The Economic Dimension of Great-Power Competition and the Role of Cyber as a Key Strategic Weapon

Samantha F. Ravich, PhD, and Annie Fixler

Napoleon Bonaparte may have said that an army marches on its stomach, but it is perhaps even truer that a military force marches, sails, flies, and attacks on the back of its nation's economy. Cripple an enemy's economy and not only will the stomachs of its fighting forces go empty, but commerce, trade, and innovation will grind to a halt, sapping the will of the people and depriving the leadership of most of the parts needed for the machinery of war.

Ancient civilizations recognized that economic warfare could destroy an adversary during conflict and weaken him during more peaceful times to keep him from becoming a rival. The catalyst for the Peloponnesian War nearly 2,500 years ago was an act of economic warfare. The Athenians imposed crippling economic sanctions against an ally of Sparta in order to sow dissension and weaken the coalition's ability to threaten Athens and its allies. Recognizing the danger, Sparta responded with military action. The war culminated in a final act of economic warfare when Sparta (with Persia's assistance) blockaded Athens and forced its surrender.[1]

Closer to our own time, Napoleon made wide use of economic aggression in hopes of shaping the battlefield to his advantage. In 1806, in an attempt to weaken England's fighting forces by ruining the economy that undergirded its power, he issued the Berlin Decree declaring the British Isles to be in a state of blockade. While not as successful in that case—in fact, some scholars blame it for the ultimate ruin of France—the military strategy of using economic means to cripple the adversary has never fallen out of favor.[2]

Economic Warfare, Invention, and Innovation

Economic warfare and, conversely, economic invention and innovation have been integral to American strategy since the Founding. George Washington believed so strongly in the importance of encouraging the advancement and protection of inventions for the benefit of the national defense that he called for passage of the Patent Act in his first State of the Union address on January 8, 1790. "To be prepared for war is one of the most effectual means of preserving peace," Washington declared, and to be prepared, manufacturing, "particularly for military supplies," had to be encouraged and protected.[3] Washington personally signed and sealed each of the 150 patents issued during his presidency.[4]

Having witnessed British attempts to use blockades to weaken the rebellious American colonies,[5] Alexander Hamilton encouraged another kind of economic warfare to advantage fledgling American industries and curb the military prowess of England. In his *Report on*

the Subject of Manufactures sent to Congress in 1791, Hamilton encouraged the new nation to engage in extensive private theft and application of foreign intellectual property in order to transfer wealth-generating capabilities to the new nation.[6] England recognized the threat posed by this pervasive intellectual property theft not only to the British economy, but also to its national security and thus implemented initiatives, including barring the export of key technologies, to prevent it from succeeding.[7]

The Great Wars

In the first half of the 20th century, America watched Great Britain incorporate economic warfare into its World War I and World War II strategies. In the lead-up to the Great War, the Naval Intelligence Department of the British Admiralty developed a plan to cripple Germany's ability to wage war by leveraging British advantages in "the largely British-controlled infrastructure of international trade." Specifically:

> Economic warfare strategy entailed doing "all in our power" to disrupt the already strained enemy economy, recognizing that significant additional pressure could be exerted upon the German economy by systematically denying access to the largely British-controlled infrastructure of international trade—British banks, insurance companies, and communications networks. In essence, the Admiralty argued that the beginning of a major war would find the German economy teetering on the edge of a precipice and that British strategy should seek to push it over the edge and down into "unemployment, distress, &c., and eventually in bankruptcy."[8]

The idea was that Britain could prepare for such a collapse and even leverage it, while Germany would be immobilized. Although the plan was never fully implemented, partly because England feared loosing the economic dogs of war more than it feared traditional military conflict, at the start of the Second World War, London created a new Ministry of Economic Warfare (the successor to the Ministry of Blockade during World War I) and specified that "[t]he aim of economic warfare is so to disorganise the enemy's economy as to prevent him from carrying on the war."[9]

During this time, but before the United States formally entered World War II, Washington also turned to economic warfare. President Franklin Roosevelt ordered a U.S. embargo of all sales of oil and scrap metal to Japan, hoping to constrain Japanese foreign aggression. The result may not have been what Washington desired: Emperor Hirohito's diaries from those years reveal that Japan went to war with the United States because of the embargo.[10]

Despite that outcome, economic coercion has become a key component of U.S. national security strategy, and Washington has relied increasingly on economic sanctions to deny adversaries access to global markets, thereby significantly degrading their capabilities. The United States controls the essential infrastructure that underpins global trade, and over the past two decades, we have used it to further our foreign policy and national security aims.

Fine-Tuning U.S. Strategy for Economic Warfare

The sophistication of U.S. sanctions began 15 years ago with efforts to punish Pyongyang's illicit activities and deny the regime funds to support its nuclear weapons program. When the United States slapped money-laundering sanctions on a little-known bank in Macau, Banco Delta Asia, in 2005, Washington "unleashed financial furies" unlike any the world had seen before.[11] Juan Zarate, Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes, said that after those sanctions, "[e]very conversation [with the North Koreans] began and ended with the same question: 'When will we get our money back?'"[12] During the Six Party Talks, an inebriated North Korean delegate admitted that with those sanctions, "[y]ou Americans have finally

found a way to hurt us."[13] With the world's largest economy standing behind it, the almighty dollar was a powerful foe, and given the relative lack of economic engagement between the U.S. and North Korea, American businesses never felt any pain from the sanctions imposed by Washington or the U.N.

Washington then took this preliminary playbook and developed its economic toolkit by testing its powers against Iran. Six months after Congress passed comprehensive sanctions against Iran's energy sector, then-Undersecretary for Political Affairs William Burns testified in December 2010 that the legislation had already cost Iran between $50 billion and $60 billion.[14] As a result of U.S. sanctions and economic mismanagement, Iran's gross domestic product (GDP) contracted by 6 percent in 2012/2013 and another 2 percent in 2014/2015.[15]

The imposition of sanctions following U.S. withdrawal from the international nuclear agreement with Tehran has similarly triggered worsening economic conditions.[16] In April 2018, one month before the U.S. decision to withdraw, average annual inflation was 8 percent. Less than a year later, inflation had more than tripled to about 30 percent.[17] Both the International Monetary Fund and the World Bank have begun to forecast deepening recession.[18] As recently as June 2018, the World Bank was projecting a 4.1 percent GDP growth for 2018 and 2019, but in January 2019, it had revised those numbers down to 1.5 percent and 3.6 percent GDP reduction.[19]

The U.S. government estimates that between May 2018 and April 2019, sanctions had taken 1.5 million barrels of Iranian oil off the market and "denied the regime direct access to more than $10 billion in oil revenue."[20] As a result, Tehran's regional proxies are starved for cash. Hezbollah has appealed for donations for the first time and has implemented austerity measures.[21] Militants in Syria have missed paychecks, and projects are going unfunded.[22] Without access to capital, it is difficult for Tehran to project power in the region and threaten U.S. interests and allies.

