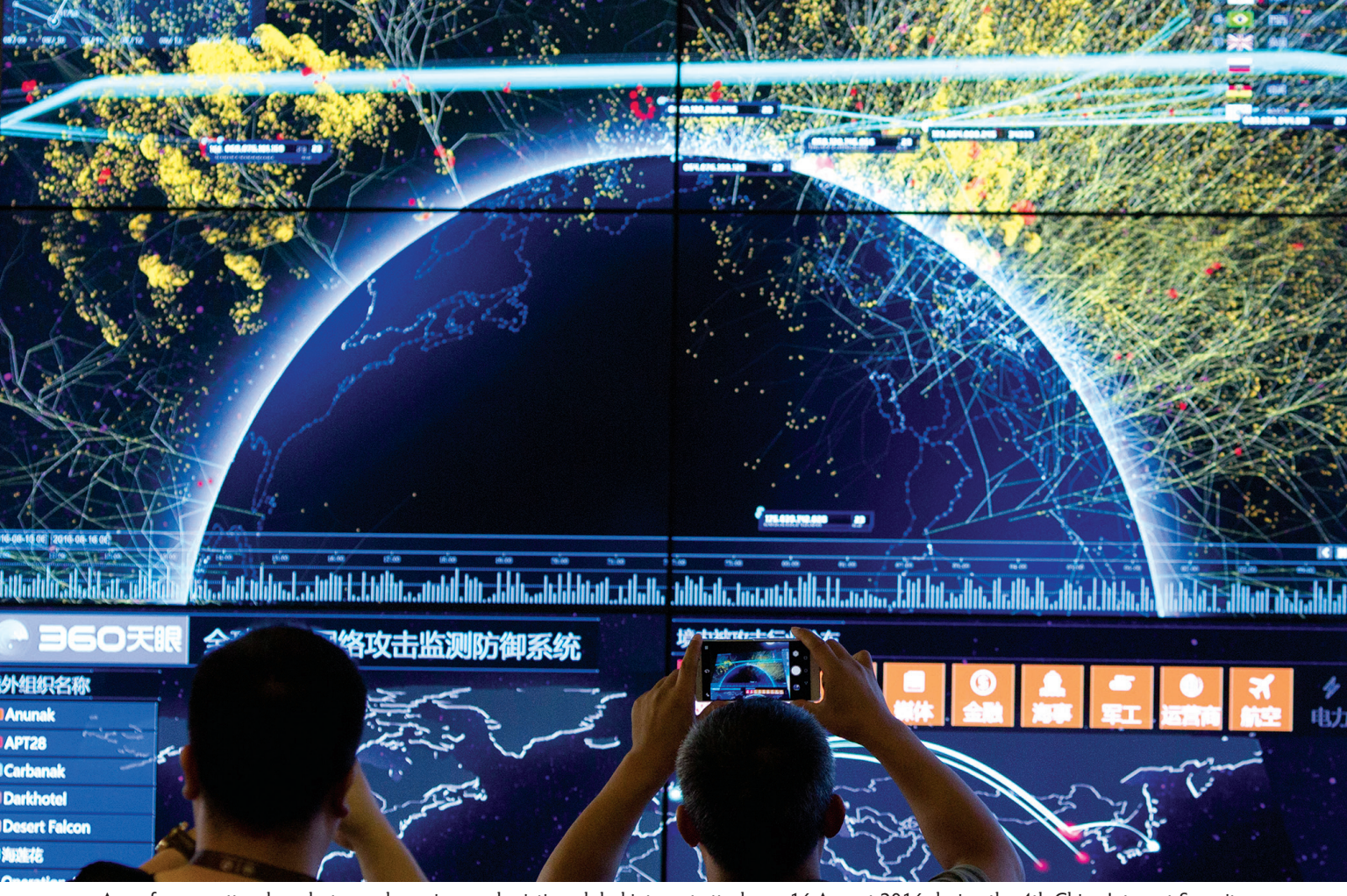


A conference attendee photographs an image depicting global internet attacks on 16 August 2016 during the 4th China Internet Security Conference (ISC) in Beijing. Having reached a level of sophistication today that renders even the most advanced internet protection systems vulnerable to sustained hacking attacks, Chinese government-sponsored internet theft of proprietary information of all kinds (e.g., industrial, scientific, military, economic, and personal) from the United States and other nations has reached pandemic proportions. (Photo by Ng Han Guan, Associated Press)

Steal the Firewood from Under the Pot

The Role of Intellectual Property Theft in Chinese Global Strategy

Capt. Scott Tosi, U.S. Army

In September 2015, the United States and China reached an agreement in principle that specified, among other stipulations, that "neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property [IP]."[1] However, less than two years later, China's use of cyber-enabled IP theft was outlined bluntly in the 2017 National Security Strategy, which stated that "every year, competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars."[2] This snapshot of cyber-enabled IP theft represents a broader issue of IP theft by China that spans a wide range of methods and means. According to estimates, China's total annual amount of IP theft ranges from $225 billion to $600 billion; moreover, China is responsible for 50 to 80 percent of all IP theft occurring against the United States.[3]

Chinese IP theft has broad implications for the U.S. Army and the Department of Defense (DOD), particularly as U.S. strategic focus shifts from counterinsurgency to large-scale combat operations among great powers.[4] IP theft of Army and DOD equities and research and development threatens U.S. military technological superiority in future decades as China states it "will upgrade our military capabilities," so "that by the mid-21st century our people's armed forces have been fully transformed into world-class forces."[5]

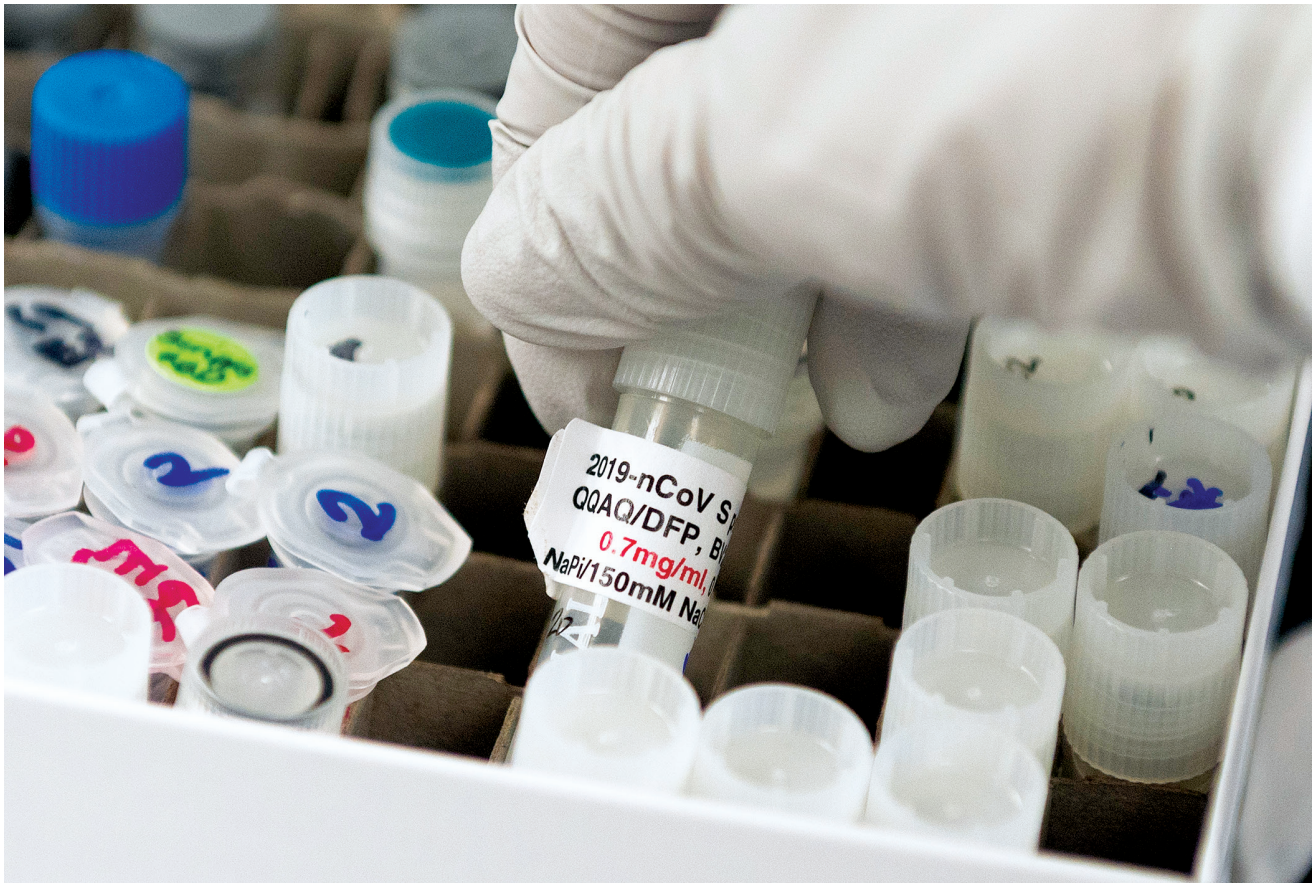
Early Chinese IP Theft: Hide Our Capacities and Bide Our Time

