SYM-AM-20-082

Proceedings
of the
Seventeenth Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 13–14, 2020

Published: April 20, 2020

Approved for public release; distribution is unlimited.

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Chinese Influence in Federal DoD Contracting Spend—Strategic Peril for United States

E. Cory Yoder—is a faculty member of the Naval Postgraduate School's Graduate School of Defense Management (GSDM), currently serving as a senior lecturer and Associate Dean of Instruction. Yoder was originally assigned to NPS in July 2000 on active duty as a Naval Commander and retired from active duty in 2004. In June 2004, he became a lecturer at NPS and was promoted to senior lecturer in May 2008. He has performed duties as Academic Associate (program manager) for the 815 (MBA), a three-year appointment which ended July 2005, and served as Academic Associate for the 835–MSCM (Master of Science in Contract Management program) for 12 years (2002–2014). Yoder has significant acquisition and contracting experience, combined with several challenging acquisition, logistics, industrial, headquarter, and combat support operations leadership assignments. Yoder received the Louis D. Liskin Award for Teaching Excellence in July 2016, and in December 2019 and the Rear Admiral John Jay Schieffelin Award for Excellence in Teaching for academic year 2010, presented in June 2011, and was a "Top Five Percent" nominee in academic years 2006, 2007, 2008, and 2009.

Abstract

The purpose of this ARP Symposium paper is to highlight major shifts in Chinese policy directed at infiltrating U.S. defense industries through federal contracting and supply chain assimilation and infiltration, and the necessity to enact legislation and regulations to prevent it. It represents a shorter version of a working paper in the NPS ARP working paper series under the same title. In the past decade, the amount of U.S. DoD contracted spend with Chinese national firms has skyrocketed. This represents a major strategic challenge and potential hazard for U.S. national security.

China now holds a high position in the Defense News Top 100 contractor profile. Examining the top 20 of the top 100 shows the new preeminence of China and its emergence as a strong participant in the receipt of U.S. defense spend. Seven of the top 20 DoD spend recipient firms are Chinese. Totaling the amount of spend with Chinese firms from the 2018 data in the 2019 extraction yields $92,040 defense revenue in millions of dollars—in other words, more than $92 billion. The change in one decade, from zero dollars to more than $92 billion is significant in terms of sheer value, but also in the strategic inroad that it represents in the United States' reliance on China on prime contract support. This includes hardware and services.

This paper highlights the major issues and challenges the DoD faces in protecting its military systems from Chinese influence and outright compromise, which can damage U.S. national security. The Chinese, through its long-term strategy "China Made 2025" and the "Belt and Road" initiatives, plan to take control of major portions of U.S. intellectual, technological, and production capability. And this isn't just in theory; it's been happening and is happening currently. The Chinese have a long-term vision, more so than most U.S. policy-makers and business planners are accustomed. The long-term Chinese vision, although already showing strong inroads, and dangerously proactive measures to acquire and supplant U.S. supply chains, through U.S. contracting out, outsourcing, green-fielding, and corporate and political influence and takeover is a Sun Tzu strategy—long term and persistent. And take note! This is not a flash fad that the Chinese will abandon easily or without a fight. For every step the United States takes, and will take in the future, it's very likely going to be met with a subtle, yet effective, counter-plan. Sun Tzu strategy calls for long term vigilance—the Chinese are noted for their persistence. But that doesn't mean the United States should not take proactive action to stop the many talons of Chinese communist infiltration of our supply chains, productive capabilities and capacities, and intellectual property assimilation and piracy. On the contrary, the United States should do everything at its disposal to end the onslaught. This is a call to action!

Introduction

Purpose

The purpose of this ARP Symposium paper is to highlight major shifts in Chinese policy directed at infiltrating U.S. defense industries through federal contracting and supply chain assimilation and infiltration, and the necessity to enact legislation and regulations to prevent it. It represents a shorter version of a working paper in the NPS ARP working paper series under the same title. In the past decade, the amount of U.S. DoD contracted spend with Chinese national firms has skyrocketed. This represents a major strategic challenge and potential hazard for U.S. national security. First, when discussing national security, it's essential to understand the current elements of the National Security Strategy (NSS) and National Military Strategy (NMS).

The National Security Strategy (NSS)

President Donald J. Trump's National Security Strategy of the United States of America, dated December 2017, directly references China and Chinese threats to U.S. security and prosperity 16 times and indirectly dozens more (White House, 2017).

> A Competitive World
>
> The United States will respond to the growing political, economic, and military competitions we face around the world.
>
> China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity. They are determined to make economies less free and less fair, to grow their militaries, and to control information and data to repress their societies and expand their influence. (White House, 2017)

Within the second pillar of the NSS, "Promote American Prosperity," the strategy specifically calls for the promotion and protection of the U.S. National Security Innovation Base, to wit:

> Every year, competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars. Stealing proprietary technology and early-stage ideas allows competitors to unfairly tap into the innovation of free societies. Over the years, rivals have used sophisticated means to weaken our businesses and our economy as facets of cyber-enabled economic warfare and other malicious activities. In addition to these illegal means, some actors use largely legitimate, legal transfers and relationships to gain access to fields, experts, and trusted foundries that fill their capability gaps and erode America's long-term competitive advantages.
>
> We must defend our National Security Innovation Base (NSIB) against competitors. The NSIB is the American network of knowledge, capabilities, and people—including academia, National Laboratories, and the private sector—that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life. The genius of creative Americans, and the free system that enables them, is critical to American security and prosperity.
>
> Protecting the NSIB requires a domestic and international response beyond the scope of any individual company, industry, university, or government agency. The landscape of innovation does not divide neatly into sectors. Technologies that are part of most weapon systems often originate in diverse

> businesses as well as in universities and colleges. Losing our innovation and technological edge would have far-reaching negative implications for American prosperity and power. (White House, 2017)

The National Military Strategy (NMS)

The National Military Strategy, naturally follows the construct of the NSS. In its abbreviated non-classified version, titled *Description of the National Military Strategy 2018*, by the Joint Staff, China and Russia are directly identified as part of the NMS strategic approach (Joint Chiefs of Staff [JCS], 2019). Specifically, the short eight-page description states:

> From its global perspective, the NMS premises an adaptive and innovative Joint Force capable of employing its capabilities seamlessly across multiple regions and all domains—continuing the transition from a regional to a global mindset and approach.
>
> This strategy anchors its approach against a set of clearly identified security trends outlined in the NDS (see inset).
>
> **NDS Relevant Security Trends**
> - Reemergence of great-power competition
> - Post-World War II order—resilient but weakening
> - Technology and the changing character of war: diffusion, competition, and new threats
> - Empowered non-state actors
> - Homeland is no longer a sanctuary
> - Threat of weapons of mass destruction (WMD)
> - Allies and partners—evolving opportunities
> - Battle of narratives
> - Scale and urgency of change
>
> These trends, especially those posed by the reemergence of great power competition with China and Russia, represent the most difficult challenges facing the Joint Force. However, the full scope of global integration must recognize uncertainty and be vigilant for emerging threats to the security and interests of the United States, its allies and partners. In a security environment where the homeland is no longer a sanctuary and every operating domain is contested, competitors and adversaries will continue to operate across geographic regions and span multiple domains to offset or erode Joint Force advantages. (JCS, 2019)

Then and Now—Examining the Top DoD Contractors and the Increased Presence of the Chinese over the Past Decade

Top DoD Contractors—2009

An examination of top DoD contractors highlights recent changes in the nationality of major contractors in the DoD. For specifics, in 2009, a decade ago, there were no Chinese flagged firms in the top 100 contractors and companies receiving U.S. DoD contracted dollars. Figure 1 shows the profile of companies making up the top 20 of the top 100 in 2009 (*Defense News Online*, 2019).