Washington's Economic Warfare Blind Spot

Disturbingly, despite the continued use of economic coercion by Washington since September 11, 2001, U.S. policymakers have an economic warfare blind spot: We have forgotten that we can be the victim and not just the perpetrator of economic warfare. Perhaps we have grown complacent because since the early years of the Republic, we have not faced a great-power rival with the ability to damage our economic wherewithal not just during, but also before and below the level of armed conflict.

Not even during the height of the Cold War, when the Soviet nuclear arsenal contained at least 55,000 warheads, did the best of America's military strategists consider how Moscow could undermine American economic wherewithal to weaken the United States strategically. This snapshot in time, roughly 1947–1991, frames much of the assessment and planning for great-power conflict by today's strategic thinkers, but there is a major deficiency in seeing that past as prologue.

The Soviet economy did indeed possess the strength to create one of the world's strongest militaries during its heyday, but in the end, it was self-defeating. As the late Dr. Charles Wolf, Jr., wrote, the Soviet system was based on five fundamental principles:

> (1) Pervasive and centralized political and social control; (2) rule by a self-perpetuating political/military elite; (3) domination of military/security priorities over civil ones; (4) persistent cultivation of external/internal threats, and requirement for international "struggle"; and (5) preference for self-reliance.[23]

These principles, when operationalized, left the Soviet Union in an ever-weaker position vis-à-vis the United States. Although there was little doubt that Moscow's nuclear capability could indeed obliterate both Wall Street and Main Street, in the absence of that cataclysmic event, the United States grew more prosperous,

more innovative, and more capable of shaping the world to its advantage.

During the postwar period between the 1950s and mid-1970s, some Western economists assessed Soviet economic growth rates as averaging about 5 percent per year, suggesting that the USSR was outpacing the average growth of the United States.[24] More detailed studies of the Soviet economy, however, recognized the mendacious data upon which those growth numbers were based and estimated a truer measure of the two countries that ranged from the Soviet economy's being equal to only 14 percent of the U.S. economy on the low side to 30 percent at the high end.[25] In 1988, Soviet foreign purchases and sales were roughly $200 billion, less than one-third those of the United States, and much of that trade was with other Soviet states that had no choice but to buy the inferior products foisted upon them in the closed Soviet system.[26]

Chinese Cyber-Enabled Economic Warfare Threatens U.S. Supremacy

The largest U.S. companies of 1980, from Exxon Mobil to General Motors to IBM to General Electric (first, second, eighth, and ninth, respectively, on the *Fortune* 500 list of that year[27]), did not fear that Moscow might execute a coordinated campaign to steal intellectual property, contaminate the supply chain, degrade operational systems, or offer below-market prices on key technological solutions to drive them out of business and weaken the digital fabric of the American national security industrial base. The reality today is far different, and so are the contours of the battlefield upon which the U.S. is now forced to engage.

"[U]nlike the 'bad old days' of the U.S.–Soviet Cold War, when our economic engagement with the USSR was relatively insignificant," Assistant Secretary of State for International Security and Nonproliferation Christopher Ford has commented, "the United States and its friends and allies have deep and extensive economic ties to China in this era of high-technology international commerce."[28] In the words of General Paul Nakasone, head of the National Security Agency and U.S. Cyber Command:

> We are in a period where our adversaries are looking to really take us on below that level of armed conflict, to be able to steal our intellectual property, to be able to leverage our personally identifiable information, to be able to sow distrust within society, to be able to attempt to disrupt our elections.[29]

China's economy is the second largest in the world behind the United States and the "largest if measured in purchasing price parity terms."[30] China has been the largest single contributor to world growth since 2008.[31] While the real size and growth rate are likely far below the Chinese Communist Party's official claims,[32] the reach of China's global investments gives Beijing leverage that it can use to challenge U.S. supremacy.

China conducts cyber-enabled economic warfare against the United States and its allies.[33] After South Korean conglomerate Lotte Group provided its government the land on which to deploy the Terminal High Altitude Area Defense (THAAD) missile defense system, Chinese hackers unleashed cyberattacks, and the government issued trumped-up regulatory action against the company as a way to pressure Seoul to change its policies.[34] Beijing's tactics seem to have succeeded: South Korea acquiesced to military constraints in return for relief from Chinese economic warfare.[35]

Today, China is engaged in a massive, prolonged campaign of intellectual property theft, using cyber-enabled technologies to target nearly every sector of the U.S. economy.[36] China's strategy is one of "rob, replicate and replace. Rob the American company of its intellectual property, replicate the technology, and replace the American company in the Chinese market and, one day, in the global market," according to the U.S. Department of Justice. "From 2011–2018, more than 90 percent of the Department's cases alleging economic espionage by or to benefit a state involve China,

and more than two-thirds of the Department's theft of trade secrets cases have had a nexus to China."[37] Even when technology is commercially available, China engages in a "concerted effort to steal, rather than simply purchase" these products.[38]

For a sense of scale, intellectual property theft costs the U.S. economy as much as $600 billion per year.[39] If China respected intellectual property rights, the U.S. economy would gain 2.1 million jobs and $107 billion in sales.[40] In just one case in which wind turbine company Sinoval stole trade secrets from U.S.-based AMSC, the company "lost more than $1 billion in shareholder equity and almost 700 jobs, over half its global workforce."[41]

Beijing's military–civil fusion[42] means that none of this intellectual property theft is driven purely by commercial motivation. President Xi Jingping has called "military–civilian integration" a "prerequisite for building integrated national strategies and strategic capabilities and for realizing the Party's goal of building a strong military in the new era."[43] Particularly with emerging technologies, the line between civilian and military purposes is disappearing.[44] Beijing's effort to build national champions in sensitive technologies "directly complements the PLA's modernization efforts and carries serious military implications," according to the U.S. Department of Defense (DOD).[45]

Meanwhile, more than 60 percent of Chinese export violations are attempts to acquire critical technologies that have military applications,[46] and the targets of Chinese hackers align with the priorities of Beijing's Made in China 2025 strategy.[47] China's J-20 fighter plane, for example, bears striking similarities to the F-22 Raptor made by Lockheed Martin—the same company from which the Department of Justice accused a Chinese national of stealing technical data.[48] At the time, a nine-man team run by Chinese intelligence officers was hacking a French aerospace manufacturer and U.S. companies that made parts for turbofan jet engines, and "a Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft manufactured in China and elsewhere," according to the Department of Justice.[49] Meanwhile, press reports revealed that one group of Chinese hackers has targeted dozens of universities and private companies over the past two years to steal military-related maritime technology.[50]

Each cyberattack, each espionage operation, each export control violation is "part of an overall economic policy of developing China at American expense" and "stealing our firepower and the fruits of our brainpower," in the words of Assistant Attorney General for National Security John Demers.[51]

