SYM-AM-22-043

Excerpt from the Proceedings
of the
Nineteenth Annual Acquisition Research Symposium

Acquisition Research:
Creating Synergy for Informed Change

May 11–12, 2022

Published: May 2, 2022

The research presented in this report was supported by the Acquisition Research Program 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).

Supply Chain Resilience in an Era of Long-Term, Peacetime Competition: The Semiconductor Case and a New Framework for Supply Chain Assessment

Emily de La Bruyere—is a co-founder of Horizon Advisory, a geopolitical consultancy. Her work focuses on China's digital ambitions, industrial policy, and platform geopolitics, as well as their implications for global security, economics, and human rights. Her analysis has been featured in The New York Times, The Wall Street Journal, and The Washington Post. She has testified before the Senate Banking Commission and the US-China Economic Security and Review Commission. She holds a BA summa cum laude from Princeton University and an MA summa cum laude from Sciences Po, Paris, where she was the Michel David-Weill fellow. [ebde@alumni.princeton.edu]

Nathan Picarsic—is a co-founder of Horizon Advisory, a geopolitical consultancy. His work focuses on the development of competitive strategies that help businesses, investors, and governmental actors navigate economic, technological, and political change. His research on topics ranging from geopolitical competition to human rights abuses has been profiled in The New York Times, the Wall Street Journal, and the Washington Post, among other leading international outlets. His expertise has been cited by outlets ranging from Barron's to Vice and he has testified before the US-China Economic Security and Review Commission on US-China relations and the strategic role of capital markets. He serves as a mentor and advisor to technology startups at Carnegie Mellon University's Project Olympus. He holds a Bachelor of Arts from Harvard College and has completed executive education programs through Harvard Business School and the Defense Acquisition University. [nate.picarsic@post.harvard.edu]

Abstract

The U.S. defense acquisition system is positioning for strategic competition with China. That effort must be informed by and responsive to the nuances of China's global supply chain positioning—a competitive dynamic unique relative to past eras of great power competition. Updating for this reality demands a thorough understanding of how Beijing leverages its military–civil fusion (MCF) strategy to weaponize its manufacturing prowess, relative industrial self-reliance, and the asymmetric supply chain dependencies that result. The immediate security risks of Beijing's approach—and the challenge it poses to the U.S. ability credibly to compete—have been evident since China cut off rare earths exports to Japan in the midst of a territorial dispute in 2010. Yet U.S. acquisition processes have not updated. The Pentagon, military services, and defense acquisition program officials must rethink frameworks for assessing supply chain integrities, the risks that dependencies all along acquisition program value chains can create, and responsive acquisition processes. Until it does so, the U.S. approach to defense acquisition will feed into Beijing's continued, subversive global positioning.

The U.S. defense industrial base is grappling with two parallel and mutually reinforcing trends: a growing role in military supply lines for dual-use commercial technologies, and a growing reliance on complex, global supply chains. Both create *efficiencies* in terms of cost, access to, and pace of adopting innovation. But both also create major vulnerabilities that threaten the *effectiveness* of the U.S. security apparatus; the resilience of individual weapons programs in the face of supply shocks; and, in turn, the credibility of U.S. deterrence and power projection capacity *vis-à-vis* strategic competitors.

Specifically, the past generation of increasingly globalized supply lines shaping defense-relevant technology exposes the U.S. defense industrial base dependence on, and access from, an insecure, international ecosystem—and, with it, the risk of adversarial influence. Pandemic-induced supply chain challenges have brought these risks to the fore over the past several years. But even that recent and available manifestation of the challenge glosses over the reality: Chinese dominance of upstream materials, component assembly and testing, and manufacturing and production grant the Chinese Communist Party—the American military's pacing threat—leverage over critical defense-relevant supply chains.