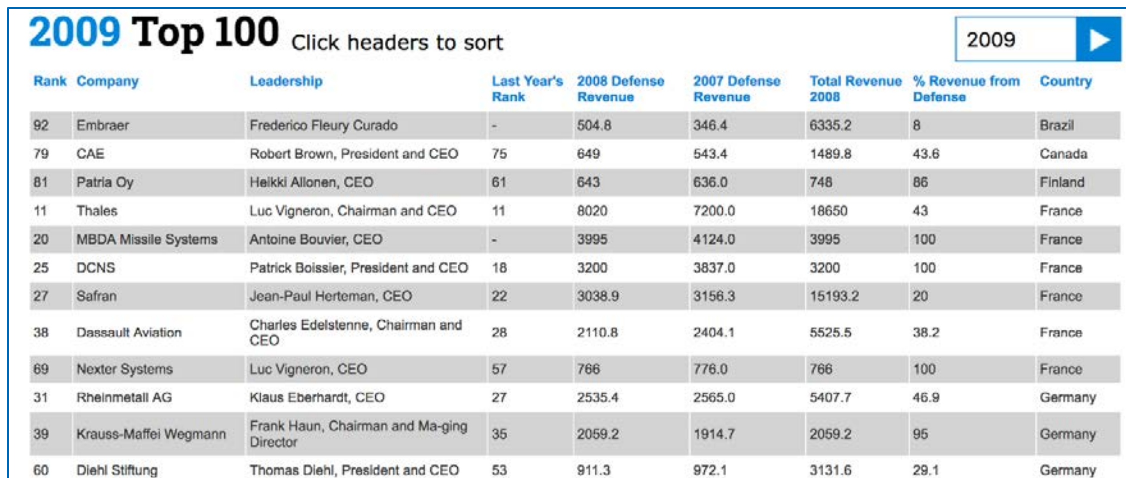
2009 Top 100 Click headers to sort 2009

Rank	Company	Leadership	Last Year's Rank	2008 Defense Revenue	2007 Defense Revenue	Total Revenue 2008	% Revenue from Defense	Country
1	Lockheed Martin	Robert Stevens, Chairman, President and CEO	1	39550	38513.0	42731	92.5	U.S.
2	BAE Systems	Ian King, CEO	3	32667	29800.0	34351	95.1	U.K.
3	Boeing	W. James McNerney, Chairman, President and CEO	2	31082	31175.0	60909	51	U.S.
4	Northrop Grumman	Ro-ld Sugar, Chairman and CEO	4	26579	24497.0	33887	78.4	U.S.
5	General Dy-mics	Jay Johnson, President and CEO	5	22854	21519.0	29300	78	U.S.
6	Raytheon	William Swanson, Chairman and CEO	6	21551.8	19809.9	23174	93	U.S.
7	EADS	Louis Gallois, CEO	7	16206.6	12241.3	63639.4	25.5	Netherlands
8	L-3 Communications	Michael Strianese, Chairman, President and CEO	8	12159	11239.0	14901	81.6	U.S.
9	Finmeccanica	PierFrancesco Guarguaglini, President and CEO	9	10219	9861.0	22119	46.2	Italy
10	United Technologies	Louis R. ChÃªnevert, President and CEO	10	9975.8	8761.4	58681	17	U.S.
11	Thales	Luc Vigneron, Chairman and CEO	11	8020	7200.0	18650	43	France
12	SAIC	Ken Dahlberg, Chairman and CEO	12	7661	6503.0	10070	76	U.S.
13	ITT	Steven Loranger, Chairman, President and CEO	17	6282	4176.0	11694.8	53.7	U.S.
14	KBR	William Utt, Chairman, President and CEO	13	5997.1	5967.0	11581	51.8	U.S.
15	Honeywell	David Cote, Chairman and CEO	14	5313	5017.0	36556	14.5	U.S.
16	Almaz-Antei	Vladislav Menshikov, Director	24	4335.2	2782.1	4616.8	93.9	Russia
17	Rolls-Royce	(Sir) John Rose, CEO	16	4237.6	4402.8	16950.6	25.2	U.K.
18	GE Aviation	David Joyce, President and CEO	15	4000	4500.0	19200	20.8	U.S.
19	-vistar	Daniel Ustian, Chairman, President and CEO	89	4000	429.0	14724	27.2	U.S.
20	MBDA Missile Systems	Antoine Bouvier, CEO	-	3995	4124.0	3995	100	France

Figure 1. 2009 Top 20 DoD Contractors. Data Sorted by Revenue in Prior Year. (*Defense News Online*, 2019).

Notice that a clear majority of the top 20 firms in 2009 sorted by total defense revenue are for U.S. and NATO country firms. The notable exception is Almaz-Antei ranked 16th from Russia, a company that specializes in anti-aircraft weapons and military technical support for intelligence and communications (*Defense News Online*, 2019).

Specifically sorting the *Defense News* data from 2009 by country, the results show no Chinese firms in receipt of DoD dollars. Again, there is no reported direct DoD contract dollars awarded to Chinese firms in the 2008 year (as reported in the 2009 snapshot).



2009 Top 100 Click headers to sort — 2009

Rank	Company	Leadership	Last Year's Rank	2008 Defense Revenue	2007 Defense Revenue	Total Revenue 2008	% Revenue from Defense	Country
92	Embraer	Frederico Fleury Curado	-	504.8	346.4	6335.2	8	Brazil
79	CAE	Robert Brown, President and CEO	75	649	543.4	1489.8	43.6	Canada
81	Patria Oy	Heikki Allonen, CEO	61	643	636.0	748	86	Finland
11	Thales	Luc Vigneron, Chairman and CEO	11	8020	7200.0	18650	43	France
20	MBDA Missile Systems	Antoine Bouvier, CEO	-	3995	4124.0	3995	100	France
25	DCNS	Patrick Boissier, President and CEO	18	3200	3837.0	3200	100	France
27	Safran	Jean-Paul Herteman, CEO	22	3038.9	3156.3	15193.2	20	France
38	Dassault Aviation	Charles Edelstenne, Chairman and CEO	28	2110.8	2404.1	5525.5	38.2	France
69	Nexter Systems	Luc Vigneron, CEO	57	766	776.0	766	100	France
31	Rheinmetall AG	Klaus Eberhardt, CEO	27	2535.4	2565.0	5407.7	46.9	Germany
39	Krauss-Maffei Wegmann	Frank Haun, Chairman and Ma-ging Director	35	2059.2	1914.7	2059.2	95	Germany
60	Diehl Stiftung	Thomas Diehl, President and CEO	53	911.3	972.1	3131.6	29.1	Germany

Figure 2. 2009 Contractors by Country. Data Sorted by Country in Prior Year. (*Defense News Online*, 2019).

Top DoD Contractors—2019

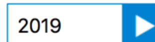
A little over a decade later, in 2020, utilizing the most recently available data from the October 2019 database, the statistics are strikingly different. China now holds a high position in the *Defense News* contractor profile. Examining the top 20 of the top 100 shows, the new preeminence of China and its emergence as a strong participant in the receipt of U.S. defense spend. Seven of the top 20 DoD spend recipient firms are Chinese. Totaling the amount of spend with Chinese firms from the 2018 data in the 2019 extraction yields $92,040 defense revenue in millions of dollars—in other words, more than $92 billion. The change in one decade, from zero dollars to more than $92 billion is significant in terms of sheer value, but also in the strategic inroad that it represents in the United States' reliance on China on prime contract support. This includes hardware and services. And of further note, the data collected by *Defense News* only show the consolidated values of prime contracts, not subcontracts. The Federal Procurement Data System-Next Generation (FPDS-NG) only reports prime contract data, not subcontract data. So, a large firm acting as an integrator, which often occurs, won't reflect the amounts that a prime has placed on their own contracts, at any level or tier. No subcontract data is reflected in the tables. Of particular note is that on average, complex systems contracts may have up to 50%–70% of the prime dollars further awarded to suppliers and subcontractors—for tangible goods, manufacturing, and services. So, the likelihood that the $92 billion dollars represented is an understatement of the actual amount of U.S. dollars being spend with Chinese firms.

The DoD top contractor data collected is limited to prime contractors—stemming from limitations of the data collection systems currently utilized within the DoD—the Federal Procurement Data System–Next Generation (FPDS-NG). According the FPDS-NG introduction page, the following data elements will not be found in FPDS-NG. Contracting officers can't put this information in FPDS-NG even if they want to. Most of this data resides at the individual contracting office.

- Subcontracting data from either the government or the prime contractors with whom we do business. The government does have a method to collect this data at www.esrs.gov. The two data sources work together (Federal Procurement Data System–Next Generation, 2020).

Top 100 for 2019

2019 Top 100 Click headers to sort



Rank	Last Year's Rank	Company	Leadership	Country	2018 Defense Revenue (in millions)	2017 Defense Revenue (in millions)	% Defense Revenue Change	2018 Total Revenue (in millions)	Revenue From Defense
1	1	Lockheed Martin [1]	Marillyn Hewson, Chairman, President and CEO	U.S.	$50,536.00	$47,985.00	5%	$53,762.00	94%
2	5	Boeing [2]	Dennis Muilenburg, Chairman, President and CEO	U.S.	$34,050.00	$20,561.00	66%	$101,127.00	34%
3	4	Northrop Grumman	Kathy J. Warden, CEO and President [*]	U.S.	$25,300.00	$21,700.00	17%	$30,095.00	84%
4	2	Raytheon Company [1]	Thomas Kennedy, Chairman and CEO	U.S.	$25,163.94	$23,573.64	7%	$27,058.00	93%
5	NEW	Aviation Industry Corporation of China	Tan Ruisong, Chairman of the Board, and Luo Ronghuai, President	China	$24,902.01	$22,898.73	9%	$66,405.36	38%
6	6	General Dynamics	Phebe Novakovic, Chairman and CEO	U.S.	$24,055.00	$19,587.00	23%	$36,200.00	66%
7	3	BAE Systems [3]	Charles Woodburn,CEO	U.K.	$22,477.48	$22,380.04	0%	$24,569.06	91%
8	NEW	China North Industries Group Corporation Limited	Jiao Kaihe, Chairman, and Liu Dashan, President	China	$14,777.77	$14,206.36	4%	$68,100.30	22%
9	7	Airbus [4]	Guillaume Faury, CEO [*]	Netherlands/France	$13,063.82	$11,185.91	17%	$75,220.59	17%
10	NEW	China Aerospace Science and Industry Corporation	Gao Hongwei, Chairman of the Board, and Liu Shiquan, General Manager	China	$12,130.93	$11,206.28	8%	$37,909.17	32%
11	NEW	China South Industries Group Corporation	Xu Ping, CEO, and Gong Yande, Director and General Manager	China	$11,963.37	$14,121.77	-15%	$38,591.53	31%
12	NEW	China Electronics Technology Group	Xiong Qunli, Chairman	China	$10,275.58	$9,518.91	8%	$33,354.01	31%
13	10	Leonardo	Alessandro Profumo, CEO	Italy	$9,828.51	$8,856.48	11%	$14,453.69	68%
14	NEW	China Shipbuilding Industry Corporation	Hu Wenming, Chairman of the Board, and Wu Yongjie, President	China	$9,795.47	$9,337.91	5%	$48,977.36	20%
15	8	Almaz-Antey	Yan Novikov, CEO	Russia	$9,660.14	$9,125.02	6%	$9,896.67	98%
16	9	Thales [1]	Patrice Caine, Chairman and CEO	France	$9,575.57	$8,926.13	7%	$18,775.63	51%
17	11	United Technologies [1, 5]	Gregory Hayes, Chairman and CEO	U.S.	$9,310.00	$7,826.00	19%	$66,500.00	14%
18	12	L3 Technologies [6]	Bill Brown, Chairman, President and CEO	U.S.	$8,249.00	$7,749.00	6%	$10,200.00	81%
19	NEW	China Aerospace Science and Technology Corporation	Wu Yansheng, Chairman of the Board, and Yuan Jie, Executive Director and President	China	$8,138.47	$7,514.73	8%	$38,030.23	21%
20	13	Huntington Ingalls Industries [1]	Mike Petters, President and CEO	U.S.	$7,767.00	$7,030.00	10%	$8,176.00	95%

Figure 3. 2019 Top Contractors. Data Sorted by Country in Prior Year. (*Defense News Online*, 2019).