Beijing's strategy is to weaken U.S. geopolitical and military capabilities and advance its own by using all means available including cyberattacks to undermine the defense industrial base and the broader U.S. economy from which America draws its strength. "U.S. military superiority since World War II has relied on both U.S. economic scale and technological superiority," a January 2018 DOD study concluded.[52]

Washington should never send its soldiers into a fair fight. Our adversaries agree, so they are trying to defeat our weapons systems and undermine our military capabilities before we realize that we are already at war. Belatedly, the U.S. military and intelligence communities are starting to take notice. For example:

- In its annual report to Congress on China's military capabilities, the Pentagon has warned that Beijing uses its cyber capabilities to "exfiltrate sensitive information from the [defense industrial base]" which in turn "threaten[s] to erode U.S. military advantages and imperil the infrastructure and prosperity on which those advantages rely."[53]

- The head of FBI counterintelligence has testified similarly that China's "economic aggression, including its relentless theft of U.S. assets" through cyber and traditional means, "is positioning China to supplant [the United States] as the world's superpower."[54]

- The U.S. Navy reportedly has made the economic endgame of adversaries such as China even more explicit: "The systems the U.S. relies upon to mobilize, deploy and sustain forces have been extensively targeted by potential adversaries, and compromised to such extent that their reliability is questionable."[55]

Global Trade, Rule Enforcement, and China's Civil–Military Fusion

As the U.S. military considers how to fight and win wars in the 21st century when it has an adversary with an economy that is quickly advancing on its own, diagnosing how Beijing's creeping invasion of our national security industrial base could have gone unnoticed—or, perhaps worse, been noticed but not addressed—is critical.

A 2005 RAND study, for example, warned that Huawei and other ostensibly private companies are in fact merely the "public face for, sprang from, or are significantly engaged in joint research" with the Chinese military. Huawei itself "maintains deep ties with the Chinese military."[56] An even earlier 2001 report in the *Far Eastern Economic Review* concluded that Huawei is "financially and politically supported by the Chinese government."[57] In 2012, the House Intelligence Committee concluded that Huawei's "assertions denying support by the Chinese government are not credible."[58] Yet Western media continue to treat Huawei's ownership as an unanswered question,[59] and the CIA is still trying to convince U.S. allies that Huawei receives state funding.[60]

We have known since that 2012 House Intelligence Committee investigation that Chinese telecommunications giant Huawei shows a "pattern of disregard" for intellectual property rights.[61] This state-backed, multibillion-dollar company is accused of stealing innovations from everyone from start-ups to multinational companies, yet the press was surprised that Huawei had a policy of providing bonuses to employees who stole trade secrets.[62]

Huawei's theft of trade secrets is just one example of China's persistent efforts to steal research and development, intellectual property, and proprietary technology. In another example, China announced in 2014 that it intended to spend $150 billion to become dominant in the semiconductor industry.[63] Semiconductors are critical components of all modern technology. The Semiconductor Industry Association warned that while the United States has led previous semiconductor innovations, "overseas governments are seeking to displace U.S. leadership through huge government investments in both commercial manufacturing and scientific research."[64] Their efforts include stealing trade secrets from American companies that make the world's most advanced semiconductors.

Boise, Idaho-based Micron provides as much as a quarter of the world's Dynamic Random Access Memory (DRAM) integrated circuits, which are used in everything from personal computers to the U.S. military's next-generation thermal weapon sights.[65] In 2018, the U.S. government indicted Chinese state-owned Fujian Jinhua Integrated Circuit Company for stealing Micron's trade secrets[66] and added Fujian Jinhua to its Entity List, barring the export of any U.S.-origin goods to the company.[67] The theft began after Micron turned down an acquisition offer from a Chinese company.[68] Before this intellectual property theft, China did not possess DRAM technology, but instead of investing in research and development, it "conspired to circumvent Micron's restrictions on its proprietary technology," according to the indictment.[69]

Nor was this American company the only target of Chinese operations. Dutch company ASML, a global supplier to the semiconductor industry, was also the victim of commercial espionage but quickly denied any "national conspiracy." ASML's CEO said, "We resent any suggestion that this event should have any implication for ASML conducting business in China. Some of the individuals (involved) happened to be Chinese nationals."[70]

This defensiveness is perhaps understandable given the limited recourse available to companies that are victimized by Chinese

government–supported espionage. After the Department of Justice accused Chinese military hackers of cyber-enabled espionage and trade secrets theft against U.S. Steel,[71] the company has tried to bring a case before the U.S. International Trade Commission against Chinese firm Baosteel for selling a high-tech steel similar to its own products, but U.S. Steel faces a problem. It is asserting that Baosteel stole proprietary technology, but the indicted hackers worked only for the Chinese military, never for Baosteel.[72] The global trade system and mechanism for enforcing the rules are not set up to address China's military–civil fusion.

Additionally, the U.S. legal system is not well suited to combating China's exploitation of the rules-based system for its geopolitical and military gain.[73] For example, instead of undergoing a Committee on Foreign Investment in the United States (CFIUS) process, which likely would have resulted in a negative review,[74] Chinese firm Wanxiang waited until A123 Systems went bankrupt and purchased the company's technology for fast-charging lithium-ion batteries.[75] When high-end microchip producer ATopTech went bankrupt, Chinese firm Avatar Integrated Systems used the judicial system to block U.S. competitor Synopsys from raising CFIUS concerns[76] and purchased ATopTech's technology.[77]

The bankruptcy process is not the only area in which China has figured out how to maneuver around the CFIUS process. The U.S.–China Economic and Security Review Commission warned in a May 2019 report that CFIUS and export control regulations "have been unable to adequately assess and address the risks of increased technology transfers to China." As a result, China has been able "to pursue investments in critical U.S. technologies that could jeopardize U.S. technological innovation and national security."[78]

China participates in more than 10 percent of all venture capital deals in the United States and in 2015 alone invested $11.5 billion in early-stage technology deals.[79] Investments in emerging technology, including artificial intelligence, augmented reality/virtual reality, robotics, and financial technology, represent about 40 percent of China's overall investments.[80] Put succinctly, because innovation occurs in the private sector, "state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed," as the National Defense Strategy recognized.[81]

Meanwhile, Beijing requires foreign companies interested in selling into the Chinese market to form joint ventures with local firms and uses "the administrative licensing and approvals process to require or pressure the transfer of technology" from foreign firms to their Chinese counterparts, according to an in-depth U.S. Trade Representative study of China's unfair trade policies.[82] The American Chamber of Commerce in China has similarly warned that Chinese government authorities often demand "unnecessary disclosure" of confidential technological and other information.[83] European companies report feeling similarly compelled to give away critical technology to gain access to the Chinese market.[84]

In short, China uses all means to acquire sensitive, national security–related technology at the expense of America's economy and military capabilities. China uses illegal means like industrial and cyber espionage and forcible technology transfers as well as legal ones like strategic investment.[85]

As the United States considers how these economic battle campaigns could affect the outcome of military engagements, it is wise to consider that World War II could have ended differently had such adversarial practices been in place at that time. General Dwight Eisenhower attributed U.S. victory to Andrew Jackson Higgins, a small-boat builder who adapted his shallow-draft boat designs to fulfill the U.S. military's request for a small vessel that could transport both troops and vehicles from ships to the beach.[86] Higgins's story is a combination of individual ingenuity and the American military's ability to gain an advantage over the adversary by deploying next-generation weaponry and matériel onto the battlefield.