These risks are particularly acute considering China's deliberate approach to competing in peacetime competition with the United States: Beijing's strategy of military–civil fusion (军民融合) (MCF). With MCF, Beijing leverages commercial positioning for military ends, and vice versa. This approach includes turning supply chains into battlefields for geopolitical competition. Beijing seeks to weaponize its manufacturing dominance, relative industrial self-reliance, purchasing power of its domestic market, and resultant asymmetric supply chain dependencies in order to secure coercive leverage over the international system. This has been evident for over a decade: In 2010, China cut off rare earth exports—critical for both commercial and security applications—to Japan in the midst of a territorial dispute.

U.S. acquisition processes must update for this reality and the security threats it poses. As acquisition reform and rewiring of a Cold War–era shaped bureaucracy take place, the Pentagon, military services, and defense acquisition program officials must rethink frameworks for assessing supply chain integrity, the risks that dependencies all along acquisition program value chains can create, and responsive acquisition processes. More broadly, the U.S. government and capital markets need to rethink investment in the domestic industrial base to ensure that these new frameworks can be operationalized and capitalized; that the necessary industrial capacity exists so that developments in U.S. military–relevant capabilities can create a more lethal fighting force, not a more vulnerable one.

Using the semiconductor industry as a case study, this paper seeks to develop and present such an updated framework for supply chain assessments—tailored to today's era of peacetime, strategic competition with China. The framework differentiates itself along three core dimensions:

- First, it looks not only at provision of goods and technology, but also at provision of capital. For example, a Chinese pool of capital's investments in a semiconductor manufacturer should be considered a risk factor—alongside, say, reliance of that manufacturer on electronic-grade polysilicon sourced from China or dependence on China-based or -owned packaging steps in the semiconductor value chain.
- Second, the framework looks holistically all along the supply chain, from the upstream to the downstream: Beijing's approach to weaponizing supply chains treats them as integrated wholes, and in many cases prioritizes upstream footholds over the more surface-level, downstream ones. Accordingly, U.S. acquisition processes should include screening against these n-th tier supply chain risks within the definition of program requirements and assessment of alternatives.
- Third, in its analysis, this paper seeks also to present best practices for using open-source information to implement supply chain assessments, focusing on information that is available for, and often goes overlooked in, the Chinese industrial ecosystem. Examples of such open-source information include strategic partnership agreements, government subsidies, and the network of MCF industry projects that animate China's positioning in military-relevant semiconductor supply chains.

The first section of this paper reviews the semiconductor supply chain as an example of under-appreciated risks in military-relevant value chains, compounded by China's effort to secure influence in key international industries as well as a growing U.S. interest in commercial solutions to military problems. The second section explains the inadequacies in existing methods for vetting and programs for protecting against these risks. And the conclusion presents an outline for a new, updated framework to inform the defense acquisition apparatus's approach to supply chain integrity. This framework's application could vary in tactics at different stages of the acquisition cycle. But the microelectronics realm demonstrates the imperative that protection against adversarial supply chain influence be incorporated into strategic planning for the use of acquisition as a means of influence in long-term, peacetime competition with China.

The Semiconductor Supply Chain

Semiconductors—which are cited here as shorthand for the realm of microelectronics covering memory chips and microprocessors—are necessary inputs into the entire basket of modern electronic products, ranging from computers to smartphones to medical equipment. They are broadly recognized as critical for the defense industry: Semiconductors are a prerequisite for everything from unmanned aerial vehicles to fighter planes to electronic warfare components (Defense Microelectronics Activity. n.d.). And in some cases, sophisticated military systems rely on the same semiconductors that fuel civilian, consumer goods (Inboden & Klein, 2022).

Accordingly, semiconductors used for defense purposes also rely on the same—global, interconnected—value chain as do those used for civilian purposes. The semiconductor production process is comprised of three main steps: design, fabrication, and assembly. Every step requires its own set of technological equipment, and chemical and material inputs. No single country has every element of the semiconductor production stack within its borders. Rather, production of these critical goods depends on a multi-step value chain integrating the United States, Taiwan, South Korea, Japan, Europe, and China. This global value chain promises an efficient division of labor. But in creating efficiencies, it sacrifices effectiveness. And, this paper argues, beyond simply raising concerns about the supply chain's resilience, today's global semiconductor value chain layout also hardwires a dangerous reliance on China that permeates many downstream acquisition supply lines.