Another way to view the Chinese push into U.S. DoD through contracting phenomenon is to sort the 2019 data by country—isolating Chinese firms specifically, as shown in Figure 4. The company ranking in the DoD Top 100 profile is listed in the left-most column. This is significant in terms of total dollars, more than 92 billion in the 2019 year reporting the 2018 data, but also in terms of the relative ranking of the firms in the list.

5	NEW	Aviation Industry Corporation of China	Tan Ruisong, Chairman of the Board, and Luo Ronghuai, President	China	$24,902.01	$22,898.73	9%	$66,405.36	38%
8	NEW	China North Industries Group Corporation Limited	Jiao Kaihe, Chairman, and Liu Dashan, President	China	$14,777.77	$14,206.36	4%	$68,100.30	22%
10	NEW	China Aerospace Science and Industry Corporation	Gao Hongwei, Chairman of the Board, and Liu Shiquan, General Manager	China	$12,130.93	$11,206.28	8%	$37,909.17	32%
11	NEW	China South Industries Group Corporation	Xu Ping, CEO, and Gong Yande, Director and General Manager	China	$11,963.37	$14,121.77	-15%	$38,591.53	31%
12	NEW	China Electronics Technology Group	Xiong Qunli, Chairman	China	$10,275.58	$9,518.91	8%	$33,354.01	31%
14	NEW	China Shipbuilding Industry Corporation	Hu Wenming, Chairman of the Board, and Wu Yongjie, President	China	$9,795.47	$9,337.91	5%	$48,977.36	20%
19	NEW	China Aerospace Science and Technology Corporation	Wu Yansheng, Chairman of the Board, and Yuan Jie, Executive Director and President	China	$8,138.47	$7,514.73	8%	$38,030.23	21%
22	NEW	China State Shipbuilding Corporation	Lei Fan Pei, Chairman, and Yang Jin Cheng, General Manager	China	$4,954.07	$4,842.69	2%	$30,962.94	16%

Figure 4. 2019 Chinese Companies Doing Contracted Business with the DoD from the Top 100 List. (*Defense News Online*, 2019).

Why the Incursion? "China Made 2025" and "Belt and Road" Doctrines Explained

"China Made 2025" Doctrine by the Chinese Government

The trend of increasing engagement of Chinese firms within U.S. DoD contracting, can be explained, in part, by the recent Chinese industrialization doctrine titled "China Made 2025." According to the Council on Foreign Relations and many other sources, the Chinese government launched the "Made in China 2025" initiative in 2015 (McBride & Chatzky, 2019). The Chinese state-led initiative is an industrial policy that has, as its aim, domination in global high-tech manufacturing. The program uses Chinese government subsidies, a large-scale mobilization of state-owned enterprises (notably that's most of all Chinese international businesses), and incorporation of the strategy throughout its enterprises and endeavors.

According to authors James McBride and Andrew Chatzky with the Council on Foreign Relations, the "Made in China 2025" doctrine and the associated tactics of implementation by the Chinese will adversely affect industrialized democracies.

> For the United States and other major industrialized democracies ... these tactics not only undermine Beijing's stated adherence to international trade rules but also pose a security risk. Washington argues that the policy relies on discriminatory treatment of foreign investment, forced technology transfers, intellectual property theft, and cyber espionage, practices that have encouraged President Donald J. Trump to levy tariffs on Chinese goods and block several Chinese-backed acquisitions of technology firms. (McBride & Chatzky, 2019)

What Effect to the United States?

To reiterate, the strategic goal of "Made in China 2025" is domination of the industrial high-tech manufacturing arena on a global scale. The 10-year plan, now going into its fifth year has demonstrable impacts on the international industrial trade environment. But has it affected the industrial profile of the United States' top 100 DoD contractors? In other words, is there a correlation between "Made in China 2025" and the DoD portfolio and spend on

contract? The simple answer is YES. There is a direct correlation in the appearing, in a BIG manner, in the number of Chinese firms on the top 100 DoD contractor list, and a BIG amount of money being awarded on DoD contracts—as prime contracts—to Chinese-owned firms.

To demonstrate, the “Made in China 2025” doctrine was enacted by Beijing in 2015. Utilizing the Defense News Top 100 list and extracted the top 100 in the year just preceding the “Made in China 2025” implementation, to wit, the 2014 data, and found that within the top 100, there were no Chinese companies—none. In the years following the implementation, a slow incursion took place, until in 2019 (based on 2018 data) there were seven major Chinese firms receiving more than $92 billion dollars in DoD contacts—in that year alone.

Of particular concern, of course, is the DoD spend with China. But the “Made in China 2025” doctrine has other tines extending into the United States. For instance, the doctrine calls for very specific Chinese state and corporate actions designed to wrest control of U.S. production assets. Key pillars of the strategy and tactics include:

1. Setting explicit targets for public and private firms to achieve the established goals,
2. Providing direct subsidies via Chinese state funding, tax breaks, and other means (estimates place this at hundreds of billions),
3. Foreign investment and acquisitions—specifically acquiring U.S. firms. In 2016, the Chinese spent $45 billion in acquiring U.S. high tech firms. (McBride & Chatzsky, 2019)

“Belt and Road”—Chinese Initiative Aimed at Global Enterprise, Market Control, and Dominance

The communist Chinese government’s “Belt and Road” initiative is another central government policy aimed at restoring the silk road from a century ago. This initiative is designed to create the policies, infrastructure and means to have an Asian, Middle East, and southern European economic trade and transportation alliance under the control, albeit dominance, of the Chinese.

One of the secondary effects of the “Belt and Road” initiative is that the Chinese are executing huge amounts of capital leverage with the nations that are participating. The policy calls for large Chinese investments in infrastructure, including roads, shipyards, ports, mining and mineral extraction, fuel and oil production and distribution, etc. This investment is more often than not based on “loans” to the participating nations. These loans are significant, particularly to poorer nations that have agreed to allow the Chinese to invest in the sovereign countries. The relationship creates an insurmountable debt load on the participant nations, often with high demands being imposed by the Chinese to strong-arm participants struggling to pay on the debt. In many instances, in many African nations, and some European and Middle-Eastern nations, find themselves surrendering strategic infrastructure as a means to pay back the debt. In Italy, for example, several deep-water ports are now under the notional control of the Chinese communist government. Figure 5 indicates the current sphere of influence from the “Belt and Road” initiative (Ma, 2019).

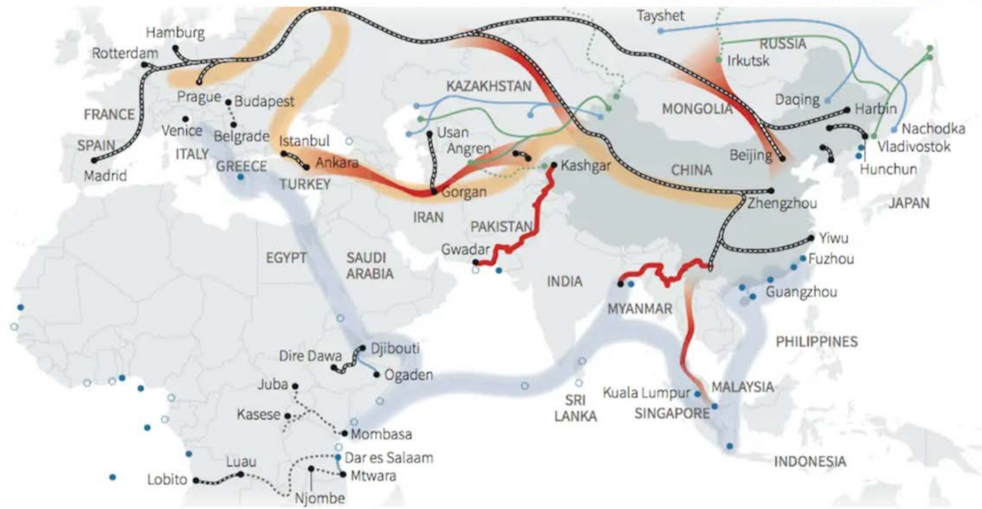


Figure 5. Sphere of Influence from the "Belt and Road" Initiatives. (Ma, 2019).