- What would have happened if the Axis Powers had stolen Higgins's boat designs before he could get his product into the hands of the U.S. military?

- What would have happened if, when he applied for his patent, Japanese government–affiliated entities had beaten him to the punch and filed a patent using designs they had stolen?

- What if, during the interwar period, Higgins had decided to sell into the European market but had been forced to form a joint venture with German firms and transfer critical technology to a government the U.S. would soon face on the battlefield?

Controlling the data of the battlefield is akin to controlling the commanding heights. With such control, one can see the gathering armies, their supply lines, and their points of weakness. China is engaged in "eco-political terraforming" to achieve such a position by planting its equipment throughout the global infrastructure and then leveraging that equipment to gather, manipulate, or otherwise control the vast amounts of data moving through the system.

The import of the Huawei issue is the import of the future of high-speed bidirectional data transmission, which is critical for the functioning of a modern military and a modern economy. With an estimated 75 billion devices connected to the Internet by 2025, who controls the telecommunications architecture and infrastructure ultimately can control the data those devices carry. The road that is being built to carry that data is 5G, and the U.S. government does not wish to see those personal, consumer, technological, and military data travelling that road to Beijing.

Yes, the build-out of 5G infrastructure is ideal for China's eco-political terraforming strategy.

Building a Secure Infrastructure for National Security Data Transmission

With a challenge as large as the one presented by China's eco-political terraforming, the solutions to the problem of preserving U.S. military superiority necessarily come from all corners of the government. While the "whole of government" mantra sounds nice, it has become synonymous with "whole of little." The battlefield of the 21st century will truly demand a more unified approach.

Fifteen years after the United States unleashed its financial furies against its adversaries, Congress added the Secretary of the Treasury as a statutory member of the National Security Council,[87] but battles of the latter half of the 20th century and the beginning of the 21st have not taught policymakers the importance of other elements of the U.S. government like the Department of Commerce and the Federal Communications Commission (FCC). These agencies and others will be central to Washington's ability to defend its economic, defense, and overall national security interests against its adversaries' campaigns.

In May 2019, for example, the FCC rejected an application by state-owned China Mobile to provide international service for U.S. callers,[88] citing a recommendation from the Commerce Department to deny the application because of national security and law enforcement concerns.[89] The FCC also issued a proposed rule banning the use of federal funds by local municipalities to purchase equipment from "companies that pose a national security threat to United States communications networks or the communications supply chain."[90] The FCC is awaiting input from the Commerce Department with respect to which companies would fit the ban's criteria.[91] The Commerce Department, for its part, is attempting to define emerging technologies and introduce export controls to prevent the sale of these technologies to adversaries.[92]

Most recently, the President issued an executive order banning all U.S. persons from purchasing information communication technology from firms controlled by a foreign adversary and deemed to pose "an unacceptable risk to the national security of the United States or the security and safety of United States persons."[93] The executive order itself does not

name specific companies and technologies and does not mention U.S. adversaries by name, but it is widely seen as addressing Chinese technology companies in general and Huawei in particular.[94] To emphasize this point, on the same day, the Commerce Department added Huawei to its Entity List.[95]

Federal agencies, meanwhile, are working with U.S. allies to create lists of trusted suppliers in an effort to cultivate viable alternatives to Chinese products. As Department of Homeland Security Cybersecurity and Infrastructure Security Agency Director Christopher Krebs has testified, allied coordination would "drive the dynamics that could move the market" to address "China's predatory industrial policy approach."[96]

Coordination creates market incentives for companies to innovate and create more secure products. Without these incentives, U.S. companies might not be able to compete with Chinese firms' discounted prices and thus not be able to convert innovation into commercial success and commercial success back into additional innovation, which in turn would leave the U.S. at a disadvantage across a broad range of security interests. The Prague 5G summit in May 2019, for example, set out a nonbinding but common approach to ensuring that 5G decisions consider not only economic, but also national security concerns.[97] More broadly, a consortium of likeminded nations that identifies both trusted vendors and the companies and technology that pose risks to critical infrastructure and communications systems would protect the integrity of networks and data on which the U.S. and allied military capabilities depend.

Conclusion

The U.S. government's recognition that the private sector is a conduit through which adversaries conduct cyber-enabled economic warfare and other cyberattacks[98] and that the future information and communications infrastructure must therefore have security at its core is welcome but insufficient. Without robust defense and concerted counteroffensive investments, hostile adversaries will rapidly erode our military and political strength.

The United States is now in a peer competition, and if our adversaries are embedded in both our publicly and privately owned and operated critical infrastructure, the U.S. military cannot fully trust its warfighting capability. Mutually Assured Destruction was a central tenet of Cold War deterrence in the nuclear age. Much is now being written about how to achieve deterrence in a cyber-enabled world.[99] If the U.S. is to maintain the advantage over adversaries who try to undermine our ability to trust our own systems, and if it is to eliminate or mitigate vulnerabilities to such attacks, perhaps the adversary must also be skeptical of the integrity of his own weapons and communications systems. Call it Mutually Assured Military Standoff if you will.

In any event, it is abundantly clear that competition—and outright conflict if and when it occurs—between great powers will incorporate the full range of tools available to major states, including economic and cyber measures that directly attack both the military's might and the citizenry's willpower. To ensure its standing as the world's largest free-market democracy, the U.S. must not only recognize the importance of the economy to our ability to defend ourselves, but also take the necessary steps to prepare for this domain of 21st century state warfare.