Capt. Scott Tosi, U.S. Army, is the company commander for Headquarters and Headquarters Company, 501st Military Intelligence Brigade in Camp Humphreys, Korea. He holds a BS in history and social sciences education from Illinois State University and an MPA from the University of Illinois–Springfield. His assignments include Yongsan, Korea; Fort George G. Meade, Maryland; and Camp Lemonnier, Djibouti.

China's systematic targeting of foreign IP began at the outset of its modernization under Deng Xiaoping in 1978, when it implemented the Four Modernizations (agriculture, industry, science and technology, and defense). China elicited economic and technological development from the United Nations Development Programme and World Bank that same year, and within a decade it began sending millions of Chinese students abroad to study. Four Modernizations included two major efforts designed to establish science and technology industries within China. The first, the National High-Tech Research and Development Program, sought to emphasize science and technology at Chinese universities under the direction of a central government committee and the People's Liberation Army (PLA). The second, the Torch Program, sought to bring back thousands of Western-trained Chinese academics.[6] Together, these programs served as the government's early attempt to centralize science and technology research and development within the Communist Party of China (CCP) and the PLA in order to establish the early forms of the state-owned enterprises (SOE) that work hand-in-hand with the CCP, PLA, and foreign private enterprises to acquire technology.

As early as 1998, Chinese theft of U.S. IP had grown problematic enough to warrant the creation of the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China. In 1999, the committee released a report that highlighted the efforts by China, as early as the 1970s, to target U.S. national labs to acquire sensitive technology.[7] The report also highlighted the primary means of acquisition at the time: illegally transferring technology from third countries, exploiting dual-use products, utilizing front companies to illegally acquire technology, using commercial enterprises as cover for technology acquisition, and acquiring interests in U.S. technology companies.[8] However, as China entered the twenty-first century, it looked toward a more aggressive means of sensitive technology acquisition.

Under President Hu Jintao, China launched the "National Medium- and Long-Term Plan for Development of Science and Technology (2006-2020)," or the "indigenous innovation" policy, in 2006. This policy implemented procurement rules that compelled foreign companies to hand over IP in exchange for access to Chinese markets.[9] Furthermore, the indigenous innovation increased domestic technological research and development funding while simultaneously pushing for "enhancing original innovation through co-innovation and re-innovation based on the assimilation of imported technologies."[10] Additional measures within the policy included state-run product testing geared toward studying foreign design and production



Dr. Nita Patel, director of antibody discovery and vaccine development, lifts a vial containing a potential COVID-19 vaccine 20 March 2020 at Novavax Labs in Gaithersburg, Maryland. The FBI has stated that the current Chinese government-directed effort to steal research related to development of a coronavirus vaccine as well as other industrial and military research through hacking has reached an unprecedentedly high level. (Photo by Andrew Caballero-Reynolds, Agence France-Presse)

methods, government procurement policies that blocked products not designed and produced in China to encourage foreign companies to disclose production methods within Chinese borders, and antimonopoly laws protecting SOEs that cooperated either under direct control or in close coordination with the CCP and the PLA.[11] Together, these policies promoted both legal and illegal acquisition of export-controlled IP from the United States and third countries as a quid pro quo for conducting business within mainland China.

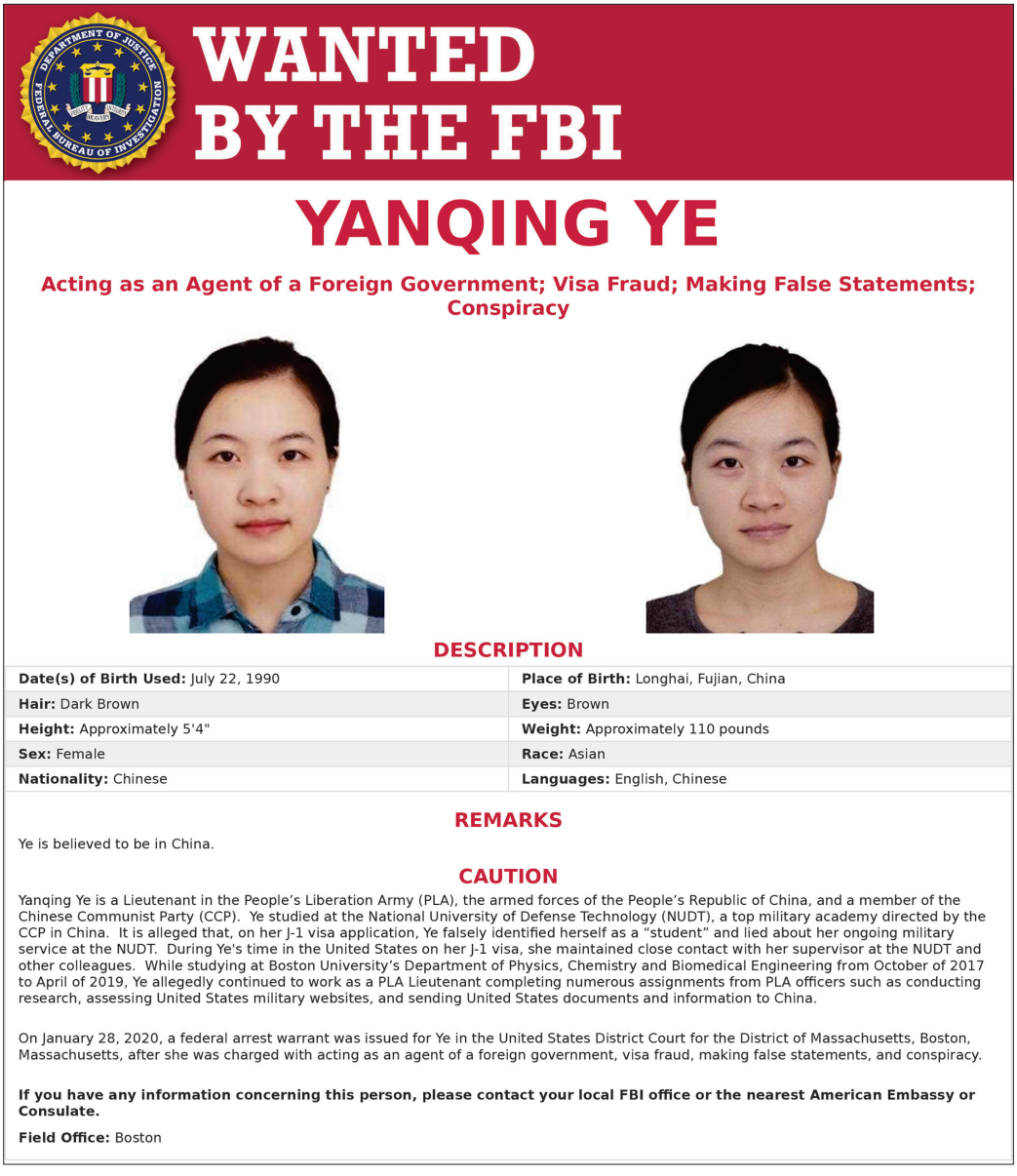
A Shift in Chinese Policy: Xi Jinping's Thoughts on Socialism with Chinese Characteristics for a New Era