Sounds far-fetched? The Chinese communists have been employing similar tactics for decades, long before the recent "China Made 2025" and "Belt and Road" initiatives. In recent decades, there have been similar actions aimed at U.S. strategic interests. To wit, the Panama Canal, built and operated jointly with the Panamanian government, was surrendered wholly to Panama in the 1970s by then President Jimmy Carter. The Panama Canal is now under a long-term lease agreement with the Panamanian government and the People's Republic of China, which controls and operates the canal. Additionally, as another example, the Long Beach Naval Shipyard and Naval Station Long Beach, one of the West Coast's largest naval ship facilities, and home to one of only two sail-in dry docks capable of accommodating modern air craft carriers and battleships, was closed by Congressional BRAC in 1996. The original plan was to have the city of Long Beach lease the yard to a domestic U.S.-based firm for either a commercial yard or as a container shipping port facility. Several U.S. firms were in negotiations for the lease. However, in late 1996 to early 1997, plans changed—the Clinton administration directed the Naval Shipyard and Naval Station Long Beach be leased to COSCO, China Overseas Shipping Company. Now, the Chinese hold a long-term lease on what was a strategic U.S. facility and port. Now, years later, these expansionist and control-wresting policies by the Chinese Communists are done on a massive and more globalized scale, as indicated by the "China Made 2025" and "Belt and Road" initiatives.

Federal Laws and Current Practices—Not Enough to Stem the Incursions

There are some indirect approaches in dealing with the Chinese incursion into U.S. markets and supply chains—indirect in that these are significant at stemming the time of the incursions but are not a direct and specific means of addressing the phenomenon of U.S. DoD and the U.S. defense industry from spending directly and indirectly with Chinese firms. I will make specific recommendations for this later in this paper.

The White House Position On and Utilization of Tariffs and the Trade Deal

President Trump has been forceful with Chinese economic aggression and predatory international trade policies—long before recent events associated with the COVID-19 events. In September 2018, the executive branch, under President Trump, took firm and decisive action to stem unfair practices, as quoted in the following extraction:

Today, following seven weeks of public notice, hearings, and extensive opportunities for comment, I directed the United States Trade Representative (USTR) to proceed with placing additional tariffs on roughly $200 billion of imports from China. The tariffs will take effect on September 24, 2018, and be set at a level of 10% until the end of the year. On January 1, the tariffs will rise to 25%. Further, if China takes retaliatory action against our farmers or other industries, we will immediately pursue phase three, which is tariffs on approximately $267 billion of additional imports.

We are taking this action today as a result of the Section 301 process that the USTR has been leading for more than 12 months. After a thorough study, the USTR concluded that China is engaged in numerous unfair policies and practices relating to United States technology and intellectual property—such as forcing United States companies to transfer technology to Chinese counterparts. These practices plainly constitute a grave threat to the long-term health and prosperity of the United States economy.

For months, we have urged China to change these unfair practices, and give fair and reciprocal treatment to American companies. We have been very clear about the type of changes that need to be made, and we have given China every opportunity to treat us more fairly. But, so far, China has been unwilling to change its practices. To counter China's unfair practices, on June 15, I announced that the United States would impose tariffs of 25% on $50 billion worth of Chinese imports. China, however, still refuses to change its practices—and indeed recently imposed new tariffs in an effort to hurt the United States economy.

As President, it is my duty to protect the interests of working men and women, farmers, ranchers, businesses, and our country itself. My Administration will not remain idle when those interests are under attack.

China has had many opportunities to fully address our concerns. Once again, I urge China's leaders to take swift action to end their country's unfair trade practices. Hopefully, this trade situation will be resolved, in the end, by myself and President Xi of China, for whom I have great respect and affection. (White House, 2018)

U.S. Trade Laws Authorizing the President's Tariff Actions

Section 201 of the Trade Act of 1974—Allows the President to impose temporary duties and other trade measures if the U.S. International Trade Commission (ITC) determines a surge in imports is a *substantial cause or threat of serious injury* to a U.S. industry.

Section 232 of the Trade Expansion Act of 1962—Allows the President to adjust imports if the Department of Commerce finds certain products are imported in such quantities or under such circumstances as to *threaten to impair U.S. national security*.

Section 301 of the Trade Act of 1974—Allows the United States Trade Representative (USTR) to suspend trade agreement concessions or impose import restrictions if it determines a U.S. trading partner is *violating trade agreement commitments or engaging in discriminatory or unreasonable practices that burden or restrict U.S. commerce*.

Figure 6. U.S. Trade Laws Authorizing President's Tariff Actions. (Congressional Research Service [CRS], 2019).

While all three of the above provisions are being utilized, the majority of tariffed Chinese goods covered by tariffs actions fall under the provisions of Section 301 of the Trade Act of 1974. This provision allows for imposing tariffs on a trading partner that is violating agreements or commitments, or engaging in discriminatory of unreasonable practices that burden or restrict U.S. commerce. The Trump administration's position is that China has violations assorted with currency manipulation, dumping goods into U.S. markets with the intent to harm or cripple U.S. domestic industry, and technological and intellectual espionage and capture. When taken in context with the "China Made 2025" program officially instituted by the Chinese communist government, it seems clear that such actions by the Chinese and their industries was intentional, and hence, in my opinion, called for actions by the United States in diplomatic and economic capabilities to slow or halt. Note that I purposely left out the third leg of potential U.S. action sets, the military, notwithstanding the military and the DoD are those entities engaged in contracting with Chinese communist firms—the premise of this paper. Later, I will provide my findings and recommendations.

Chinese Investments in U.S. Companies and Influence Via U.S. Corporate Boards of Directors—Mergers and Acquisitions—CFIUS Reviews

Concurrent with the "China Made 2025" and "Belt and Road" initiatives, the Chinese communist government has encouraged its state-owned, state-controlled industries to either acquire major positions in U.S. firms, outright acquire them, and/or place Chinese sponsored representatives on U.S. company boards or directors.

The Committee on Foreign Investment in the United States (CFIUS) was established by President Gerald Ford in 1975. It was first exercised to supervise foreign direct investments in the United States. Its jurisdiction has since expanded, and its process has been changed to review any national security concerns related to foreign companies investing in and taking control of U.S. companies. Currently, CFIUS is composed of the heads of the Department of the Treasury, Department of Justice, Department of Homeland Security, Department of Commerce, Department of Defense, Department of State, Department of Energy, the Office of the U.S. Trade Representative and Office of Science & Technology Policy. The secretary of the Treasury is the chairperson of CFIUS.

A legal site, Fosters and Garvey, which specializes in international law, has concerns over attempted acquisitions (Li & Hoff, 2018). CFIUS is the one of the official determiners of

whether foreign investment in U.S. firms pose a security concern. According to Li and Hoff, as a recent example of CFIUS's decisions making, on January 2, 2018, CFIUS rejected foreign investment firm Ant Financial's plan to acquire U.S. money transfer company MoneyGram International over national security concerns. According to a Reuters report, CFIUS rejected the deal due to concerns over the safety of data that can be used to identify U.S. citizens. There have been several large company acquisition reviews subsequently rejected by CFIUS recently.

> A high-profile deal that was recently blocked by President Donald Trump was Canyon Bridge Capital Partners Inc.'s planned $1.3 billion acquisition of chipmaker Lattice Semiconductor Corp. on September 13, 2017, in which the President sided with CFIUS's decision that the involvement of Chinese investors presents a national security concern. This is the fourth time in the past 30 years that a U.S. president has blocked foreign companies' acquisitions in the United States due to national security concerns. All four deals have involved investors from China with three of the deals having occurred in the past five years.
>
> President George Bush blocked China Aero Technology Import & Export Co.'s acquisition of a Washington-based aerospace manufactory company, MAMCO Manufacturing, Inc. President Barack Obama blocked SANY Heavy Industry Co., Ltd–backed Ralls Corp.'s investment in building a wind power plant in Oregon because the plant was too close to a U.S. Navy base. President Barack Obama also blocked a Chinese company's acquisition of a German semiconductor company, AIXTRON SE, because the acquisition would have also included the company's U.S. subsidiary and assets in California. (Li & Hoff, 2018)

Note that there were several hundred mergers and takeovers of U.S. firms by the Chinese. The CFIUS indicates that in the reporting years 2012–2017, more than 800 acquisition transactions of U.S. firms were reviewed for security issues. Some of these seem relatively benign, such as a Chinese company making a bid to purchase a chip manufacturer that makes chips for automotive firms. Although seemingly harmless, the underlying premise is that the Chinese would acquire the intellectual property, control production, and potentially, in the longer-term, transfer production and control to China. This type of potential acquisition, in the long run, erodes the U.S. industrial based and loss of supply chain integrity and control for critical manufactured goods (Li & Hoff, 2018).

Chinese Firms Opening Production in the United States—Reverse Offshoring—Green Fielding

Closely related to mergers and acquisition of U.S. firms, a new phenomenon—Chinese opening their own production facilities in the United States—has emerged, which is called "green fielding" by many experts. Particularly in the past five years, the trend is increasing rapidly, coincident with the "China Made 2025" initiative which the Chinese implemented in 2015.

Chinese companies are spending huge sums in the United States on new projects and expansions of existing subsidiaries. Between 2000 and 2016, Chinese firms spent $8.6 billion in the United States on 778 green field investments (that is, when a parent company builds a new foreign operation from the ground up). In 2016 alone, companies spent $1.4 billion on 34 green field projects, defined and newly constructed facilities, in various manufacturing sectors. "We've seen this trend since about 2009, but there's been an uptick especially in the past two years," says Cassie Gao, a Research Analyst focusing on China's

international trade and investment flows at the Rhodium Group. “In terms of dollar value, the top industries we see are automotive and other transportation equipment, chemicals, metals, and basic materials.” (Hu, 2017).