Endnotes

1. Mark Cartwright, "Peloponnesian War," *Ancient History Encyclopedia*, May 2, 2018, https://www.ancient.eu/Peloponnesian_War/ (accessed June 12, 2019), and "Peloponnesian War," *Encyclopaedia Britannica*, https://www.britannica.com/event/Peloponnesian-War (accessed June 12, 2019).
2. "Blockades—Development of the Law," American Foreign Relations, https://www.americanforeignrelations.com/A-D/Blockades-Development-of-the-law.html (accessed June 12, 2019), and Frank J. Merli and Robert H. Ferrell, "Blockades," in *Encyclopedia of American Foreign Policy*, 2nd ed., Vol. 1, Chronology A–D, ed. Alexander DeConde, Richard Dean Burns, Frederick Logeval1, and Louise B. Ketz (New York: Charles Scribner's Sons, 2002), pp. 171–184, http://1.droppdf.com/files/X3CPy/encyclopedia-of-american-foreign-policy.pdf (accessed June 12, 2019).
3. "From George Washington to the United States Senate and House of Representatives, 8 January 1790," National Archives, *Founders Online*, https://founders.archives.gov/documents/Washington/05-04-02-0361 (accessed June 12, 2019).
4. "10 Facts About the 18th Century Patents," George Washington's Mount Vernon, https://www.mountvernon.org/george-washington/the-first-president/patents/ (accessed June 12, 2019).
5. Ben Baack, "The Economics of the American Revolutionary War," Economic History Association, EH.Net, https://eh.net/encyclopedia/the-economics-of-the-american-revolutionary-war-2/ (accessed June 12, 2019).
6. "Alexander Hamilton's Final Version of the Report on the Subject of Manufactures, [5 December 1791]," National Archives, *Founders Online*, https://founders.archives.gov/documents/Hamilton/01-10-02-0001-0007#ARHN-01-10-02-0001-0007-fn-0123 (accessed June 12, 2019).
7. Michael Hsieh, "Intellectual Property Piracy as Economic Privateering," in *Cyber-Enabled Economic Warfare: An Evolving Challenge*, ed. Samantha F. Ravich (Washington: Hudson Institute, 2016), pp. 73–92, https://s3.amazonaws.com/media.hudson.org/files/publications/2015.08CyberEnabledEconomicWarfareAnEvolvingChallenge.pdf (accessed June 12, 2019).
8. Nicholas A. Lambert, *Planning Armageddon: British Economic Warfare and the First World War* (Cambridge, MA: Harvard University Press, 2012), p. 124, http://the-eye.eu/public/concen.org/Nicholas%20A.%20Lambert%20-%20Planning%20Armageddon%20-%20British%20Economic%20Warfare%20and%20the%20First%20World%20War%20-%20pdf%20%5BTKRG%5D/Nicholas%20A.%20Lambert%20-%20Planning%20Armageddon%20-%20British%20Economic%20Warfare%20and%20the%20First%20World%20War%20-%20pdf%20%5BTKRG%5D.pdf (accessed July 19, 2019).
9. Quoted in W. N. Medlicott, *The Economic Blockade*, Vol. 1 (London: His Majesty's Stationery Office and Longmans, Green and Co., 1952), p. 1, https://archive.org/stream/economicblockade012328mbp/economicblockade012328mbp_djvu.txt (accessed June 13, 2019).
10. Daniel Yergin, "Blood and Oil: Why Japan Attacked Pearl," *The Washington Post*, December 1, 1991, https://www.washingtonpost.com/archive/opinions/1991/12/01/blood-and-oil-why-japan-attacked-pearl/1238a2e3-6055-4d73-817d-baf67d3a9db8/?utm_term=.bcbd1805075d (accessed June 13, 2019).
11. Juan C. Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: Public Affairs, 2013), p. 240.
12. Ibid., p. 244.
13. Victor Cha, *The Impossible State: North Korea, Past and Future* (New York: HarperCollins, 2013), p. 266.
14. William J. Burns, Under Secretary for Political Affairs, U.S. Department of State, testimony in hearing, *Implementing Tougher Sanctions on Iran: A Progress Report*, Committee on Foreign Affairs, U.S. House of Representatives, 111th Cong., 2nd Sess., December 1, 2010, p. 14, https://www.govinfo.gov/content/pkg/CHRG-111hhrg62665/pdf/CHRG-111hhrg62665.pdf (accessed June 13, 2019).
15. Figure 7, "Sentiment Stagnated in Late 2014/Early 2015 But at Much Improved Levels from 2012/2013 (Red Line = Sentiment)," in Mark Dubowitz, Annie Fixler, and Rachel Ziemba, "Iran's Economic Resilience Against Snapback Sanctions Will Grow Over Time," Foundation for Defense of Democracies, Center on Sanctions and Illicit Finance, and Roubini Global Economics, June 2015, p. 13, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/publications/Iran_economy_resilience_against_snapback_sanctions.pdf (accessed June 13, 2019).
16. Geneive Abdo and Firas Maksad, "Evidence Trump's Iran Policy Is Working," *New York Daily News*, May 2, 2019, https://www.nydailynews.com/opinion/ny-oped-evidence-trumps-iran-policy-is-working-20190502-xwjyle54rbed5jcounqz5d4tjm-story.html (accessed June 13, 2019).
17. Saeed Ghasseminejad, "Inflation in Iran Is on the Rise," Foundation for Defense of Democracies *Policy Brief*, April 30, 2019, https://www.fdd.org/analysis/2019/04/30/inflation-in-iran-is-on-the-rise/ (accessed June 13, 2019).
18. Mark Dubowitz, "Midterm Assessment: Iran," Foundation for Defense of Democracies, January 21, 2019, https://www.fdd.org/analysis/2019/01/31/midterm-assessment-iran/ (accessed June 13, 2019).

19. Table 2.4.2, "Middle East and North Africa Economy Forecasts," in World Bank Group, *Global Economic Prospects: The Turning of the Tide?*, June 2018, p. 136, http://pubdocs.worldbank.org/en/731741526414103878/Global-Economic-Prospects-June-2018-Middle-East-and-North-Africa-analysis.pdf (accessed June 13, 2019), and Table 2.4.2, "Middle East and North Africa Economy Forecasts," in World Bank Group, *Global Economic Prospects: Darkening Skies*, January 2019, p. 94, http://pubdocs.worldbank.org/en/478341542818395087/Global-Economic-Prospects-Jan-2019-Middle-East-and-North-Africa-analysis.pdf (accessed June 13, 2019).

20. Fact Sheet, "Advancing the U.S. Maximum Pressure Campaign on Iran," U.S. Department of State, April 22, 2019, https://www.state.gov/advancing-the-u-s-maximum-pressure-campaign-on-iran/ (accessed June 13, 2019).

21. Liz Sly and Suzan Haidamous, "Trump's Sanctions on Iran Are Hitting Hezbollah, and It Hurts," *The Washington Post*, May 18, 2019, https://www.washingtonpost.com/world/middle_east/trumps-sanctions-on-iran-are-hitting-hezbollah-hard/2019/05/18/970bc656-5d48-11e9-98d4-844088d135f2_story.html?utm_term=.61f2c6117eb2 (accessed June 13, 2019).

22. Ben Hubbard, "Iran's Allies Feel the Pain of American Sanctions," *The New York Times*, March 28, 2019, https://www.nytimes.com/2019/03/28/world/middleeast/iran-sanctions-arab-allies.html (accessed June 13, 2019).

23. Abstract of Charles Wolf, Jr., "Future Directions for Analysis of the Soviet Economy," RAND Corporation *Paper*, 1984, https://www.rand.org/pubs/papers/P7040.html (accessed June 13, 2019).