At a surface level, the United States is a leader in the international semiconductor industry, boasting major, downstream, high-tech brand names like Intel, Micron, and Qualcomm. Intel is the world's largest semiconductor company by revenue. U.S. companies maintain a near-monopoly over global Electronic Design Automation (EDA) software tools, on which leading-edge chip design depends (Kleinhans & Baisakova, 2020). The United States houses some of the world's major equipment vendors, including Applied Materials, KLA, and Lam Research (Kleinhans & Baisakova, 2020). In 2019, the United States claimed a more than 50% global market share of integrated circuits, based on total sales. The U.S. leadership in core elements of semiconductor technology is sufficient that export restrictions on sales to China in recent years have imposed real costs on Chinese industry (He, 2021).

But this surface level and downstream leadership belies a set of major dependencies. First, U.S. semiconductor national champions depend on Chinese production, testing, and packaging as well as the Chinese market of downstream electronics product assembly. This grants Beijing the ability to disrupt their operations—as well as to influence their boardrooms. Second, the upstream of the international semiconductor value chain disproportionately relies on Chinese inputs. This means that the industry is built on a foundation controlled by Beijing.

Dependent Champions

China dominates international production of electronic components and the subsystems and commercial products built on top of them. As a result, most U.S., and international, semiconductor vendors have some degree of dependence on manufacturing facilities in China. They also sell their products back into the Chinese market. The result is a pincer of dependence whereby a centralized Chinese economic system enjoys leverage over the global market by virtue of both supply and demand.

Intel offers a ripe example. Intel directly supplies the Department of Defense (Cherney, 2021). It also cooperates with key defense contractors, like Lockheed Martin, on military technologies (Lockheed Martin, 2022). Intel's website lists 17 campuses in China, the company has at least two production sites in China, and it operates a series of innovation and R&D centers across the country (Intel, n.d.; Intel China, n.d.). Intel also relies on a host of Chinese suppliers. And on the sales side, in 2020, China accounted for 20.26 billion USD of Intel's 77.9 billion in revenue, or 26% (Pan, 2022). These ties in terms both of production and sales grant Beijing influence over Intel's operations, and therefore over the U.S. industry, including defense industry, built on top of them. Disruption in China, intentional or not, can stop Intel production: In September 2021, forced power shutdowns imposed by the CCP compelled key Intel suppliers in China to shut down their facilities (Shilov, 2021). And Intel's revenue stream requires that it remain in favor with the CCP. In January 2022, Intel removed reference to Xinjiang from its annual letter after facing backlash from China (Pan, 2022). Nor is this a vulnerability unique to Intel. Micron, the major U.S. DRAM company, had to halt production at its Xi'an, China, manufacturing facility in December 2021 as COVID-19 shut down the city (King, 2021).

Other international semiconductor companies from allied and partner countries with whom the United States cooperates risk even greater exposure to Chinese industrial influence. Take, for example, TSMC, the world's most valuable semiconductor company by market capitalization, recently lauded for beginning construction of a new facility in Arizona (Reuters, 2021). China serves as a critical manufacturing hub and revenue generator for TSMC; the company has supply relationships with customers that participate in China's MCF strategy; and TSMC invests into and alongside semiconductor-relevant Chinese government-guidance funds.