The likelihood of increased tariffs has actually increased this trend of Chinese communist firms green fielding in the United States. With ever increasing labor costs in China, due to improvements in living standards and concurrent wage increases, the cost of conducting operations in their wholly-owned production facilities in the United States becomes more financially viable. On the plus side for the United States, this creates jobs in the new plants as demand for labor, in many cases skilled labor, is created. Seems like a good deal for Americans at face value. But the secondary effect is that once U.S. production capability and capacity is reverting to Chinese communist control. These firms must still adhere to U.S. labor laws, OSHA, etc., but the controlling firm in terms of business operations, is Chinese.

Although green fielding by China in the United States is really a recent phenomenon, South Korea and Germany have green fielded production in the United States decades earlier. To wit, BMW in South Carolina and Hyundai in Alabama as example. Japanese firms, such as Toyota, Honda, and Subaru green fielded U.S. production in the 1990s. So why the concern over China doing the same green fielding practice that other Southeast Asian countries have done? The answer lies in the intent of the Chinese as it relates to the “China Made 2025” and the “Belt and Road” initiatives. These are specifically designed to wrest control of production, technical innovation, and supply chains of Western countries in Europe and the United States. And this by a power recognized as adversarial to the United States economically and militarily.

Notably, China’s mergers and acquisitions (M&A) seem to far outnumber the amount of green fielding. But the disparity between M&A and green fielding may lessen as higher Chinese labor costs continue to increase, and the full effects of tariffs put upward pricing pressure on Chinese imported goods, particularly if the tariffs remain for a long period of time. Figure 7 shows the M&A and green fielding data trends up through 2016 as a look at what’s actually happening.

Figure 7. M&A and Green Fielding Data Trends. (Hu, 2017).

GAO Analysis of Offshoring and Foreign Investment—Effects on the DoD Industrial Base

The GAO issued a report in September 2019, titled *Defense Supplier Base Challenges and Policy Considerations Regarding Offshoring and Foreign Investment Risks*, which details many of the critical issues associated with U.S. outsourcing, M&A and green fielding by the Chinese (GAO, 2019). Unlike many other sources of information, the GAO report has very specific details of the impacts of these practices and harmful effects on the U.S. military, the DoD, and our supply chains.

According to the GAO, the DoD relies on a globalized network of suppliers for the components and technologies involved in its weapons systems. Domestic companies that offshore their operations or accept foreign investment can help the DoD save money and access more technology. But a globalized supply chain can also make it harder for the DoD to get what it needs if, for example, other countries cut off U.S. access to critical supplies (GAO, 2019).

The GAO, with assistance of the Bureau of Economic Analysis (BEA) and a panel of expert advisors, assembled for the report data gathering, analysis, and interpretation, and culminated on specific elements of the report's findings. They note that there isn't a solid body having a mission to collect and analyze data on offshoring, although the BEA does some of the work on a regular basis, along with other government departments. The BEA's publicly available data allow for high-level analyses of new foreign investments in the United States. For example, BEA data on new foreign direct investment show that annual investments from foreign entities in U.S. companies ranged from $277 billion to more than $460 billion for calendar years 2014 through 2018; see Figure 8 (GAO, 2019).

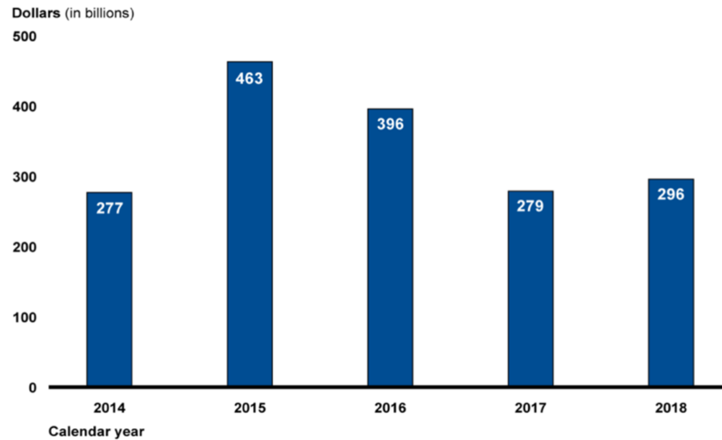


Figure 8. Annual Investments from Foreign Entities in U.S. Companies, 2014–2018. (GAO, 2019).

The ability of the Chinese to exact control over U.S. industries and supply chains, as indicated, is manifest in three primary ways, according to the GAO. Note that there are manifold methods in which the Chinese can exercise influence and control; however, the GAO report focused on the three most visible and prominent. These three, according to the GAO, are first, establishing a legally binding relationship with a U.S. firm; second, expanding a U.S.-based affiliate where a legal relationship exists, and; third, outright acquisition of a firm or its affiliate. The GAO determined that making any sound statistical analysis of the outsourcing phenomenon is challenging, as there is no agreed upon consensus of what exactly constitutes outsourcing or a commonly agreed definition, neither by industry, nor the government (GAO, 2019).

The GAO finds that foreign entities may, and often do, gain sensitive production, capability, and other information when the United States allows for foreign investment and acquisitions. This is placed directly in the context of the DoD's military hardware and software industries. To wit:

> Panelists discussed how foreign investments or offshoring business activities can, under certain circumstances, lead to a risk of transferring intellectual property or sensitive information related to critical technologies from the United States to strategic competitors and potential adversaries. This transfer of technology may, in turn, negatively affect the U.S. defense industrial base and technological superiority. According to the DoD, one of the foundations of the U.S. defense industrial base is developing and maintaining military technological superiority over strategic competitors such as China and Russia. The key to U.S. technological superiority is the development of critical and emerging technologies that are, or have the potential to be, used to support DoD weapons systems that are critical to national security.
>
> According to the DoD, foreign investment into the United States is used as a tool for strategic competitors and adversaries to obtain sensitive intellectual property in order to boost their own technological capabilities. Many of the emerging technologies critical to maintaining U.S. military superiority are dual-use technologies—with applications for both commercial and military use. Further, panelists we spoke with stated that commercial companies and

> universities are increasingly working on dual-use technologies that are of interest to the DoD. We have previously reported that the DoD has acknowledged the need to further leverage technological innovations that can be used to bolster military technology from companies that have not worked regularly with the DoD. (GAO, 2019)

These risks can be exasperated by companies that utilize "dual-use" and "single process" initiatives—those that share commonalities in technologies and production between commercial use and DoD use, with perhaps, some modifications for DoD use. Examples include using a commercial aircraft frame and propulsion system for a DoD application, such as the P8 anti-submarine warfare aircraft. The Boeing P-8 Poseidon (formerly Multi-mission Maritime Aircraft) is a military aircraft developed and produced by Boeing Defense, Space & Security, modified from the 737-800ERX (Military.com, 2020). There are numerous other examples, including Military Sealift Command (MSC) ships, training aircraft, military communications gear, and a host of others.

> China's Technology Transfer Strategy stated that China has been strategically investing in U.S. companies that develop or produce critical dual-use technologies as part of China's plans to develop its own technology base. The report noted that these investments represent a broader threat of China boosting its own military technology capability at the expense of the United States. The report also identified various ways that China seeks access to key technologies, including: (1) Chinese companies investing directly in established U.S. companies, (2) Chinese companies directly acquiring U.S companies, and (3) Chinese private equity firms investing in U.S.-based startups. For example, the DIU report stated that Chinese entities have invested more than $200 million in U.S. robotics startups from 2010 to 2017. According to the report, Chinese investments in U.S. companies can facilitate China's ability to obtain sensitive intellectual property related to the development of dual-use critical technologies from U.S. companies. Further, the report noted that the Chinese government is often directly connected to the activities of Chinese companies, which are often state-owned enterprises or enterprises with strong government connections. (GAO, 2019)

The propensity to save costs and create broader markets, both U.S. and Chinese firms have capitalized on outsourcing, contracting out, off-shoring, and green fielding. The negative effects of these 30-year trends are becoming strategically clear, and not in a positive light considering the loss of control and technological advantages the United States has lost to an economic and military adversary.

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)

The Congressional Research Service (CRS) in its February 2020 report titled *The Committee on Foreign Investment in the United States (CFIUS)* examined the background of CFIUS and recent changes to the review of foreign investment cases, instituted by President Trump's administration (Jackson, 2020). In 2018, prompted by concerns over Chinese and other foreign investment in U.S. companies with advanced technology, members of Congress and the Trump Administration enacted the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which became effective on November 11, 2018. This measure marked the most comprehensive revision of the foreign investment review process under CFIUS since the previous revision in 2007, the Foreign Investment and National Security Act (FINSA). On February 13, 2020, the Department of the Treasury issued final regulations that implement key parts of FIRRMA concerning how certain real estate and noncontrolling investments will be scrutinized. Recent changes expand CFIUS's purview to

include a broader focus on the economic implications of individual foreign investment transactions and the cumulative effect of foreign investment on certain sectors of the economy or by investors from individual countries (Jackson, 2020).