In his address to the CCP's 19th National Congress on 18 October 2017, Xi outlined his plan for China to become "a global leader in terms of composite national strength and international influence" by 2050, surpassing the United States and the West as the dominant world power both economically and militarily.[12] This tone is in stark contrast to Deng's "24-Character Strategy" of the 1990s, which stated "observe calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership."[13] While China's overall goal to rise to prominence on the global stage has not changed from Deng's time to Xi's, the tone and aggressiveness at which economic, technological, and military goals are pursued have changed drastically.

Changes in policy and national law complemented this shift in tone beginning in 2016 with its Cybersecurity Law. Among numerous other changes and restrictions, this law mandates that all business firms that produce "important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China."[14] If the data is required to be transferred out of China for

business purposes, it must be examined and approved by Chinese authorities prior to release, opening the potential for widespread collection and theft of private data among companies operating in China.[15]

Additionally, China released the National Intelligence Law in 2017, which established an unprecedented level of cooperation between state agencies (such as the Ministry of State Security [MSS] and the PLA), private organizations, and people. Article 7 of the law opens private cooperation with state security, stating, "any organization or citizen cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public. The State protects individuals and organizations that support, assist and cooperate with national intelligence work."[16] Article 12 strikes a similar cooperative tone between state intelligence collection and private enterprise, stating, "the state intelligence work organization may, in accordance with relevant state regulations, establish cooperative relations with relevant individuals and organizations and entrust relevant work."[17]



WANTED BY THE FBI

YANQING YE

Acting as an Agent of a Foreign Government; Visa Fraud; Making False Statements; Conspiracy

DESCRIPTION

Date(s) of Birth Used: July 22, 1990	**Place of Birth:** Longhai, Fujian, China
Hair: Dark Brown	**Eyes:** Brown
Height: Approximately 5'4"	**Weight:** Approximately 110 pounds
Sex: Female	**Race:** Asian
Nationality: Chinese	**Languages:** English, Chinese

REMARKS

Ye is believed to be in China.

CAUTION

Yanqing Ye is a Lieutenant in the People's Liberation Army (PLA), the armed forces of the People's Republic of China, and a member of the Chinese Communist Party (CCP). Ye studied at the National University of Defense Technology (NUDT), a top military academy directed by the CCP in China. It is alleged that, on her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the NUDT. During Ye's time in the United States on her J-1 visa, she maintained close contact with her supervisor at the NUDT and other colleagues. While studying at Boston University's Department of Physics, Chemistry and Biomedical Engineering from October of 2017 to April of 2019, Ye allegedly continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing United States military websites, and sending United States documents and information to China.

On January 28, 2020, a federal arrest warrant was issued for Ye in the United States District Court for the District of Massachusetts, Boston, Massachusetts, after she was charged with acting as an agent of a foreign government, visa fraud, making false statements, and conspiracy.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Boston

Screenshot of an FBI wanted advisory for a suspected Chinese agent posted in 2020.

The shift in tone under Xi marks a transformation in an increasingly belligerent Chinese foreign policy economically, technologically, and militarily that has reflected the increased IP theft of U.S. technologies. Theft of IP directly complements the PLA's goal to modernize into a global power by the middle of the twenty-first century. The Information Office of the State Council outlined the future goals for the PLA in China's new global role in a 2015 white paper titled "China's Military Strategy." The white paper stated the PLA will "accelerate the modernization of national defense and armed forces … for achieving the national strategic goal of the 'two centenaries' and for realizing the Chinese Dream of achieving the great rejuvenation of the Chinese nation."[18]

Concurrent to military innovation, the Ministry of Industry and Information Technology (MIIT), under the leadership of Premier Li Keqiang, announced its "Made in China 2025" campaign in 2015. Made in China 2025 placed emphasis on emerging technology development, domestic innovation, and a shift from quantity-based production to quality-based production to enable China to become the leading innovative global manufacturer by 2049.[19] The overarching goal is to diminish Chinese reliance on foreign nations for advanced technology and quality goods by producing 70 percent of high-technology materials domestically by 2025.[20] According to a 2018 White House Office of Trade and Manufacturing Policy, Chinese foreign technology investment has been in line with those outlined in Made in China 2025.[21]

> "Chinese indigenous science and technology are not assessed to be advanced enough to independently compete with the U.S. and Western defense industrial base."

While experts argue Chinese SOE defense industries are attempting indigenous innovation and production, China still continues to struggle with critical technology development.[22] PLA modernization, therefore, still requires acquisition of sensitive technology and research and development, which is far more difficult to acquire through legal trade laws under the "indigenous innovation" program than other commercial technologies. Therefore, the CCP and the PLA rely heavily on illegal IP theft to acquire all or portions of critical technology to reverse engineer for domestically produced weapons.

Methods of Chinese IP Theft: Steal the Firewood from Under the Pot

The Thirty-Six Stratagems, a collection of proverbs believed to be from the Three Kingdoms Period of China, outlines a strategy for defeating a superior enemy: "Steal the firewood from under the pot."[23] This proverb outlines the indirect approach of removing the enemy's source of strength—in this case, the technological superiority of the U.S. and Western militaries. This method was summarized in the 2013 revision of *The Science of Military Strategy*, published by the Academy of Military Sciences of the PLA, which stated, "After the outbreak of the Gulf War, the Party Central Committee and the Central Military Commission foresaw that the war situation caused great changes had [*sic*] taken place, and the military's strategic policy of active defense has been adjusted in a timely manner, increasing the use of high technology."[24] The authors continue by outlining the future need for technological parity with or superiority over the West, stating, "The development of science and technology has opened the way forward for the evolution of the form of war."[25]

Under Hu in 2004 and currently under Xi, and highlighted in *The Science of Military Strategy*, the PLA has emphasized efforts on matching the West in high military technology.[26] However, as stated before, Chinese indigenous science and technology are not assessed to be advanced enough to independently compete with the U.S. and Western defense industrial base (DIB), necessitating the theft of current and developing technologies. To achieve this, China utilizes several means, both legal and illegal, for undermining U.S. and Western military technology, research and development, and DIB production methods. The *National Security Strategy* outlines the basic methods China uses to steal U.S. IP: "Rivals have used sophisticated means to weaken our businesses and our economy as facets of cyber-enabled economic warfare and other malicious activities. In addition to these illegal means, some actors use largely legitimate, legal transfers and relationships to gain access to fields, experts, and trusted foundries."[27] The four methods of Chinese IP theft are open source, commercial, academia, and cyber-enabled.