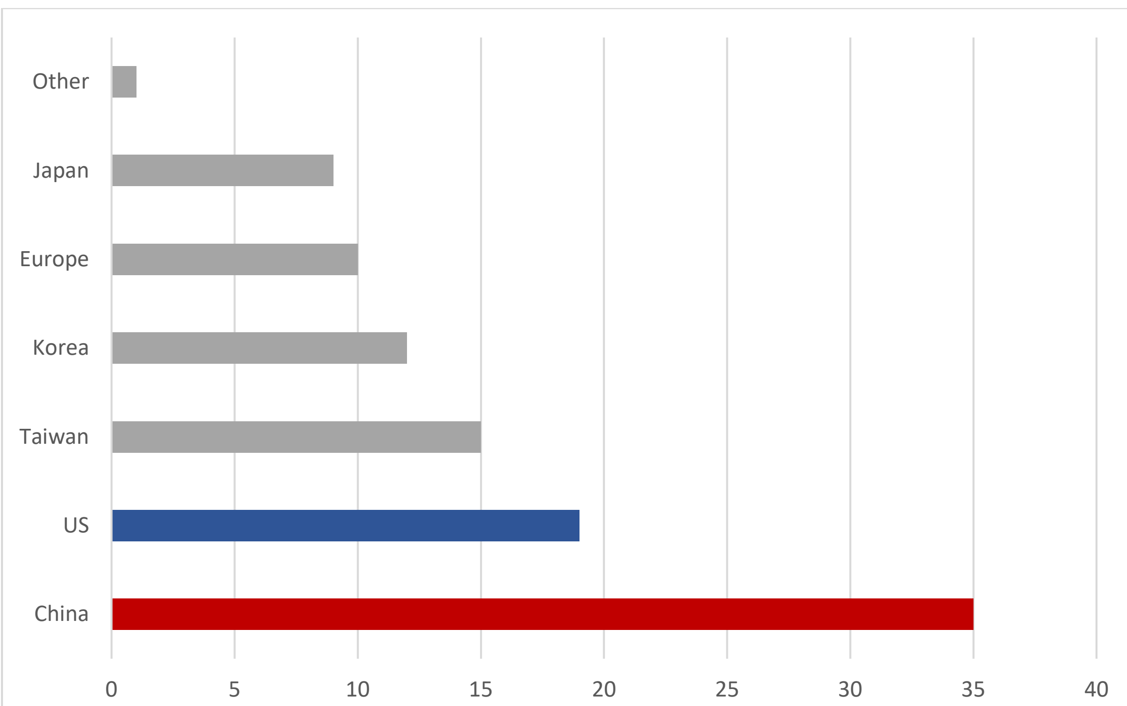

Figure 1. Global Semiconductor Sales by Location of Electronic Device Assembled (Semiconductor Industry Association, 2021)

A Chinese Communist Party Foundation

In addition, while the United States may boast high-profile leaders at the downstream of the semiconductor value chain, China increasingly dominates the upstream. These steps—including packaging and testing as well as production of electronic-grade silicon—are not the flashy or high-margin segments of the semiconductor value chain. They are considered “dumb”; labor and energy but not as capital or technology intensive. Yet their relative sophistication has little bearing on the influence that can be derived from dominating them. This is the foundation on which the international semiconductor industry is built. And this is where China has succeeded in making well-defended inroads.

After silicon wafers are manufactured in a fab, they proceed to the “back-end” packaging and testing step. This process is highly labor intensive. It does not require cutting-edge technology. And China has been investing significantly in this step of the value chain. Between 2009 and 2019, China’s share of the global assembly and testing market grew from less than 5% to higher than 19%. In 2020, that figure stood at 38% (Kleinhans & Baisakova, 2020). Beijing’s influence in semiconductor assembly and testing extends beyond explicitly Chinese companies as well. China has also invested in other, major, international assembly and testing (OSAT) players, securing concealed beachheads. For example, the largest shareholder of Powertech Technology Inc., a Taiwanese OSAT operation that in 2019 ranked fifth in the world by revenue, is the State-owned China Life Insurance Co., Ltd.