> Recently, final regulations on February 12, 2020, concerning the review process for certain real estate and noncontrolling investments.
>
> Upon enactment, FIRRMA: (1) expanded the scope and jurisdiction of CFIUS by redefining such terms as "covered transactions" and "critical technologies"; (2) refined CFIUS procedures, including timing for reviews and investigations; and (3) required actions by CFIUS to address national security risks related to mitigation agreements, among other areas. Treasury's interim rules updated and amended existing regulations in order to implement certain provisions immediately. FIRRMA also required CFIUS to take certain actions within prescribed deadlines for various programs, reporting, and other plans.
>
> FIRRMA also broadened CFIUS's mandate by explicitly including for review certain real estate transactions in close proximity to a military installation or U.S. government facility or property of national security sensitivities. In addition, FIRRMA: provides for CFIUS to review any noncontrolling investment in U.S. businesses involved in critical technology, critical infrastructure, or collecting sensitive data on U.S. citizens; any change in foreign investor rights; transactions in which a foreign government has a direct or indirect substantial interest; and any transaction or arrangement designed to evade CFIUS. Through a "sense of Congress" provision in FIRRMA, CFIUS reviews potentially can discriminate among investors from certain countries that are determined to be a country of "special concern" (specified through additional regulations) that has a "demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect U.S. leadership in areas related to national security." (Jackson, 2020)

Unfortunately, the CFIUS body has a dismal track record of success when it comes to identifying and precluding transactions the pose a "special concern" for the United States. Since the reporting protocols for transactions are volunteered by the participants to the transactions, the case itself may be packaged to steer the CFIUS decision to favor the transaction for approval. The actual number of reviewed cases that have resulted in non-approval is less than 0.5% of the cases reviewed, and these from the candidate cases that supposedly warranted special attention and scrutiny by the CFIUS board (Jackson, 2020).

However, despite the low success rate of CFIUS to halt potentially damaging international transactions with the Chinese, there is new promise that this may change. According to *Fortune* business, "On January 13, the Treasury Department issued landmark regulations that will scrutinize foreign investments into critical technology firms—especially those from China. These rules will dramatically expand the scope of the Committee on Foreign Investment in the United States (CFIUS), a U.S. interagency committee that considers the threat, vulnerability, and potential impact on national security of a foreign investment transaction. The new regulations constitute a seismic shift in the way the U.S. government views and regulates foreign direct investment (FDI)" (Ricardel, 2020).

New regulations under the Trump administration are aimed at tightening controls and broadening the definition of what is considered "threatening" to the United States. Once only focused on a strict definition of DoD security, the regulations framing and guiding the transactions for review have greatly expanded over the decades.

> This move reflects a fundamental reassessment of what constitutes U.S. national security. From 1975, when CFIUS was established by executive order, until 2001, national security was defined largely in terms of the U.S. defense posture and capabilities. Post-9/11, this was enlarged to encompass homeland security and associated infrastructure. The 2020 regulations reflect a much wider view that economic security—based on technological superiority—is a central component of America's national security. (Ricardel, 2020)

Hopefully, the new regulations expand the definition to include those transactions designed to create a technological superiority from foreign entities, such as China. But, if the CFIUS reporting and review system isn't addressed, wherein the firms party to the transaction self-report, and in essence, shape the decision, then there will not likely be any significant change in the weakening of U.S. superiority in this arena. I state this, as from the empirical record, the actual success rate, if I may phrase it as such, is less than 0.5% of all reviewed transactions. And yet, we can see the erosion of U.S. dominance in technological superiority—something that is clearly the intent of the "Chinese First 2025" initiative as discussed earlier in this work.

Export Control and Current Initiatives

Three specific legislative acts control the transfer of technology to foreign entities, firms and manufacturers, either through the sale of such technologies, or from other means such as those mentioned in the previous section. The Arms Export Control Act (AECA), the International Emergency Economic Powers Act (IEEPA), the Export Controls Act of 2018 (ECA), and other authorities, the United States restricts the export of defense articles; dual-use goods and technology; certain nuclear materials and technology; and items that would assist in the proliferation of nuclear, chemical, and biological weapons or the missile technology used to deliver them. U.S. export controls are also used to restrict exports to certain countries on which the United States imposes economic sanctions. The ECA legislates dual-use controls (CRS, 2020).

There are myriad organizations within the export control landscape that deal with transfer review and approvals, licensing, monitoring, and penalizing offenders. So many, in fact, that then-Secretary Gates called for reforming the network of agencies and entities involved in this arena to simplify and consolidate all processes and protocols.

In April 2010, then-Defense Secretary Robert M. Gates proposed an outline of a new system based on four singularities: 1) a single export control licensing agency for dual-use, munitions exports, and Treasury-administered embargoes, 2) a unified control list, 3) a single primary enforcement coordination agency, and 4) a single integrated information technology (IT) system (CRS, 2020). However, these recommendations have not been addressed or implemented.

Buy American Act—Shouldn't the DoD Be Sourcing from U.S. Firms?

The Buy American Act (BAA), based on the act's name alone, should prevent the DoD and its source manufacturers and suppliers from contracting, outsourcing, and conducting business for goods and services from China—but it doesn't. In fact, if it did, there wouldn't be the current trend exhibited wherein U.S. DoD prime contract dollars are being directly spent with Chinese firms. And add the fact that many U.S. weapons systems contractors, telecommunications contractors, and general supply and service contractors on prime and subcontracts at all tiers have seen a dramatic rise in actions and dollars spent with Chinese communist firms. This, as indicated earlier, is part of the "China Made 2025" and "Belt and Road" initiatives instituted by the Chinese government.

Examining, in a concise manner, the Buy American Act may reveal what the BAA does.

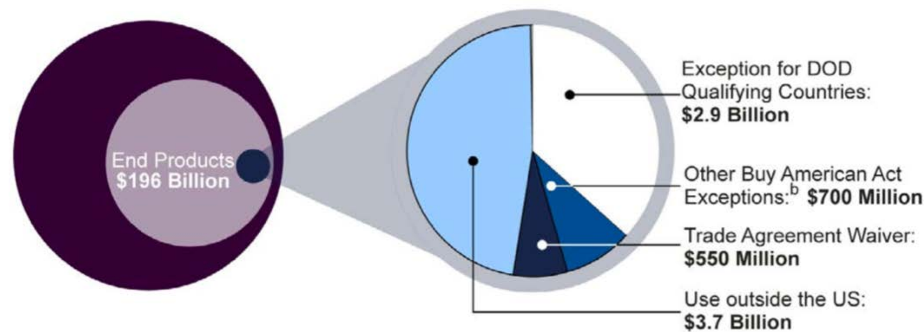
> The Buy American Act (BAA) (41 U.S.C.10a – 10d) was passed in 1933 and restricts the purchase of supplies that are not domestic end products. It applies to all U.S. federal government agency purchases of goods valued over the purchase threshold, but does not apply to services. Under the Act, all goods for public use (articles, materials, or supplies) must be produced in the U.S., and manufactured items must be manufactured in the U.S. from U.S. materials. The BAA uses a two-part test to define a domestic end product.
>
> a. The article must be manufactured in the United States
> b. The cost of domestic components must exceed 50 percent of the cost of all the components
> c. Unmanufactured products mined or produced in the United States
>
> The DoD has issued a final rule amending DFARS 252.225-7000 and 252.225-7001 provision and clause which includes a partial waiver to the two part test. The waiver allows a Commercial Off-The-Shelf (COTS) item to be treated as a domestic end product if it is manufactured in the U.S., without tracking the origin of the item's components.
>
> Exceptions that allow the purchase of a foreign end product are listed at FAR 25.103 and DFARS 225.103. (Acquisition Notes, 2020)

Some exemptions exist, including, but not limited to: public interest and pursuant to existing free trade zones, items and mined sourced materials that are not in sufficient quantities to meet demand, if U.S. sources are at unreasonable price or cost (the contracting officer's determination), and for commercial telecommunications not restricted under other provision of law.

According to a December 2018 GAO Report titled *Buy American Act—Actions Needed to Improve Exception and Waiver Reporting and Selected Agency Guidance*, only 5% of all agency procurements were subject to the BAA provisions, and out of those, over half qualified for an exemption to the BAA through either federal trade agreements, or via specific agency waivers. Of the roughly $508 billion in expenditures reported under the FPDS-NG system, which as pointed out earlier in this paper, only captures prime contract awards, only a fraction of the total was subject to BAA. Noting also, that the FPDS-NG only required the capture of BAA from 2018 and onward—much of the historical data and reporting is suspect at best. And of those initially BAA eligible, a significant number were exempted (GAO, 2018). See Figure 9.

Federal Obligations for Foreign End Products, Fiscal Year 2017

Total Federal Obligations: $508 Billion **Foreign End Product Obligations: $7.8 billion[a]**



[a] This includes nearly $16 million for awards under the micro-purchase threshold (generally $3,500 at the time of our review) that were not subject to the Buy American Act.

[b] Other Buy American Act exceptions include public interest (excluding DOD Qualifying Countries), domestic non-availability, unreasonable cost, commercial information technology, and commissary resale

Source: GAO analysis of federal procurement data. | GAO-19-17

Figure 9. Federal Obligations for Foreign End Products, FY 2017. (GAO, 2018).

One of the biggest deficiencies of the BAA, outside of the low applicability and high exemption rates, is the method of determining what is actually American. Contractors actually self-report on their products content and manufacture, and only those meeting reporting standards are required to report at all. The notion of self-reporting, only briefly addressed, is a huge concern from an accuracy, accountability, and auditability standpoint. In a student research briefing from MBA students Conan Greaser and A. J. Osman in November 2015, it was pointed out that often violations are not detected at all, due to self-reporting. And when some program contracts were reviewed and violations found, the agency issued retroactive waivers (Greaser & Osman, 2015).