Method 1. Open Source

According to James Mulvenon, open-source collection and databasing of publicly available information is the key resource of science and technology

innovation, stating, "Innovation in China is driven by foreign developments, tracked through open sources."[28] Like all Chinese bureaucratic apparatuses, open-source collection structure is complex and redundant. Organizations such as the Institute of Scientific and Technical Information of China operate under the guise of innocuous databasing and cataloging but target publicly facing science and technology technical documentation for reverse engineering and domestic production, publicly available information on research organizations and their employees for targeting purposes by state intelligence, and incorrectly declassified or mistakenly released classified information.[29] While the system is run similarly to a library-based catalog, it is directed and run by Chinese intelligence experts working at the behest of the party, serving as a shortcut for Chinese industry to develop research and technology, and is cataloged and disseminated in coordination with either private or SOE developers and manufacturers.[30]

The open-source program has, as of 2013, extracted and cataloged over 4.7 billion titles and abstracts, 644 million full-text documents, 1.2 million conference papers, 1.8 million foreign science and technology reports, and 9.8 million microfilmed products.[31] This vast collection of nonclassified, unclassified, and improperly classified public and private information reduces cost, time, and risk to China's military and civil development. The open-source program has been so successful that former Institute of Scientific and Technical Information of China director He Defang boasted that due to open-source collection, "China's researchers reduced their costs by 40-50% and their time by 60-70%."[32]

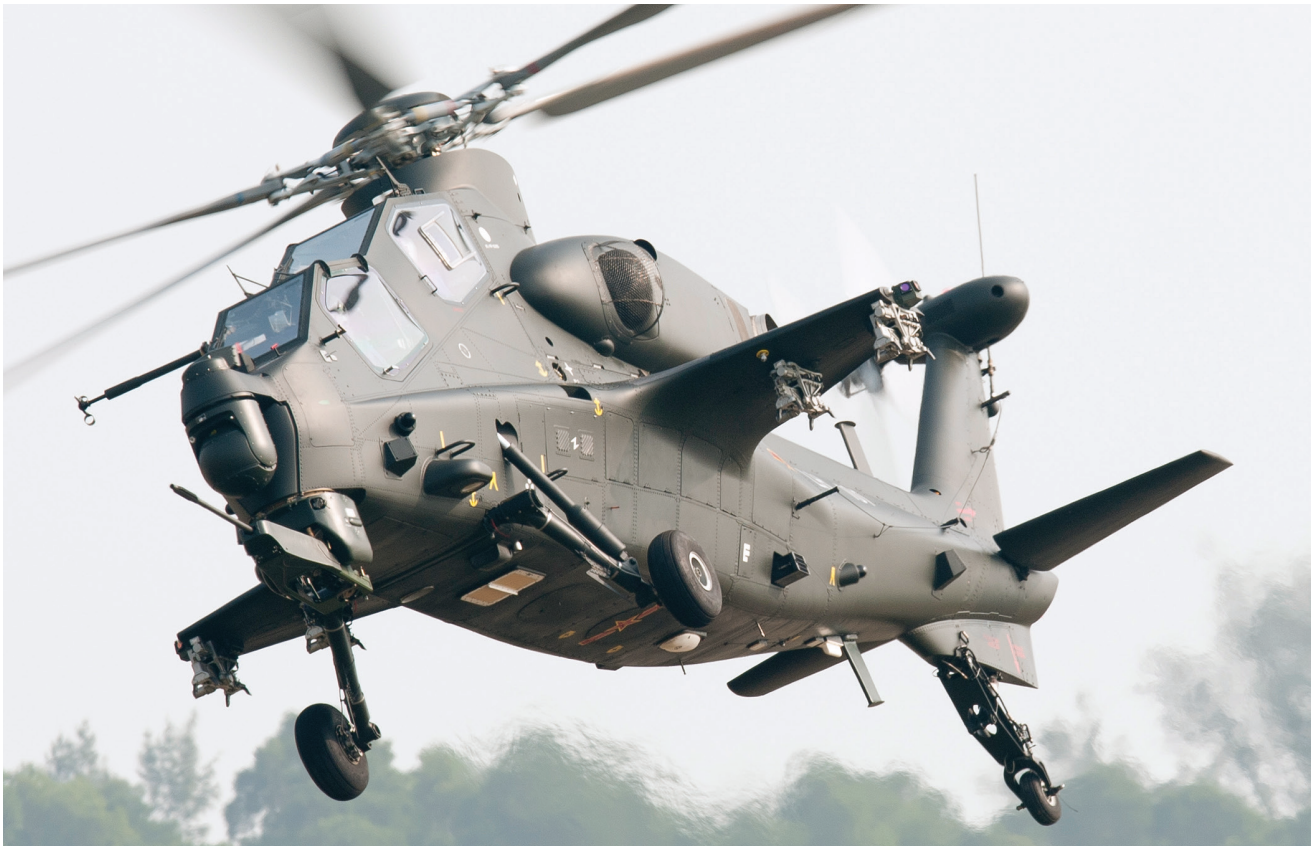
The implications of such a thorough and targeted collection of open-source information for the Army and DOD are profound. Public accountability and transparency in the United States and Western countries can be used to target military technology development and developers. For example, government contract awards posted almost daily on the DOD "Contracts" news page offer information on technology being developed, costs, contractors, subcontractors, contract lengths, locations, branches served, etc.[33] Additionally, contract awardee websites often provide information on organizational structure, personnel, locations of facilities, and nonclassified or unclassified information on research and development. This information, along with other information from countless other publicly facing government and privately owned websites, provide China with a clear picture of U.S. research and development priorities, long-term intentions, strategies, priorities for the force, and opportunities for collection via other means outlined below.