24. Glenn E. Curtis, ed., *Russia: A Country Study*, Library of Congress, Federal Research Division, Area Handbook Series, 1998, https://cdn.loc.gov/master/frd/frdcstdy/ru/russiacountrystu00curt/russiacountrystu00curt.pdf (accessed June 13, 2019).

25. Charles Wolf, Jr., and Steven W. Popper, eds., *Defense and the Soviet Economy: Military Muscle and Economic Weakness* (Santa Monica: RAND Corporation, 1992), p. 6, https://www.rand.org/content/dam/rand/pubs/notes/2007/N3474.pdf (accessed June 13, 2019).

26. Chris C. Carvounis and Brinda Z. Carvounis, "Economic Competition and Cooperation Between the Soviet Union and the United States in Less-Developed Countries," *Business Economics*, Vol. 25, No. 1 (January 1990), pp. 36–41.

27. Fortune 500, "1980 Full List," http://archive.fortune.com/magazines/fortune/fortune500_archive/full/1980/ (accessed June 13, 2019).

28. Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, "Chinese Technology Transfer Challenges to U.S. Export Control Policy," remarks delivered to the Center for Strategic and International Studies Project on Nuclear Issues, Los Alamos, New Mexico, July 11, 2018, https://www.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/chinese-technology-transfer-challenges-to-u-s-export-control-policy/ (accessed July 18, 2019).

29. Mark Pomerleau, "Is the Defense Department's Entire Vision of Cybersecurity Wrong?" *Fifth Domain*, November 14, 2018, https://www.fifthdomain.com/dod/2018/11/14/is-the-defense-departments-entire-vision-of-cybersecurity-wrong/ (accessed June 13, 2019).

30. World Bank Group, "China at-a-Glance: Overview," last updated April 8, 2019, https://www.worldbank.org/en/country/china/overview (accessed June 13, 2019).

31. Ibid.

32. Salvatore Babones, "China's Economy: Not So Big After All," *The National Interest*, March 12, 2019, https://nationalinterest.org/feature/chinas-economy-not-so-big-after-all-46887 (accessed June 13, 2019).

33. Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," Foundation for Defense of Democracies, Center on Sanctions and Illicit Finance *Resource Document*, February 22, 2017, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/MEMO_CyberDefinitions_07.pdf (accessed June 13, 2019).

34. Simon Atkinson, "Is China Retaliating Against Lotte Missile Deal?" BBC News, March 6, 2017, http://www.bbc.com/news/business-39176388 (accessed June 13, 2019); Joyce Lee and Adam Jourdan, "South Korea's Lotte Reports Store Closures in China amid Political Stand-off," Reuters, March 5, 2017, https://www.reuters.com/article/us-southkorea-china-lotte/south-koreas-lotte-says-four-retail-stores-in-china-closed-after-inspections-idUSKBN16D03U (accessed June 13, 2019); and Bill Ide, "Chinese Media Call for Boycott of South Korean Goods," Voice of America, March 2, 2017, https://www.voanews.com/a/chinese-media-call-for-boycott-of-south-korean-goods/3746701.html (accessed June 13, 2019).

35. David Josef Volodzko, "China Wins Its War Against South Korea's US THAAD Missile Shield—Without Firing a Shot," *South China Morning Post*, November 18, 2017, https://www.scmp.com/week-asia/geopolitics/article/2120452/china-wins-its-war-against-south-koreas-us-thaad-missile (accessed June 13, 2019).

36. Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," Foundation for Defense of Democracies, September 2018, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_China_CEEW.pdf (accessed June 13, 2019), and U.S. Department of Defense, Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017*, May 15, 2017, pp. 59–60, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF (accessed June 13, 2019).

37. John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice, statement before the Committee on the Judiciary, United States Senate, for a hearing on "China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses," December 12, 2018, p. 5, https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf (accessed June 13, 2019).

38. Press release, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," U.S. Department of Justice, October 30, 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal (accessed June 13, 2019).

39. Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, National Bureau of Asian Research, February 2017, p. 7, http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf (accessed June 13, 2019). For the commission's original report, see Commission on the Theft of American Intellectual Property, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*, National Bureau of Asian Research, May 2013, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf (accessed June 13, 2019).

40. U.S. International Trade Commission, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, Investigation No. 332-519, May 2011, pp. xviii–xx, https://www.usitc.gov/publications/332/pub4226.pdf (accessed June 13, 2019).

41. Press release, "Chinese Company Sinovel Wind Group Convicted of Theft of Trade Secrets," U.S. Department of Justice, January 24, 2018, https://www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets (accessed June 13, 2019).

42. Lorand Laskai, "Civil–Military Fusion and the PLA's Pursuit of Dominance in Emerging Technologies," The Jamestown Foundation *China Brief*, Vol. 18, Issue 6 (April 9, 2018), https://jamestown.org/program/civil-military-fusion-and-the-plas-pursuit-of-dominance-in-emerging-technologies/ (accessed June 13, 2019).

43. Xinhua, "Xi Calls for Deepened Military–Civil Integration," March 12, 2018, http://www.xinhuanet.com/english/2018-03/12/c_137034168.htm (accessed June 13, 2019).

44. Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit Experimental, January 2018, p. 3, https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf (accessed June 13, 2019).

45. U.S. Department of Defense, Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019*, May 2, 2019, pp. 101–102, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf (accessed June 13, 2019).

46. Nicholas Eftimiades, "Uncovering Chinese Espionage in the US," *The Diplomat,* November 28, 2018, https://thediplomat.com/2018/11/uncovering-chinese-espionage-in-the-us/ (accessed June 13, 2019).

47. Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-enabled Economic Warfare," p. 19; Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011*, October 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf (accessed June 13, 2019); and Executive Office of the President, Office of the United States Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of The Trade Act of 1974*, March 22, 2018, pp. 167–168, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF (accessed June 13, 2019).

48. Laura Sullivan and Cat Schuknecht, "As China Hacked, U.S. Businesses Turned a Blind Eye," NPR, April 12, 2019, https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blind-eye (accessed June 13, 2019).

49. Press release, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years."

50. Dustin Volz, "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets," *The Wall Street Journal*, updated March 5, 2019, https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800 (accessed June 13, 2019), and Gordon Lubold and Dustin Volz, "Chinese Hackers Breach U.S. Navy Contractors," *The Wall Street Journal*, updated December 14, 2018, https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401?mod=article_inline (accessed June 13, 2019).

51. Press release, "Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies," U.S. Department of Justice, October 10, 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading (accessed June 13, 2019).