Even farther upstream, the material most frequently used in semiconductors is silicon. In 2021, China accounted for some 70% of global silicon production. This is a function of deliberate government industrial policy, not natural endowment. Silicon is the second most abundant element in the Earth’s crust, surpassed only by oxygen. But extracting and processing it is energy-intensive. Recognizing silicon’s strategic value in industries ranging from semiconductors to solar power technology, the CCP has, over the past two decades, provided significant State support (e.g., subsidies) to domestic silicon producers, allowing them to undercut their international competitors and dominate the market. Silicon might be among the least sophisticated inputs into the semiconductor value chain. But it is also the input on which all others depend: Advanced EDA software tools have little value without a product to design.

Military–Civil Fusion and an Underappreciated Defense Acquisition Risk Environment

Chinese leverage over the international semiconductor value chain creates very real risks for the defense industrial base. China sees today’s international competition as one for control of supply chains. And over the past decades, Beijing has deliberately invested to capture key nodes in strategic international supply chains, including that for semiconductors, in order to secure coercive leverage in strategic competitions. At the same time, Beijing has sought to build relatively autonomous domestic industrial capabilities in order to ensure that its coercive leverage be asymmetric; that it be able to threaten adversary’s industrial bases without facing equivalent consequences. Beijing’s industrial policy explicitly states this ambition: “The competition in the global industrial and supply chain is becoming increasingly fierce,” declared the director of the National Development and Reform Commission’s Price and Cost Investigation Center in 2021. “We must improve the resilience of China’s industrial and supply chain through coordination of ‘supplementing the chain’ and ‘strengthening the chain’; filling in gaps but also consolidating ‘industries with competitive advantages’” (Economic Daily, 2021) Beijing’s actions also bear it out. In 2010, China cut off rare earth exports to Japan in the midst of a territorial dispute—proving that it was prepared to weaponize supply chains in geopolitical contests (Bradsher, 2010).

U.S. acquisition processes have not updated for this reality. Existing protocols for assessing supply chain integrity fail appropriately to address upstream vulnerabilities or dependencies that influence firm decision-making through means other than majority ownership—precisely the areas where China's manufacturing prowess and enormous market risk granting it the greatest influence. Even the most thorough application of existing tools for foreign ownership, control, or influence (FOCI) review of industrial base players would miss, entirely, the scope of dependencies that contemporary Chinese economic statecraft pursues and leverages. And mitigation against risks of that nature is not formally incorporated into the development of requirements at a program level. As the U.S. defense acquisition apparatus is increasingly turning to off-the-shelf commercial products and dual-use technologies and seeking more rapid acquisition approaches, these risks are certain to increase both in their number and in their impact to the complex industrial base ecosystem. Efficiencies in terms of cost and access to technology may come at the cost of relatively unscreened value chains, amplifying the defense industrial base's exposure to China's MCF strategy, and therefore injecting vulnerabilities into the fighting force.

Take the Department of Defense's Trusted Foundry Program: Formulated in the early 2000s, the program screens companies across the electronics supply chain (e.g., IC design houses, specialty foundries, packaging houses) to build a roster of trusted suppliers. But this screening doesn't go far enough: There is no evidence to suggest that the program accounts for trusted suppliers' silicon sourcing, for example. Moreover, the greater threat is that this "trusted" program is limited in its scope. Even its best intentions do not protect against supply chain risks in off-the-shelf technologies that are not produced specifically for the defense community under the purview of the Trusted Foundry Program.

The microelectronics example presents a daunting task. But it is one of universal importance across the defense acquisition system. It is also a familiar one to a range of national security stakeholders from policy-makers and legislators to warfighters. Instituting a systemic concern for supply-chain risks, like those reflected in the global semiconductor ecosystem, into acquisition considerations would go a long way toward orienting the broader defense acquisition environment for the effectiveness mission of strategic competition with China. And that, in turn, would go a long way toward making the acquisition system a viable means for signaling, deterrence, and strategic shaping of the adversary.