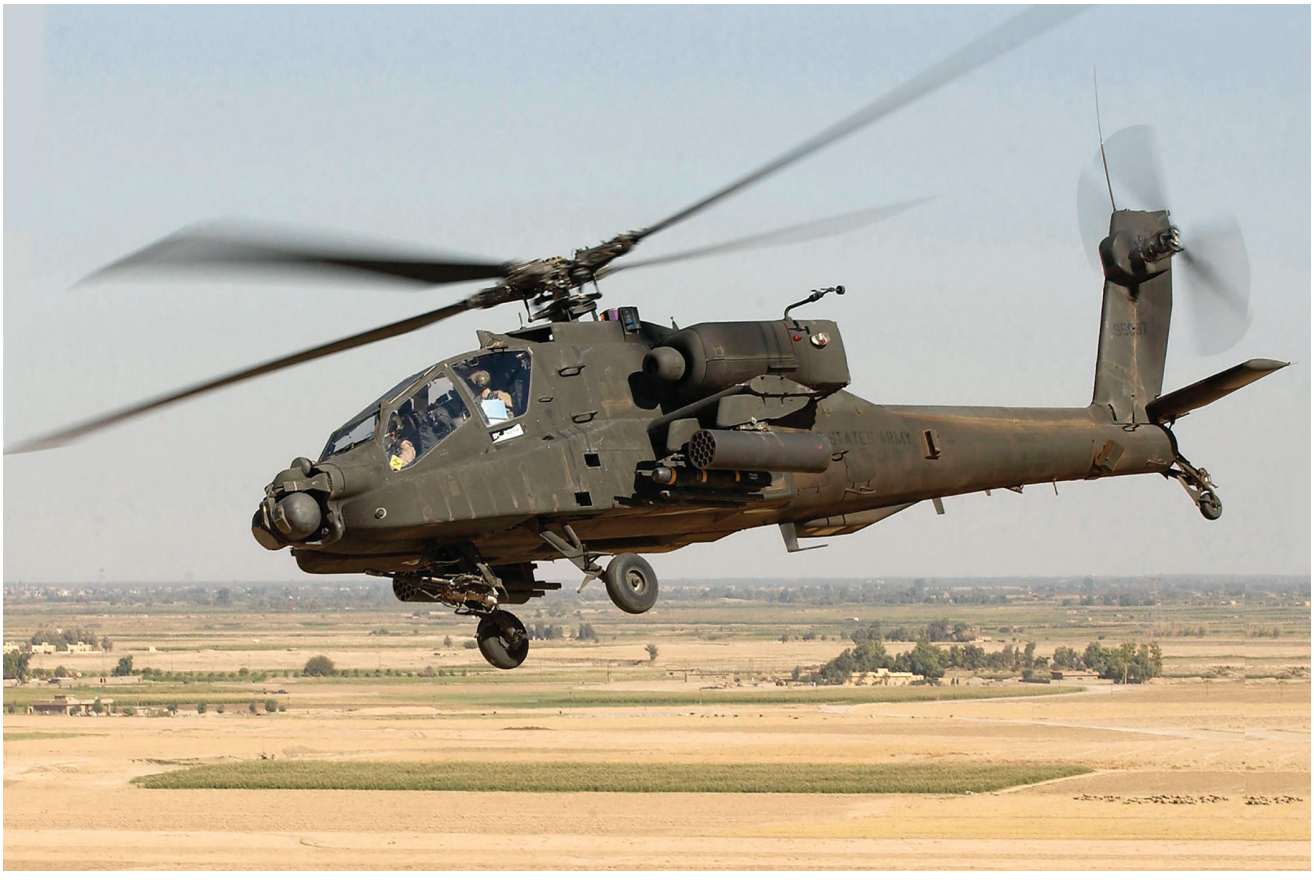
Method 2. Commercial

While China has moved from a Maoist communist nation during the Nixon administration to a mixed-market economy today, the distinction between private, public, and academia is far less profound than in the United States. Today, SOEs either directly or indirectly owned or funded by the CCP or the PLA constitute an estimated 23 to 28 percent of China's gross domestic product (GDP).[34] Some SOEs and private companies within China work either at the behest or on behalf of the CCP or PLA, either directly or indirectly, to target and acquire U.S. technology for import, reverse engineering, and domestic production that supports CCP or PLA research and development goals.[35] Subcontracts awarded to Chinese companies by prime contractors to U.S. government contracts offer insight into production methods and the capacity and capability to compile and reverse engineer technology to domestically produce high-end technology.

SOEs are linked to U.S. and other Western companies by the China Association for Science and Technology through national technology transfer centers. These centers establish cooperative relationships with American corporations and academic institutes to encourage technology transfers.[36] The CCP and the PLA fund SOEs to employ U.S. and Western science and technology experts, who account for about half of the 440,000 foreigners who currently work in China.[37]

Next page: A variety of Chinese fixed-wing and rotary-wing military aircraft appear uncannily similar in design to those developed by the United States and other countries, including many made by Russia. For example, the Chinese Z-10 helicopter (*above*), which closely resembles the U.S. AH-64 Apache helicopter (*below*) is thought to have been developed from information obtained by a combination of espionage, computer hacking, and transfer of classified trade-secret information through misleading deals with legitimate companies working under the presumption of cooperation with China to develop a "dual use" helicopter. (Photos courtesy of Wikipedia)





Other state-run programs such as 863 Program, funded and run by the Ministry of Science and Technology to develop and acquire high-level technologies, have been implicated in committing espionage, such as the 2011 conviction of Kexue Huang for stealing trade secrets from AgroSciences and Cargill Inc.[38]

As outlined in Made in China 2025, China has shifted industrial focus from cheap, low-quality goods to high quality, technologically driven innovation.[39] To accomplish this, China has shifted government-backed funding from acquiring "core natural resources" prior to the release of the policy to "acquire high-technology areas of the U.S. economy in particular."[40] China utilizes SOEs, private Chinese companies with ties to the Chinese government, and state-backed investment funds to conduct mergers, acquisitions, investment, and venture funding to acquire U.S. high technology.[41] These practices consist of legal, illicit, or sometimes illegal means to solicit, coerce, or outright steal information and technology from U.S. and other nations' private companies. According to an FBI report on China-related prosecutions since 2018, "about 80 percent of all economic espionage prosecutions brought by the U.S. Department of Justice (DOJ) allege conduct that would benefit the Chinese state, and there is at least some nexus to China is around 60 percent of all trade secret theft cases."[42]

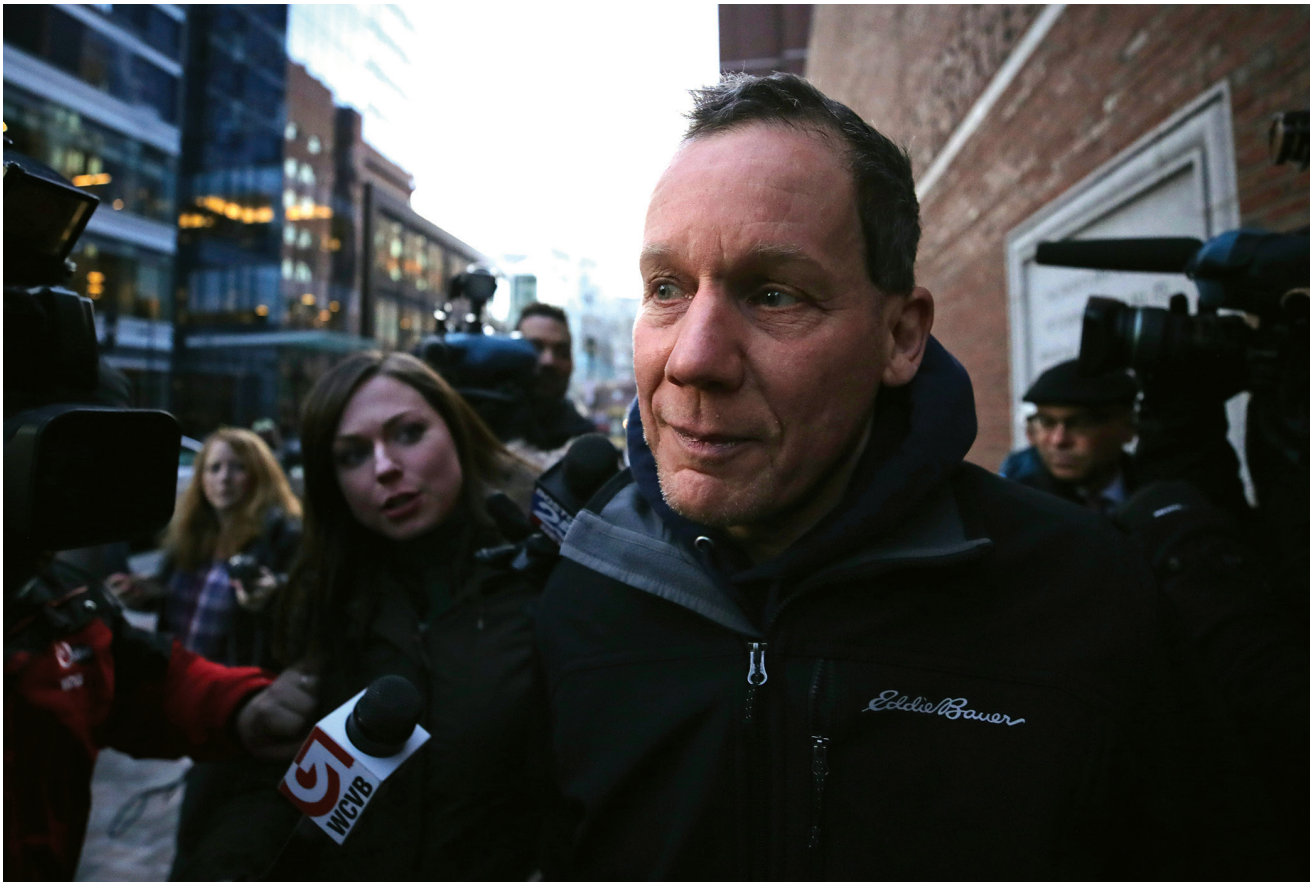
Additionally, Chinese companies, to include SOEs, have inserted themselves into U.S. military supply chains, typically at low-level subcontracts, and produced and sold illegal and substandard counterfeit parts to the United States.[43] Recent examples include component parts to the C-130J transport aircraft, the C-27J transport aircraft, the SH-60B multimission Navy helicopter, the Terminal High Altitude Area Defense (THAAD) missile defense system, and the P-8A Poseidon multimission maritime aircraft.[44] As the U.S. military increasingly relies on commercial off-the-shelf information technology equipment, the risk of Chinese companies producing compromised components is compounded, as evidenced by a 2018 Bloomberg report highlighting Chinese efforts to utilize commercial microchips to infiltrate and establish a backdoor into information technology equipment sold to government agencies.[45] Concerns over this issue are so high that in 2018, U.S. President Donald Trump signed a bill banning Huawei and ZTE (major providers of cellular phones to military service members overseas) technology in government contracts.[46]