52. Brown and Singh, "China's Technology Transfer Strategy," p. 2.

53. U.S. Department of Defense, Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019*, p. 65.

54. Ellen Nakashima, "Top FBI Official Warns of Strategic Threat from China Through Economic and Other Forms of Espionage," *The Washington Post*, December 12, 2018, https://www.washingtonpost.com/world/national-security/top-fbi-official-warns-of-strategic-threat-from-china-through-economic-and-other-forms-of-espionage/2018/12/12/38067ee2-fe36-11e8-83c0-b06139e540e5_story.html?utm_term=.1996dd45ec2c (accessed June 13, 2019).

55. Jason Miller, "Why the Navy Is Giving Agencies, Industry a Much-Needed Wake-up Call on Supply Chain Risks," Federal News Network, April 4, 2019, https://federalnewsnetwork.com/acquisition/2019/04/navy-giving-agencies-industry-much-needed-wake-up-call-on-supply-chain-risks/ (accessed June 13, 2019).

56. Evan S. Mederios, Roger Cliff, Keith Crane, and James C. Mulvenon, *A New Direction for China's Defense Industry* (Santa Monica: RAND Corporation, Project Air Force, 2005), pp. 217–218, https://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG334.pdf (accessed June 13, 2019).

57. Bruce Gilley, "Huawei's Fixed Line to Beijing," *Far Eastern Economic Review,* December 28, 2000–January 4, 2001, p. 94, http://www.web.pdx.edu/~gilleyb/Huawei_FEER28Dec2000.pdf (accessed June 13, 2019).

58. Chairman Mike Rogers and Ranking Member C. A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, Permanent Select Committee on Intelligence, U.S. House of Representatives, 112th Cong., October 8, 2012, p. 21, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf (accessed June 13, 2019).

59. Raymond Zhong, "Who Owns Huawei? The Company Tried to Explain. It Got Complicated," *The New York Times*, April 25, 2019, https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html (accessed June 13, 2019).

60. Lucy Fisher and Michael Evans, "CIA Warning over Huawei," *The Times*, April 20, 2019, https://www.thetimes.co.uk/edition/news/cia-warning-over-huawei-rz6xc8kzk (accessed June 13, 2019).

61. Rogers and Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, p. 31.

62. Erik Schatzker, "Huawei Sting Offers Rare Glimpse of the U.S. Targeting a Chinese Giant," *Bloomberg Businessweek,* February 4, 2019, https://www.bloomberg.com/news/features/2019-02-04/huawei-sting-offers-rare-glimpse-of-u-s-targeting-chinese-giant (accessed June 13, 2019), and Laurel Wamsley, "A Robot Named 'Tappy': Huawei Conspired to Steal T-Mobile's Trade Secrets, Says DOJ," NPR, January 29, 2019, https://www.npr.org/2019/01/29/689663720/a-robot-named-tappy-huawei-conspired-to-steal-t-mobile-s-trade-secrets-says-doj (accessed June 13, 2019).

63. U.S. Department of Commerce, "U.S. Secretary of Commerce Delivers Major Policy Address on Semiconductors at Center for Strategic and International Studies," remarks as prepared for delivery, November 2, 2016, https://2014-2017.commerce.gov/news/secretary-speeches/2016/11/us-secretary-commerce-penny-pritzker-delivers-major-policy-address.html (accessed July 23, 2019). See also Clay Chandler, "Why China Is Emerging as a Tech Superpower to Rival the U.S.," *Fortune*, November 21, 2017, http://fortune.com/2017/11/21/china-innovation-dji/ (accessed June 13, 2019).

64. Semiconductor Industry Association, "Winning the Future: A Blueprint for Sustained U.S. Leadership in Semiconductor Technology," April 2019, p. 3, https://www.semiconductors.org/wp-content/uploads/2019/04/FINAL-SIA-Blueprint-for-web.pdf (accessed June 13, 2019).

65. Alan Rappeport, "U.S. to Block Sales to Chinese Tech Company over Security Concerns," *The New York Times*, October 29, 2018, https://www.nytimes.com/2018/10/29/us/politics/fujian-jinhua-china-sales.html (accessed June 13, 2019).

66. Press release, "PRC State-Owned Company, Taiwan Company, and Three Individuals Charged with Economic Espionage," U.S. Department of Justice, November 1, 2018, https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage (accessed June 13, 2019).

67. Press release, "Addition of Fujian Jinhua Integrated Circuit Company, Ltd (Jinhua) to the Entity List," U.S. Department of Commerce, October 29, 2018, https://www.commerce.gov/news/press-releases/2018/10/addition-fujian-jinhua-integrated-circuit-company-ltd-jinhua-entity-list (accessed June 14, 2019).

68. Paul Mozur, "Inside a Heist of American Chip Designs, as China Bids for Tech Power," *The New York Times*, June 22, 2018, https://www.nytimes.com/2018/06/22/technology/china-micron-chips-theft.html?module=inline (accessed June 14, 2019).

69. David Ignatius, "America's Overt Payback for China's Covert Espionage," RealClearPolitics, November 16, 2018, https://www.realclearpolitics.com/articles/2018/11/16/americas_overt_payback_for_chinas_covert_espionage_138675.html (accessed June 14, 2019).

70. Toby Sterling and Anthony Deutsch, "ASML Says It Suffered Intellectual Property Theft, Rejects 'Chinese' Label," Reuters, April 11, 2019, https://www.reuters.com/article/us-asml-china-spying/asml-falls-victim-to-corporate-theft-plays-down-impact-idUSKCN1RN0DK (accessed June 14, 2019).

71. Press release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (accessed June 14, 2019).

72. Kevin L. Kearns, "U.S. Steel's Costly Battle Against China's Cyber-Hacking," *The Hill,* March 13, 2017, https://thehill.com/blogs/pundits-blog/technology/323738-us-steels-costly-battle-against-chinas-cyber-hacking (accessed June 14, 2019).

73. Camille A. Stewart, "Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings," *Journal of National Security Law & Policy*, forthcoming 2019.

74. Patrick Fitzgerald, Mike Ramsey, Mike Spector, and Ryan Tracy, "Battery Maker Files for Bankruptcy," *The Wall Street Journal*, updated October 16, 2012, https://www.wsj.com/articles/SB10000872396390443854204578060433271656440 (accessed June 14, 2019).

75. Brad Plumer, "A123 Systems Files for Bankruptcy: Here's What You Need to Know," *The Washington Post*, October 16, 2012, https://www.washingtonpost.com/news/wonk/wp/2012/10/16/a123-systems-files-for-bankruptcy-heres-what-you-need-to-know/?utm_term=.9f05ef7e3b60 (accessed June 14, 2019); Charles Ridley, "China's Wanxiang Wins Auction for A123," CNN, December 10, 2012, https://money.cnn.com/2012/12/10/news/wanxiang-a123-auction/index.html (accessed June 14, 2019); and Tom Hals and Ben Klayman, "Chinese Firm Wins A123 Despite U.S. Tech Transfer Fears," Reuters, January 29, 2013, https://www.reuters.com/article/us-a123-wanxiang-approval/chinese-firm-wins-a123-despite-u-s-tech-transfer-fears-idUSBRE90S0JN20130129 (accessed June 14, 2019).

