countering nuclear proliferation, IP theft, etc.), but also potentially offensive measures in a struggle in which trade, technology and critical infrastructure have become the focal points of international power dynamics. Viewing Section 889 in tandem with the ECRA (whose proposed list of "emerging and foundational technologies" conspicuously mirrors sectors included in the "Made in China 2025" initiative)[17] and the recent use of the BIS Entity List hint at this prospect. Might this be a multifaceted approach to mitigate the rise of Huawei – a company which itself has been criticized for using IP theft and predatory acquisition to fell Canada's Nortel[18]– and curb China more broadly from gaining greater control over global critical infrastructure? Backdoors and surreptitious listening capabilities in U.S. government agencies are certainly worrisome, but perhaps a longer-term skirmish is what really underpins provisions like 889.

---

[13] Wolf, Kevin, Chamberlain, Chris, et. al, "Agencies Release Interim Final Rule Implementing the First Phase of 2019 NDAA Section 889". Pratt's Government Contracting Law Report. Vol. 5, No. 12. December 2019.

[14] Wiley Law, "National Defense Authorization Act for Fiscal Year 2020 Includes New Acquisition Programs and Changes to Existing Laws Impacting Contractors". Dec. 26, 2019. <wiley.law/alert-National-Defense-Authorization-Act-for-Fiscal-Year-2020-Includes-New-Acquisition-Programs-and-Changes-to-Existing-Laws-Impacting-Contractors>

[15] Abdelhady, Hdeel, "Tech War: The United States' Whole-of-Government Approach to China is a Force Multiplier". May 7, 2019. MassPoint, PLLC. <https://masspointpllc.com/us-china-techwar-wholeofgovernment/>

[16] Liang, Qiao & Xiangsui, Wang. "Unrestricted Warfare: China's Master Plan to Destroy America", 1999.

[17] Leiter, Michael & Gerkin, Daniel. " Enhanced US Export Controls and Aggressive Enforcement Likely to Impact China", Skadden, Arps, Slate, Meagher & Flom, LLP. Jan. 17, 2019. <https://www.skadden.com/insights/publications/2019/01/2019-insights/enhanced-us-export-controls>

[18] Blackwell, Tom. "Did Huawei bring down Nortel? Corporate espionage, theft, and the parallel rise and fall of two telecom giants". National Post. Feb. 20, 2020. <https://nationalpost.com/news/exclusive-did-huawei-bring-down-nortel-corporate-espionage-theft-and-the-parallel-rise-and-fall-of-two-telecom-giants>

The Economic Impact: International Trade Perspective

To briefly conclude, it is important to note what the impact of 889 may be on international trade. The economic impact is impossible to quantify given the ambiguity still present in the legislation and its implementation. Regardless, supply chains are bracing for impact. So are grant recipients in sectors such as healthcare, where just one agency (NIH), awarded over $27 billion in grants in FY 2018 alone.[19] Presumably, such awards will soon be subject to 889 scrutiny. August 2020 will be a major turning point for many organizations with government ties and the market shifts that occur as a result will be of value to measure. What the impact will be on China and the global telecommunications sector remains to be seen.

However, this may also provide some opportunities for companies to become certified NDAA-compliant providers or offer services assisting businesses in reviewing their own supply chains. Somewhat analogous to the "ITAR-free" phenomenon with EU defense contractors[20], Honeywell has already begun marketing its cameras as "NDAA-compliant"[21] and universities across the country have begun reviewing their security systems.[22] It is also projected that this will disproportionately affect small businesses who may not have the budget to self-evaluate. However, Section 889 does provide stipulations for federal agencies such as Commerce, DHS and the SBA to fund and technically assist businesses transitioning to compliant operations.[23] While the final reach of the rule is being hashed out (FCC hearings[24] have already begun narrowing it to some extent and there are *de minimis* and waiver exceptions built into 889), experts claim that many business will seek to purge the covered entities entirely so as to minimize risk. Furthermore, the Security Industry Association stated that "it may not be feasible to replace the equipment at facilities in parts of the world where compliant alternatives are not available locally,"[25] serving as an additional obstacle for business.

In an age where trade and national security are becoming increasingly intertwined, Section 889 points to a larger impact on the horizon for international trade as both an operation and as a field of study. Indeed, such a conflation may not be without its practical reasons and the cost of not adopting such legislation is up for debate. Nevertheless, strategic trade controls are clearly taking a more prominent place in foreign policy across the globe and the byzantine realm of STC legislation provides an important window into the development of the 21st Century *realpolitik.*

---

[19] Id 10

[20] Stein, Roland. " The rise of ITAR-free procurement in Europe". Who's Who Legal. Sept. 24, 2018 <https://whoswholegal.com/features/the-rise-of-itar-free-procurement-in-europe>

[21] Honeywell International, Inc. "National Defense Authorization Act (NDAA)" <https://www.security.honeywell.com/ndaa>

[22]Homeland Safety Systems, Inc. "NDAA and HR5515: What They Mean For Video Surveillance". June 24, 2019. <https://www.homelandsafetysystems.com/ndaa-hr5515-and-what-they-mean-for-video-surveillance/>

[23] Sec. 889(b)(2)

[24] Federal Communications Commission, "In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Reply Comments of the Rural Wireless Association, Inc.". WC Docket No. 18-89. Dec. 7, 2018 <https://ecfsapi.fcc.gov/file/12080817518045/FY%202019%20NDAA%20Reply%20Comments%20-%20FINAL.pdf>

[25] Parker, Jake. "Public Meeting on Section 889(a)(1)(B)". Security Industry Association. Public Meeting. March 2, 2020. <https://www.acq.osd.mil/dpap/dars/publicmeeting/presentations/section889/Security%20Industry_Association-DOD_Public_Meeting_Section_889(a)(1)(B)_JakeParker.pdf>