Seal of the Thousand Talents Program

Method 3. Academia

In addition to open-source and commercial IP theft, China has employed academics to commit IP theft since the outset of Deng's "four modernizations."[47] Starting in 1978 under Deng, China shifted to a more pragmatic approach to modernizing China by sending increasing numbers of students and scientists abroad to learn from Western nations (something that was deemed dangerous under Mao after the Cultural Revolution) as well as attracting foreign talent into China.[48] China's approach to acquiring IP through academia has two distinct approaches: through open and established government-sponsored organizations and through overt and covert use of student populations and professors abroad to illegally acquire IP. Both of these methods effectually turn students and professors into state-sponsored collectors of IP at the direction of the CCP or the PLA.

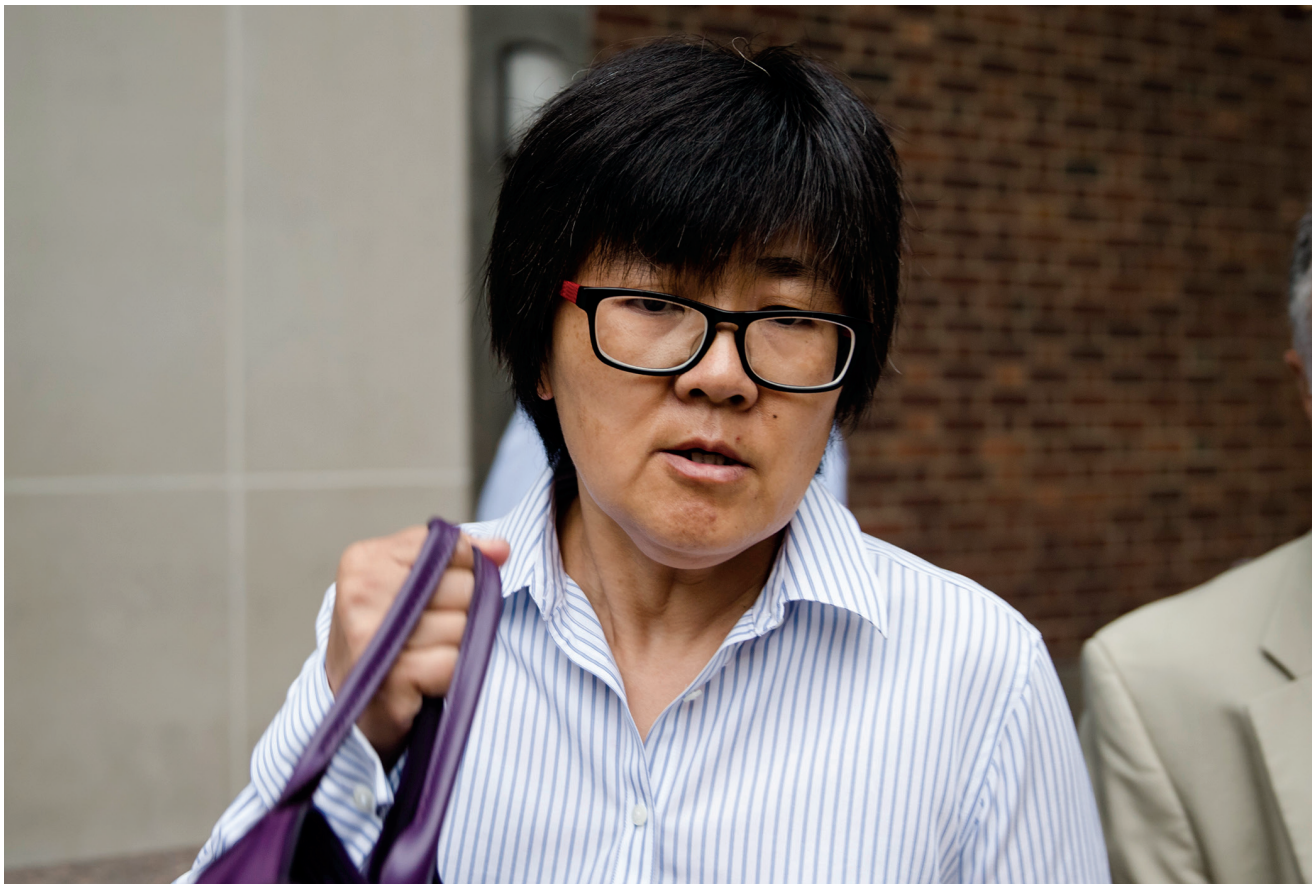
In the wake of 1989 Democracy Movement, culminating in the Tiananmen Square Massacre, the CCP sought to target domestic and overseas Chinese students to ensure party loyalty. To achieve this, the CCP expanded the existing Chinese Students and Scholarship Associations (CSSAs) abroad to ensure overseas student loyalty to CCP ideology. Additionally, in 2004, the CCP founded the first Confucius Institute, whose stated purpose is to "teach Chinese language, culture, and history at the primary, secondary, and university level around the world."[49] Currently, China operates over 140 CSSAs and 110 Confucius Institutes, all under the direction of the CCP United Front Work Department.[50] According to the 2018 U.S.-China Economic and Security Review



Harvard University Professor Charles Lieber is surrounded by reporters 30 January 2020 as he leaves the John Joseph Moakley U.S. Courthouse in Boston. Lieber, chair of the Department of Chemistry and Chemical Biology, was charged with lying to officials about his involvement with a Chinese government-run recruitment program through which he received tens of thousands of dollars. (Photo by Charles Krupa, Associated Press)

Commission, in reality, CSSAs "receive guidance from the CCP through Chinese embassies and consulates … and are active in carrying out overseas Chinese work consistent with Beijing's United Front strategy."[51] Likewise, Confucius Institutes have been accused of "improper influence over teaching and research, industrial and military espionage, surveillance of Chinese abroad and undermining Taiwanese influence as part of the reunification plan."[52] Both organizations serve to ensure Chinese student populations overseas are acting in accordance with CCP and PLA guidance and wishes.

The Thousand Talents Program, established in 2008 to both recruit non-Chinese scientists and entice foreign-educated Chinese individuals to return to the mainland, has come under open criticism by U.S. agencies for committing IP theft. In 2018, the assistant director of the Counterintelligence Division for the Federal Bureau of Investigation (FBI) stated that the Thousand Talents Program and other similar government-sponsored programs "offer competitive salaries, state-of-the-art research facilities, and honorific titles, luring both Chinese overseas talent and foreign experts alike to bring their knowledge and experience to China, even if that means stealing proprietary information or violating export controls to do so."[53] In January 2020, Charles Lieber, the chair of Harvard University's Chemistry and Chemical Biology Department, was indicted for accepting payment and living expenses from the Wuhan University of Technology after accepting a research grant from the DOD and falsifying statements regarding his participation in the Thousand Talents Program.[54] The Thousand Talents Program and other similar financially enticing programs allow China to capitalize on foreign education systems and technology development by cheaply, and often illegally, enticing scientists and researchers working on sensitive and controlled technologies to transfer foreign IP to China.