Two points of intervention may exist based on existing acquisition processes: The System Threat Assessment phases of the JCIDS process and within security monitoring requirements of program management. At present, the intelligence inputs that guide the System Threat Assessment could be extended beyond threatening offensive and defense foreign adversary operational capabilities to include the strategic-to-tactical manifestations of related supply chain risks. Capstone Threat Assessments and related foreign country- and system-specific inputs developed by the Defense Intelligence Agency for acquisition customers could also address the relative adversarial influence over material inputs and supply lines that a given program's requirements and operational objectives demand. And as reference to FOCI reviews above suggests, acquisition oversight and program management bring additional opportunity to monitor and mitigate adversarial supply chain leverage throughout a program's life cycle.

But FOCI reviews and related industrial base security monitoring and training conducted by the Defense Counterintelligence and Security Agency should be broadened in scope to address a wider means of influence and legacy vectors of industrial espionage: How can supply chain vulnerabilities and supply chains shape decision-making at a firm level? How can companies be incentivized and educated to incorporate those risks—and the latent costs they may carry—into their profit formulae?

Certainly, there are positives to be taken and expanded from past supply chain security initiatives like the Trusted Foundry example and the progress over time in understanding and protecting against insider threats within the industrial base. But today's strategic competition—and today's pacing technological threat—demand a renewed emphasis on supply chains and their impact through the acquisition process. More is needed across the board. Supply chain security is a game of effectiveness and not efficiency.

Conclusion: A Risk-Informed Defense Acquisition Process

A new framework for risk-informed defense acquisition processes should adopt a new methodology for identifying and assessing threats in the acquisition system that owe to supply chain and upstream vulnerabilities. As dual-use, commercial technologies expand throughout the U.S. defense industrial base, existing acquisition processes and inputs need to be updated and to take into account the new risks that may accompany new supply lines. Considerable effort has been dedicated to recognizing and acting on the "promote" line of effort in a defense technology competition with a strategic competitor like China. Those "promote" efforts and investments need to be paired with proactive investment in "protect" lines of effort to guarantee that the acquisition system's ability to deliver a technological edge is not built on someone else's foundation (Doshi et al., 2021).

Defense

China's MCF strategy, and the complex nature of today's global supply chains, are such that risk assessments must account for:

- Entire value chains, not just first and second tier suppliers: An updated risk assessment model requires prioritizing supply chain integrity at the upstream, "dumb" stages of production as well as at the downstream, more sophisticated points.
- Companies' sales as well as their suppliers: Adversarial influence can be secured through control over revenue as well as control over its suppliers. If the dry cleaner has all your clothes, the dry cleaner owns you.
- Sources of capital—in addition to location, sources of supply, and outright ownership: China can, and does, secure access to and influence over companies by investing in them, including through State actors masquerading as private players.

Offense

These defensive screening measures need to be paired with proactive ones to ensure that they *can* be operationalized; that the United States has alternatives to dependence on China; and that those alternatives provide resultant capabilities with credible signaling, deterrence, and adversarial shaping value. The U.S. government needs to invest in, and encourage the private sector to invest in, trusted domestic production—all along the value chain. The CHIPS Act suggests a positive intention on this front. However, it is insufficient. It fails to address upstream dependencies. It also fails to address ties at the company level (e.g., sale dependence, capital exposure) to China. And it risks failing sufficiently to marshal private sector investment, and therefore the resources necessary to resolve vulnerabilities in the U.S. defense industrial base. At a strategic level, effective proactive moves will demand:

- Investment all across the value chain, not simply at demand-side, consumer-facing stages: There is little value in building a semiconductor foundry in the United States if that foundry will remain reliant on inputs from China.
- Cooperation with the private sector to ensure that Washington's investments are a guide for Wall Street's: In today's technological and commercial environment, the government alone

cannot resolve industrial weaknesses. The private sector is a necessary partner. Washington should focus on incentivizing the private sector to invest in the long-term, strategic interest of the United States.