76. Motion of Avatar Integrated Systems, Inc. for Protective Order, United States Bankruptcy Court for the District of Delaware, In re: ATopTech, Inc., Chapter 11 Case No. 17-10111 (MFW), Ref. D.I. 275, http://bankrupt.com/misc/deb17-10111-305.pdf (accessed June 14, 2019).

77. Cory Bennett and Bryan Bender, "How China Acquires 'the Crown Jewels' of U.S. Technology," *Politico*, May 22, 2018, https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413 (accessed June 14, 2019), and Elsa B. Kania, "China's Threat to American Government and Private Sector Research and Innovation Leadership: Testimony before the House Permanent Select Committee on Intelligence," Center for a New American Security, July 19, 2018, https://www.cnas.org/publications/congressional-testimony/testimony-before-the-house-permanent-select-committee-on-intelligence#fn91 (accessed June 14, 2019).

78. Sean O'Connor, "How Chinese Companies Facilitate Technology Transfer from the United States," U.S.–China Economic and Security Review Commission *Staff Research Report*, May 6, 2019, p. 3, https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf (accessed June 14, 2019).

79. Brown and Singh, "China's Technology Transfer Strategy," p. 6.

80. Ibid., p. 7.

81. James Mattis, Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, U.S. Department of Defense, p. 3. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed June 14, 2019).

82. Executive Office of the President, Office of the United States Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of The Trade Act of 1974*, p. 19.

83. Jethro Mullen, "How China Squeezes Tech Secrets from U.S. Companies," CNN, August 14, 2017, https://money.cnn.com/2017/08/14/news/economy/trump-china-trade-intellectual-property/index.html (accessed June 14, 2019).

84. Julie Wernau, "Forced Tech Transfers Are on the Rise in China, European Firms Say," *The Wall Street Journal,* May 20, 2019, https://www.wsj.com/articles/forced-tech-transfers-are-on-the-rise-in-china-european-firms-say-11558344240 (accessed June 14, 2019).

85. Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," p. 9.

86. David Hendee, "D-Day: 'The Boat That Won the War' Was Designed by a Nebraskan," *Omaha World Herald*, May 26, 2014, https://www.omaha.com/news/military/d-day-the-boat-that-won-the-war-was-designed/article_a8d954bf-ed88-5881-8872-9090203a5569.html (accessed June 14, 2019). See also S. 991, Andrew Jackson Higgins Gold Medal Act, 107th Cong., 1st Sess., June 6, 2001, https://www.govinfo.gov/content/pkg/BILLS-107s991is/pdf/BILLS-107s991is.pdf (accessed June 14, 2019).

87. H.R. 3364, Countering America's Adversaries Through Sanctions Act, Public Law 115-44, 115th Cong., August 2, 2017, § 274, https://www.congress.gov/bill/115th-congress/house-bill/3364/text (accessed June 14, 2019).

88. Tony Romm, "U.S. Blocks Chinese State-Owned Telecom Giant out of Security Concerns," *The Washington Post*, May 9, 2019, https://www.washingtonpost.com/technology/2019/05/09/us-blocks-chinese-state-owned-telecom-giant-out-security-concerns-threatens-more-scrutiny/?utm_term=.fb9d010a9277 (accessed June 14, 2019), and Sasha Ingber, "FCC Blocks Chinese Company's Bid for International Phone Services in the U.S.," NPR, May 9, 2019, https://www.npr.org/2019/05/09/721772856/fcc-blocks-chinese-companys-bid-for-international-phone-services-in-the-u-s (accessed June 14, 2019).

89. Fact sheet, "Denial of International Section 214 Authority for China Mobile International (USA) Inc.: Memorandum Opinion and Order–IBFS File No. ITC-214-20110901-00289," Federal Communications Commission, April 18, 2019, p. 5, https://docs.fcc.gov/public/attachments/DOC-357087A1.pdf (accessed June 14, 2019), and Ajit Pai, "Fast, Reliable, and Secure," Federal Communications Commission, April 17, 2019, https://www.fcc.gov/news-events/blog/2019/04/17/fast-reliable-and-secure (accessed June 14, 2019).

90. Federal Communications Commission, "Chairman Pai Statement on Proposal to Help Protect Security of U.S. Communications Networks and Their Supply Chains," March 26, 2018, https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0326/DOC-349894A1.pdf (accessed June 14, 2019).

91. Mariam Baksh, "FCC, in Crafting Supply-Chain Proposal, Awaits Commerce Dept. 'List of Entities' Posing National Security Threat," Inside Cybersecurity, May 10, 2019, https://insidecybersecurity.com/daily-news/fcc-crafting-supply-chain-proposal-awaits-commerce-dept-list-entities-posing-national (accessed June 14, 2019).

92. U.S. Department of Commerce, Bureau of Industry and Security, "Review of Controls for Certain Emerging Technologies," *Federal Register*, Vol. 83, No. 223 (November 19, 2018), pp. 58201–58202, https://www.govinfo.gov/content/pkg/FR-2018-11-19/pdf/2018-25221.pdf (accessed June 14, 2019).

93. Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," The White House, May 15, 2019 https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (accessed June 14, 2019).

94. Damian Paletta, Ellen Nakashima, and David J. Lynch, "Trump Administration Cracks Down on Giant Chinese Tech Firm, Escalating Clash with Beijing," *The Washington Post*, May 16, 2019, https://www.washingtonpost.com/world/national-security/trump-signs-order-to-protect-us-networks-from-foreign-espionage-a-move-that-appears-to-target-china/2019/05/15/d982ec50-7727-11e9-bd25-c989555e7766_story.html?utm_term=.f3ef468f067e (accessed June 14, 2019).

95. Press release, "Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List," U.S. Department of Commerce, May 15, 2019, https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd (accessed June 14, 2019), and Annie Fixler and Mathew Ha, "Washington's Huawei Ban Combats Chinese Espionage Threat," Foundation for Defense of Democracies *Policy Brief*, May 16, 2019, https://www.fdd.org/analysis/2019/05/16/washingtons-huawei-ban-combats-chinese-espionage-threat/ (accessed June 14, 2019).

96. Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, statement on "5G: The Impact on National Security, Intellectual Property, and Competition" before the Committee on the Judiciary, U.S. Senate, May 14, 2019, pp. 5–6, https://www.judiciary.senate.gov/imo/media/doc/Krebs%20Testimony.pdf (accessed June 14, 2019).

97. "Statement from the Press Secretary," The White House, May 3, 2019, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-54/?wpisrc=nl_cybersecurity202&wpmm=1 (accessed June 14, 2019).

98. U.S. Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, p. 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed June 14, 2019).

99. See, for example, U.S. Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017, https://www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf (accessed June 14, 2019).