Yu Xue exits the federal courthouse 31 August 2018 in Philadelphia. Xue, a cancer researcher, pleaded guilty to conspiring to steal biopharmaceutical trade secrets from GlaxoSmithKline in what prosecutors said was a scheme to set up companies in China to market them. (Photo by Matt Rourke, Associated Press)

In addition to government-sponsored organizations, China has been accused of viewing all Chinese students as potential conduits for foreign technology transfer. Chinese organizations have openly advocated "expanding the role of Chinese scientists living overseas in conducting research on behalf of Chinese research institutes and facilitating technology transfer."[55] Returning overseas Chinese students are often debriefed by government officials on what technologies, research, and scientific personnel they had access to as part of general intelligence collection and to assess the potential to co-opt or recruit students. Additionally, China's MSS has been accused of approaching Chinese students and scientists who are preparing to travel overseas to task them with acquiring information or "performing other operational activity" while abroad, such as establishing covert relationships with academic personnel.[56] The use of overseas Chinese students and professors as collectors of IP poses a major challenge to the openness and transparency of academic institutions outside of China, which must contend with balancing protecting IP and promoting scientific research sharing and collaboration.

Method 4. Cyber Enabled

China uses cyber means to conduct IP theft, both directly through network intrusions and data theft or indirectly through other means such as open-source collection or in support of traditional espionage.[57] Cyber ties the previously discussed methods together because it provides a cheap and easy medium to conduct IP theft in a low-risk environment with relatively little repercussion for actions that would otherwise have major implications such as economic sanctions, arrests, and expulsion of state actors (known persona non grata in international diplomacy) if conducted on foreign soil.

IP theft via network intrusions and extraction of data from the DIB, subcontractors, academia, and government networks offers a cheap, reliable, and low-risk means of acquiring both developing and existing

sensitive military technology for reverse engineering and domestic production in China. According to the 2019 DOD annual report to Congress, "China uses its cyber capabilities to not only support intelligence collection … but also to exfiltrate sensitive information from the DIB to gain military advantage. The information targeted can benefit China's defense high-technology industry [and] support China's military modernization."[58] The report goes on to highlight the severity of the issue, stating, "These cyber-enabled campaigns threaten to erode U.S. military advantages and imperil the infrastructure and prosperity on which those advantages rely."[59]

According to a 2013 report by Verizon, 96 percent of all cyber espionage data breach cases were attributed to threat actors in China.[60] China utilizes state, business, and private cyber actors to compromise and steal $180 billion to $540 billion of IP and trade secrets annually, or 1 to 3 percent of the U.S. GDP.[61] Gen. Keith Alexander, then director of the National Security Agency and then commander of U.S. Cyber Command, stated in 2012, "In my opinion, it's [cyber-enabled intellectual property theft] the greatest transfer of wealth in history."[62]

In 2014, the U.S. Department of Justice charged five PLA officers from Unit 61398, 3PLA, with, among other charges, "economic espionage" and "accessing (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain."[63] This occasion became an historic first instance of state foreign actors charged with infiltration of U.S. commercial targets via cyber espionage.[64] In an attempt to embarrass and deter future actions by Chinese actors, the grand jury charges represented an open and public acknowledgment by the U.S. government of Chinese state actors actively and aggressively targeting critical military technology. Despite the charges, however, the ramifications and retaliation by the U.S. government remained targeted on specific individuals and highlighted the low-risk and high-reward nature of cyber espionage.

The apex of Chinese cyber activity volume was highlighted in 2013, as FireEye, a private cybersecurity firm, identified a marked decrease in Chinese cyber espionage incidents in the following years. While this was due in large part to the 2014 grand jury warrant and the 2015 U.S.-China Cyber Agreement in principle, FireEye also attributed the decrease to a professionalization and reorganization of Chinese cyber actors.[65] According to Elsa Kania and John Costello, the reduction in quantity of attacks coincides with the reorganization of Chinese cyber assets under the PLA Strategic Support Force, which centralized PLA cyber as a separate service branch under a single command and shifted focus toward a combat-oriented cyber focus. Additionally, the MSS appears to have taken the lead on commercial cyber espionage and directing nonstate actors in focused attacks on U.S. commercial interests.[66] According to a 2016 annual report to Congress, Chinese cyber activity at large has moved away from large-scale amateurish attacks such as those conducted under the PLA prior to 2014 to a more centralized and professionalized force, implying Chinese cyber espionage will be more difficult to detect in the future as the MSS and other Chinese intelligence agencies, instead of the PLA, target vulnerable commercial networks.[67] Rather than the decline in Chinese cyber espionage incidents representing a success in U.S. policy, it actually highlights a potential increase in Chinese cyber actor capabilities and a decrease in U.S. ability to detect threats.

In addition to direct network intrusion and IP theft, China utilizes information networks to target individuals online for carrying out more traditional means of IP theft mentioned previously. Chinese state intelligence actors used LinkedIn to target and clandestinely recruit a former Central Intelligence Agency and Defense Intelligence Agency employee, and the U.S. Department of Justice charged a Chinese intelligence agent in October 2018 for recruiting a General Electric Aviation engineer with whom they made initial contact on LinkedIn.[68] Profiles containing work history, degrees, and areas of expertise offer lucrative targeting information for Chinese agents seeking to acquire IP from specific technology sectors.

Cyber-enabled IP theft, like all other methods of Chinese IP theft, covers a wide spectrum of means and methods and overlaps with the aforementioned traditional methods of IP theft. Cyber-enabled IP theft stands out among other methods due to the volume and ease with which it can be carried out. However, it is worth noting that raw technical data carries little value without the methods, means, and technical expertise required to reverse engineer and domestically produce technology within China, which is achieved primarily through commercial and academic IP theft.

Mitigating Chinese IP Theft: Stemming the Tide

While internal policies and procedures within the Army and DOD may mitigate some IP theft, IP theft covers a wide spectrum across government, private, and academia, and thus the issue cannot be solved by the Army or the DOD alone. To mitigate and prevent IP theft, the DOD must strengthen existing government, private, and academic partnerships, committees, and policies. First, existing government policies, organizations, and authorities can be leveraged to combat IP theft of military technology. However, the Army and DOD must leverage the private sector and amend its contracting policies and regulations to mitigate theft by enforcing stricter information protection standards on contractors and subcontractors. Additionally, the Army and DOD must partner with academic institutes conducting research on critical technology to protect both classified and nonclassified developing or emerging technologies.

> "China utilizes state, business, and private cyber actors to compromise and steal $180 billion to $540 billion of intellectual property and trade secrets annually, or 1 to 3 percent of the U.S. gross domestic product."

Within the federal government, a comprehensive approach must be analyzed to prioritize critical high technologies. A technology that has a shorter lifecycle before becoming obsolete is less critical to defend than a technology that will remain relevant for decades with no foreseeable replacement. Furthermore, the DOD and other government agencies must ensure protection of technologies from "cradle-to-grave," a term used to describe protection of critical technologies from the time of their inception through their fielding, lifecycle, and eventual replacement by new technology. By only defending developing technologies, the DOD risks merely delaying eventual theft of technology and domestic production by adversaries.