So, it's my contention that the BAA has not precluded the increase in Chinese participation in federal and DoD contracts, as either prime, and certainly not at the tiered subcontract levels. The BAA, in essence, non-effectual in this regard.

On January 31, 2019, President Trump signed Executive Order 13858, "Strengthening Buy-American Preferences for Infrastructure Projects," reemphasizing the executive branch's policy preference (but not necessarily *mandate*) "to maximize ... the use of goods, products, and materials produced in the United States, in federal procurements and through the terms and conditions of federal financial assistance awards." This policy was expressed originally in Executive Order 13788, "Buy American, Hire American," which President Trump signed on April 18, 2017 (Gallacher & Chadwick, 2019).

FAR and DFARS Provisions Addressing DoD Contracting with China

How does existing legislative, Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulations (DFARS) address DoD contracting with China?

Federal law directly addresses some key issues related to DoD contracting with Communist China. The most direct instruction for contracting officers is 48 CFR § 252.225-7007—Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies. Note that there are other provisions related to technology transfer which are not directly to purpose of this paper, but should be consider in this context nonetheless. This legal provision flows down into subordinate implementing and governing citations, including:

Title 48. Federal Acquisition Regulations System

Chapter 2. DEFENSE ACQUISITION REGULATIONS SYSTEM, DEPARTMENT OF DEFENSE

Subchapter H. CLAUSES AND FORMS

Part 252. SOLICITATION PROVISIONS AND CONTRACT CLAUSES

Subpart 252.2. Text of Provisions and Clauses

Section 252.225-7007. Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies (Prohibition on Acquisition, 2015).

Parts 252 and 252 derivatives are under the DFARs, and primarily are implementing directives and solicitation and contract action clauses. They mandate protocols and policies related to contracting and contract actions with Chinese firms. These are relatively new, as deriving from the Title 48 provision from 2015. The text from DFARs Section 252.225-7007 Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies reads as follows:

PROHIBITION ON ACQUISITION OF UNITED STATES MUNITIONS LIST ITEMS FROM COMMUNIST CHINESE MILITARY COMPANIES (SEP 2006)

(a) *Definitions*. As used in this clause—

Communist Chinese military company means any entity that is—

(1) A part of the commercial or defense industrial base of the People's Republic of China; or

(2) Owned or controlled by, or affiliated with, an element of the Government or armed forces of the People's Republic of China.

United States Munitions List means the munitions list of the International Traffic in Arms Regulation in 22 CFR Part 121.

(b) Any supplies or services covered by the United States Munitions List that are delivered under this contract may not be acquired, directly or indirectly, from a Communist Chinese military company.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts for items covered by the United States Munitions List.

Figure 10. Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies.
(Prohibition on Acquisition, 2015).

The provision above addresses only munitions. Since taking office, the Trump administration has been proactive at addressing many of the deficiencies in federal regulations and federal contracting related to Chinese acquisitions. Canvassing the FAR and DFAR, for example, is a new 2019 provision emanating from the NDAA 2019—restricting telecommunications contracting with specified Chinese firms. This case was widely publicized, as it specifically deals with the Chinese firm responsible for some of the world's 5G wireless network infrastructure and technology to enable the 5G capability.

Per the Government Contracts Law online blog network, a respected resource and discussion board for current topics in federal contracting, the NDAA 2019 initiated action, which has translated into FAR provisions.

> In accordance with Section 889(a)(1)(A) of the 2019 National Defense Authorization Act (Pub. L. No. 115-232) (the "2019 NDAA"), which required imposition of broad restrictions on procurements involving certain Chinese telecommunications hardware manufacturers such as Huawei Technologies Co. and ZTE Corp within one year, the FAR Council has released an interim rule implementing these restrictions. On August 13, the FAR Council released Federal Acquisition Circular 2019-05 (84 Fed. Reg. 40,216), creating a new FAR Subpart 4.21, as well as two new contract clauses, FAR 52.204-24 and 52.204-25, all of which are effective August 13, 2019. These restrictions apply not only to prime contractors, but also to all subcontractors and throughout the supply chain. Government contractors need to know that these new requirements are effective immediately and that opportunities for waivers are very limited.
>
> Section 889(a)(1)(A) of the 2019 NDAA prohibits agencies from procuring "any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system." (Note: Section 889(a)(1)(B), which is the subject of a separate FAR Case, FAR Case 2019-009, more broadly prohibits agencies from entering into contracts with "an entity that uses any equipment, system, or services that uses covered telecommunications equipment or services as a substantial or essential component of any system…" The 2019 NDAA provides this prohibition will take effect next year—two years after enactment of the 2019 NDAA. This FAR Case is still under consideration.). (Bourne, 2019)

Although I do not incorporate all of the language in the FAR and DFARs parts from the aforementioned provision, I encourage readers to examine the provisions in their entirety. They address specific actions required and actually are applied retroactively to currently awarded contract actions and active indefinite delivery type contracts (IDIQs) and subcontracts. The provisions, much like the CFIUS provisions cited earlier in this paper, requires contractors and their subcontractors to self-report on telecommunications hardware, software, and services—the point here being self-reporting. This may have the same potential for contractors "gaming" the system to avoid being prohibited from engaging in business with the federal government and the DoD that the CFIUS provisions have encountered. And if it's the intent of a Chinese nationalized firm to exploit U.S. technology and information systems, then you can imagine they likely wouldn't report accurately and honestly, based on sound conjecture.

FAR Part 225.770 if the "Prohibition on acquisition of certain items from Communist Chinese military companies" implements section 1211 of the National Defense Authorization Act for Fiscal Year 2006 (Pub. L. 109-163), section 1243 of the National Defense Authorization Act for Fiscal Year 2012 (Pub. L. 112-81), and section 1296 of the National Defense Authorization Act for Fiscal Year 2017 (Pub. L. 114-328). See PGI 225.770 (DFARS/PGI view) for additional information relating to this statute, the terms used in this section, the United States Munitions List (USML), and the 600 series of the Commerce Control List (CCL).

This FAR Part 225.770, emanating from several iterations of NDAAs from 2006 through 2017, deals specifically with entities identified as Chinese military industries, particularly, munitions firms and weaponry. This may limit the applicability in instances where Chinese communist controlled industries are not specifically munitions firms, but, as example, high-tech commercial entities having or seeking technologies for capture or assimilation into their portfolio. This can be every bit as damaging to U.S. strategic interests

as if contracted with a Chinese munitions firm. In the Chinese communist government with authoritarian control and outright state ownership of many, if not most of the firms registered, have direct links, reporting, and direction of their communist party masters. So, I personally draw little distinction between Chinese firms characterized as private versus those classified as military or munitions.

Aside from the specific provisions mentioned in this section, there is little else directly governing contracting with international sources, including with China. So, restrictions in effect per the FAR and DFARs primarily deal with telecommunications, munitions, and the implementation of international technology transfer. If examining the plethora of goods and services falling under all of the outsourcing, Chinese acquired and/or controlled U.S. firms, entities that are green fielded, etc., the FAR and DFARs provisions are lacking in scope and depth.

Negative Effects in the U.S. Defense Industry through U.S. DoD Contracting with China

There are several notable issues related to having an economic and military adversary supplying many of the parts, components, assemblies and software in our military systems. As example of the problems, in the 2019 article in *Quartz* magazine titled "The U.S. Military Spent $33 Million on Tech Known to be Vulnerable to Chinese Cyberespionage" author Justine Rohrlich pointed out some of the more concerning examples of the day, embedded espionage capability in the systems supported by Chinese high-tech firms.

> The US Department of Defense (DoD) purchased and used millions of dollars worth of electronics last year containing "known cybersecurity vulnerabilities" that make them particularly susceptible to Chinese government espionage. The findings are included in a recent audit (pdf) by the Pentagon's Inspector General (IG) for DoD cyberspace operations, which warns that "missions critical to national security."
>
> Some models or brands of so-called COTS (commercial off-the-shelf) technology can allow adversaries access to communications infrastructure, command and control systems, and intelligence, surveillance, and reconnaissance networks, says the partially redacted IG report.
>
> To that end, at least $32.8 million in COTS purchases made by the U.S. Army and Air Force during the 2018 fiscal year were singled out for concern. The products include software, cameras, and networking equipment red-flagged by the Department of Homeland Security (DHS) and the Joint Chiefs of Staff Intelligence Directorate, as well as computers that have been banned for use by State Department employees since 2006. (Rohrlich, 2019)

Many companies supplying COTS items, generally considered to be benign, and not a threat that would be covered normally considered for an international technological transfer review, such as printers, copier machines, office automation, and other COTS items, may actually pose a huge threat to U.S. national security. Lenovo computers and laptops, GoPro cameras, and Lexmark printers, all have spyware and potential espionage capabilities embedded. According to the *Quartz* article,

> In 2006, the report notes, the State Department banned Lenovo products from its classified networks after reports that the company's computers were being manufactured with hidden spyware and backdoors. In 2015, the DHS issued a warning about cybersecurity vulnerabilities in Lenovo devices, and in

> 2016 the Joint Chiefs of Staff Intelligence Directorate warned that Lenovo hardware posed a cyberespionage risk to both classified and unclassified networks and had the potential to compromise the entire DoD supply chain. Still, the Army purchased 195 Lenovo products last year, for around $268,000, while the Air Force acquired 1,378 Lenovo products for $1.9 million. (Rohrlich, 2019)

Findings, Recommendations, and Conclusion

This paper highlights the major issues and challenges the DoD faces in protecting its military systems from Chinese influence and outright compromise which can damage U.S. national security. The Chinese, through its long-term strategy "China Made 2025" and the "Belt and Road" initiatives, plan to take control of major portions of U.S. intellectual, technological, and production capability. And this isn't just in theory, it's been happening, and is happening currently. The Chinese have a long-term vision, more so than most U.S. policy-makers and business planners are accustomed. The long-term Chinese vision, although already showing strong inroads, and dangerously proactive measures to acquire and supplant U.S. supply chains through U.S. contracting out, outsourcing, green fielding, and corporate and political influence and takeover is a Sun Tzu strategy—long term and persistent. And take note! This is not a flash fad that the Chinese will abandon easily or without a fight. For every step the United States takes, and will take in the future, it's very likely going to be met with a subtle, yet effective, counter-plan. Sun Tzu strategy calls for long-term vigilance—the Chinese are noted for their persistence. But, that doesn't mean the United States should not take proactive action to stop the many talons of Chinese communist infiltration of our supply chains, productive capabilities and capacities, and intellectual property assimilation and piracy. On the contrary, the United States should do everything at its disposal to end the onslaught. This is a call to action!