- Regulations on the private sector to ensure actions in the national interest: China's market and distortive industrial policies incentivize companies to defect; to share technologies, move production, and accept CCP influence. The U.S. government needs to impose an updated set of regulations on the private sector to disincentive actions that undermine the long-term, strategic interest of the United States.

More tactically as it concerns the defense acquisition system, it would be both prudent and tractable to update the threat intelligence inputs incorporated into program planning and management to account for the reality of today's complex supply chain threat environment.

References

Bradsher, K. (2010, September 22). Amid tension, China blocks vital exports to Japan. *The New York Times*. https://www.nytimes.com/2010/09/23/business/global/23rare.html

Cherney, M. (2021, August 23). Intel wins Defense department contract for advanced chips. *Barron's*. https://www.barrons.com/articles/intel-stock-chips-defense-51629757043

Defense Microelectronics Activity. (n.d.). *DMEA Trusted IC Program*. https://www.dmea.osd.mil/TrustedIC.aspx

Doshi, R., de La Bruyere, E., Picarsic, N., & Ferguson, J. (2021, April). *China as a cyber great power: Beijing's two voices in telecommunications*. The Brookings Institution. https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf

Economic Daily. (2021, October 18). 提升产业链供应链韧性要强化科技创新 [To improve the resilience of the industrial chain and supply chain, it is necessary to strengthen scientific and technological innovation].

He, T. (2021, July 27). When the chips are down: Biden's semiconductor war. *The Interpreter*. https://www.lowyinstitute.org/the-interpreter/when-chips-are-down-biden-s-semiconductor-war

Inboden, W., & Klein, A. (2022, March 20). Judge the CHIPs Act as defense policy, not industrial policy. *The Hill*. https://thehill.com/opinion/national-security/598783-judge-the-chips-act-as-defense-policy-not-industrial-policy/

Intel. (n.d.). *Worldwide campus locations*. https://www.intel.sg/content/www/xa/en/support/contact-intel.html?tab=campus-locations#support-world-locations

Intel China. (n.d.). 认识英特尔—根植中国 服务中国 [Know Intel: Rooted in China to serve China].

King, I. (2021, December 29). *Micron says output at Chinese facility hit by city's shutdown*. Bloomberg. https://www.bloomberg.com/news/articles/2021-12-29/micron-says-china-facility-output-hit-by-xi-an-city-shutdown

Kleinhans, J.-P., & Baisakova, N. (2020, October). *The global semiconductor value chain*. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/the_global_semiconductor_value_chain.pdf

Lockheed Martin. (2022, April 4). *Lockheed Martin, Intel sign agreement to advance 5G-ready communications for U.S., allied defense systems*. https://news.lockheedmartin.com/2022-04-04-Lockheed-Martin,-Intel-Sign-Agreement-to-Advance-5G-Ready-Communications-for-U-S-,-Allied-Defense-Systems

Pan, C. (2022, January 11). Intel removes reference to Xinjiang in annual letter to suppliers after Chinese backlash. *South China Morning Post*.

Reuters. (2021, June 1). *TSMC says has begun construction at its Arizona chip factory site*. https://www.reuters.com/technology/tsmc-says-construction-has-started-arizona-chip-factory-2021-06-01/

Semiconductor Industry Association. (2021, July 13). *Taking stock of China's semiconductor industry*. https://www.semiconductors.org/taking-stock-of-chinas-semiconductor-industry/

Shilov, A. (2021, September 27). *Apple, Intel, and Nvidia suppliers halt production in China due to mandated power shutdown*. Tom's Hardware. https://www.tomshardware.com/news/power-outages-in-china-could-affect-apple-intel-nvidia

Sohu News. (2019, September 24). 英特尔中国区总裁杨旭：我们要和中国一道共赢未来 [Yang Xu, president of Intel China: We want to win the future together with China]. https://web.archive.org/web/20220124200936/https://www.sohu.com/a/343026382_123753

Acquisition Research Program
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net