Findings and Recommendations

The following findings and recommendations are provided. Note that these provide a framework or guide as to what is needed.

Finding 1: The FAR and DFARS do not have enough provision through statutory or other mandate to effectively address the premise of this paper, that the DoD has been directly spending on prime contracts with Chinese national entities. And as noted in this work, the data does not include spend by the primary DoD contractor on their subcontracts, at any level, which is likely to be significant. As indicated, existing legislation has not been effective at stemming the tide of Chinese influence, including the Buy American Act (BAA) and others indicated herein.

Recommendation 1: Congress must enact legislation requiring DoD contractors to source domestically or with approved allied partners. This legislation must flow down into FAR and DFAR provisions. A strict prohibition on utilizing Chinese firms for any DoD awarded contract is recommended. Additionally, there must be sufficient oversight—monitoring and enforcement—mechanisms and practice. There must be sound enforceability. While seemingly harsh, the long-term negative effects of not prohibiting these sources is detrimental to U.S. national security.

Finding 2: The current commercial item protocols and commercial off the shelf (COTs) provisions allowing for loosened FAR protocols for FAR Part 12, FAR Part 13, and other FAR parts under commercial item protocols, has allowed a loophole for the Chinese to infiltrate the DoD through seemingly benign channels but with detrimental effects, as

indicted. Several COTs buys have resulted in damage to U.S. national security interests, and a weakening of the U.S. domestic supplier base.

Recommendation 2: Congress must enact legislation to source domestically, even for commercial and COTs items. The domestic source provision can include approved allies. As with recommendation 1 above, adequate monitoring, oversight, and penalty for violation must be part of the legislation. All legislative provisions must be accompanied by an implementation plan at all levels from Congress to the Executive Branch. Funding for enforcement must be provided.

Finding 3: The Buy American Act and the Berry Amendment. Although great in concept, the BAA and Berry Amendment to the BAA are, in essence, ineffectual. As indicated in this paper, there are too many exclusions and waivers in applicability. Plus, the self-reporting and policing policies, along with retroactive waivers, provide too many opportunities for escaping visibility and scrutiny on transactions that should be subject to the BAA and BA.

Recommendation 3: Through proactive legislative action, eliminate the many exclusions of the BAA and BA, and provide more rigid review and enforcement of waiver policies.

Finding 4: There are significant shortfalls and deficiencies in the legal and agency structures and protocols in several key areas noted herein. To wit:

- Tariffs and extent to which they can deal with Chinese influence,
- Section 301 deficiencies and waivers
- CFIUS reviews and the inability to effectively control Chinese incursions
- Green fielding— the Chinese method to outright acquire U.S. production
- FIRRMA
- Buy American Act and Berry Amendment
- FAR and DFAR provisions

All of the above were addressed in the body of this research. And all have noted, significant deficiencies precluding them from addressing the Chinese influence in an effective and efficient manner.

Recommendation 4: Congress and the Executive Branch must thoroughly review and revise these programs to address the deficiencies noted herein.

Final Thoughts and Conclusion

In summary, the Chinese are resolutely intent on subverting the United States' advantages in military, industrial, and intellectual domains. The "China Made 2025" and "Belt and Road" initiatives are the most prominent means that Chinese communist government has in place to achieve their end-state of global dominance. If the United States doesn't act now, and act decisively, we may lose our strategic advantages in these domains. As stated by John Milton:

> With scattered arms and ensigns, till anon
> His swift pursuers from Heaven-gates discern
> The advantage, and descending tread us down
> Thus drooping, or with linked thunderbolts
> Transfix us to the bottom of this gulf.
> **Awake, arise, or be forever fallen!** (Milton, 1663)

The time to act is now. Congress and the Executive Branch must be proactive and resolute in protecting our strategic interests.

References

Acquisition Notes (acqnotes.com). (2020, March 31). *Buy American Act.* Retrieved from http://acqnotes.com/acqnote/careerfields/buy-american-act

Bourne, T., Gallacher, D., & Meyer, J. E. (2019, August 13). FAR prohibition on Chinese telecommunications equipment. *Government Contracts Law*. Retrieved from https://www.governmentcontractslawblog.com/2019/08/articles/china/far-prohibition-chinese-telecommunications-equipment-2019-ndaa/

Congressional Research Service (CRS). (2019). *Trump administration tariff actions: Frequently asked questions* (CRS Report R45529). Washington, DC: Author. Retrieved from https://fas.org/sgp/crs/row/R45529.pdf

Congressional Research Service (CRS). (2020, January 28). *The U.S. export control system and the export control reform initiative* (CRS Report R41916). Washington, DC: Author. Retrieved from https://fas.org/sgp/crs/natsec/R41916.pdf

Defense News Online. (2019). Top 100 for 2019. Retrieved from https://people.defensenews.com/top-100/

Federal Procurement Data System–Next Generation (FPDS-NG). (2020). Retrieved from https://www.fpds.gov/common/html/public_welcome_text.html

Gallacher, D. S., & Chadwick, B. D. (2019, February 28). Buy American updates: Trump's executive orders, government reports, and other updates. *The National Law Review*. Retrieved from https://www.natlawreview.com/article/buy-american-updates-trump-s-executive-orders-government-reports-and-other-updates

GAO. (2019, September 5). *Defense supplier base challenges and policy considerations regarding offshoring and foreign investment risks* (GAO-19-516). Washington, DC: Author. Retrieved from https://www.gao.gov/products/GAO-19-516

GAO. (2018, December). *Buy American Act—Actions needed to improve exception and waiver reporting and selected agency guidance* (GAO-19-17). Washington, DC: Author. Retrieved from https://www.gao.gov/assets/700/696086.pdf

Greaser, C., & Osman, A. J. (2015, November 18). *Buy American Act and the Berry Amendment* [MBA student research presentation Naval Postgraduate School Course MN3315].

Hu, K. (2017, September 6). Offshoring goes full circle: Chinese firms shipping out. CKGSB Knowledge online. Retrieved from https://knowledge.ckgsb.edu.cn/2017/09/06/manufacturing/offshoring-full-circle-chinese-firms/

Jackson, J. K. (2020). *The Committee on Foreign Investment in the United States (CFIUS)* (CRS Report No. RL33388). Washington, DC: Congressional Research Services. Retrieved from https://fas.org/sgp/crs/natsec/RL33388.pdf

Joint Chiefs of Staff [JCS]. (2019). *National military strategy description 2018.* Retrieved from https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf

Li, J., & Hoff, P. (2018, January 4). CFIUS's concerns with Chinese investments and acquisitions in the U.S. *Foster and Garvey Cross Border Legal, Foreign Investors International.* Retrieved from https://www.foster.com/pp/blogpost-923.pdf?82596

Ma, A. (2019, November 11). China's belt and road initiative. *Business Insider.* Retrieved from https://www.businessinsider.com/what-is-belt-and-road-china-infrastructure-project-2018-1

McBride, J., & Chatzky, A. (2019). Is "Made in China 2025" a threat to global trade? Council on Foreign Relations. Retrieved from https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

Military.com. (2020). *Military equipment data—P8A Poseidon.* Retrieved from https://www.military.com/equipment/p-8a-poseidon

Milton, J. (1663). *Paradise Lost,* pp. 42–43. Retrieved from https://ia902901.us.archive.org/33/items/miltonsparadiselmilton/miltonsparadiselmilton.pdf

Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies. 48 CFR 252.225-7007 (2015). Retrieved from https://www.govinfo.gov/app/details/CFR-2015-title48-vol3/CFR-2015-title48-vol3-sec252-225-7007

Ricardel, M. R. (2020, January 20). These new rules might end tech's reliance on Chinese investors. *Fortune Magazine.* Retrieved from https://fortune.com/2020/01/20/cfius-rules-regulations-china-investment/

Rohrlich, J. (2019, July 31). The U.S. military spent $33 million on tech known to be vulnerable to Chinese cyberespionage. *Quartz Magazine.* Retrieved from https://qz.com/1679475/dod-spent-30m-on-china-hackable-tech-from-lenovo-gopro-others/

White House. (2017). *National security strategy*. Retreived from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

White House. (2018). *Executive briefing September 18, 2018.* Retrieved from https://www.whitehouse.gov/briefings-statements/statement-from-the-president-4/

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net