Additionally, the DOD and federal government at large must leverage existing policies and organizations to strengthen protection of private sector IP. Two examples include the Committee on Foreign Investment in the United States, which can review foreign acquisitions and mergers of critical U.S. technology; and the National Industrial Security Program, which established policy via DOD 5220.22-M, a DOD operating manual that outlines procedures for private companies working on classified government contracts.[69] By leveraging committees like the Committee on Foreign Investment in the United States, the DOD could address concerns over mergers or acquisitions of high-technology contract or subcontract companies by Chinese companies with direct or indirect ties to the CCP or PLA. Existing policies such as DOD 5220.22-M, Federal Acquisition Regulation, and the Defense Federal Acquisition Regulation Supplement (DFARS) provide frameworks upon which to improve security practices by the private sector and strengthen regulation on subcontractor access to critical and developing technology.[70] By leveraging authorities from external agencies and departments such as the FBI, the Department of Treasury, or the Department of State, the Army and DOD impose regulatory, financial, or criminal action on noncompliant companies within the United States and exert international pressure through international regulatory bodies.

Currently, any university with a federal defense contract working on controlled unclassified information under DFARS 525.204.7012 must comply with National Institute of Standards and Technology (NIST) Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* to protect controlled unclassified information.[71] DFARS 252.204.7012 established regulatory compliance with NIST 800-171 standards for all contracts awarded after 1 October 2017. However, enforcement of DFARS 252.204.7012 primarily relies on contractor notification to the DOD chief information officer of any deficiencies in complying with NIST 800-171, not on inspections or regulatory checks by any enforcing body. Furthermore, subcontractors are only required to report deficiencies in complying with NIST 800-171

to the prime contractor and not to the federal government, risking that subcontractor compliance on controlled unclassified information is deficient.[72] This reliance on self-reporting by contractors and subcontractors promotes ignoring deficiencies in required federal regulatory guidance and puts companies and the DOD at risk of vulnerable critical technology of information systems. Amending federal regulatory guidance for universities, contractors, and subcontractors working on controlled unclassified information to permit federal regulatory inspections and checks on company compliance would protect against IP theft.

The 2019 addition to DFARS 252.204-7018, which prohibited contractor or subcontractor sales to the U.S. government of end items or components produced by Huawei and ZTE or any subsidiary thereof, established a precedent for enacting regulatory action against IP theft. Additionally, DFARS 252.204-7018 requires prime contractors to include the clause in "subcontracts for the acquisition of commercial items" to prevent prohibited sales of Huawei and ZTE equipment to contractors via subcontracts.[73] Utilizing similar actions against known CCP or PLA SOEs could serve as a deterrent against SOE willingness to engage in IP theft.

No one approach or method will counteract Chinese IP theft of critical military technology. However, by partnering with other federal and state agencies and departments, private companies, and universities, as well as enacting stricter regulatory guidance and enforcement tools, the Army and DOD would more effectively prevent IP theft and retaliate against thefts after they occur. Through a public-private approach, it may be possible to deter IP theft through a combination of prevention, incentives, and retaliation, which make illegal IP theft financially unsustainable.

Conclusion

The implications of Chinese IP theft are readily apparent in the CCP and the PLA's actions, official statements, and doctrine. While the methods and techniques used to conduct IP theft are not unique to the CCP, the scope and frequency of the theft are. Despite the 2015 Agreement in Principle and subsequent retaliatory actions by the U.S. federal government, China has shown little propensity for stemming its IP theft of high technology. IP theft combined with increased military spending by China threatens to close the gap with U.S. military technological superiority and challenge American military dominance. While China may not be able to produce superior quality high-technology weapons and systems for many decades, the threat of parity in even few military high technology areas threatens overall U.S. superiority on the battlefield and leads to a diminished status on the world stage.

The challenges presented by Chinese IP theft are numerous and may require the Army and DOD to step outside their normal operating environment to counter the threat and work with agencies, departments, and partners that are not frequently associated with military action. While isolated incidents of IP theft may appear inconsequential in the present, the consequences of not taking action potentially threaten future lives on the battlefield and U.S. military dominance. Only through proactively preventing Chinese IP theft can the Army and DOD protect their technological dominance and the future of U.S. military superiority. ■

Notes

1. Barack Obama, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," The White House, 25 September 2015, accessed 13 May 2020, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

2. The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), 21, accessed 14 May 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

3. 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* (Seattle: National Bureau of Asian Research, February 2017), 1, accessed 14 May 2020, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf; Commission on the Theft of American Intellectual Property, *The IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (Seattle: National Bureau of Asian Research, May 2013), 3, accessed 12 June 2020, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

4. Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 2017), 1-1–1-2.

5. Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era" (speech, 19th National Congress of the Communist Party of China, Beijing, 10 October 2017), 25, accessed 16 June 2020, http://www.xinhuanet.

com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.

6. William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (New York: Routledge, 2013), 12.

7. Select Comm. on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, H. Rep. No. 105-851, at x–xi (1999), accessed 14 May 2020, https://www.govinfo.gov/content/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf.

8. Ibid., 20–21.

9. James McGregor, *China's Drive for "Indigenous Innovation": A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, 2010), 2–5, accessed 14 May 2020, https://www.uschamber.com/report/china%E2%80%99s-drive-indigenous-innovation-web-industrial-policies.

10. Ibid., 4.

11. Ibid., 5.

12. Xi, "Secure a Decisive Victory," 25.

13. Chuang Meng, "Deng Puts Forward New 12-Character Guiding Principle for Internal and Foreign Policies," *Ching Pao*, no. 172 (1991): 84–86, cited in Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2006* (Washington, DC: Department of Defense [DOD], 2007), 7, accessed 14 May 2020, https://fas.org/nuke/guide/china/dod-2006.pdf.

14. Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]," *Cybersecurity Initiative* (blog), New America, 29 June 2018, accessed 14 May 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

15. Ministry of Foreign Affairs and Trade and New Zealand Trade and Enterprise, "Understanding China's Cybersecurity Law: Information for New Zealand Businesses" (Wellington, NZ: National Cyber Security Centre, September 2017), accessed 14 May 2020, https://www.ncsc.govt.nz/assets/NCSC-Documents/Understanding-Chinas-cybersecurity-law.pdf.

16. National Intelligence Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., 27 June 2017, effective 28 June 2017), art. 7, accessed 16 June 2020, https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

17. Ibid., art. 12.

18. Information Office of the State Council, "China's Military Strategy (full text)" (Beijing: The State Council, 27 May 2015), accessed 14 May 2020, http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm. The "two centenaries" is a policy implemented under President Xi Jinping referring to the centenary of the founding of the Communist Party of China in 2021, at which time the Chinese will establish a large economic base and middle class, and the founding of the People's Republic of China in 2049, at which time China will become a "strong, democratic, civilized, harmonious, and modern socialist country." This generally refers to the restoration of China as the preeminent power in the world.

19. Information Office of the State Council, "'Made in China 2025' Plan Issued," The State Council, 19 May 2015, accessed 14 May 2020, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

20. "Notice of the State Council on Printing and Distributing 'Made in China 2025,'" The State Council, 8 May 2015, accessed 14 May 2020, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

21. White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World* (Washington, DC: The White House, June 2018), 16, accessed 14 May 2020, https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

22. Meia Nouwens and Helena Legarda, "China's Pursuit of Advanced Dual-Use Technologies," International Institute for Strategic Studies, 18 December 2018, accessed 10 March 2020, https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance; Mike Yeo, "China's Military Capabilities are Booming, but Does Its Defense Industry Mirror That Trend?," Defense News, 14 August 2018, accessed 10 March 2020, https://www.defensenews.com/top-100/2018/08/14/chinas-military-capabilities-are-booming-but-does-its-defense-industry-mirror-that-trend/.

23. Stefan H. Verstappen, *The Thirty-Six Strategies of Ancient China* (San Francisco: China Books and Periodicals, 1999), 91–95.

24. Shou Xiaoson, ed., *The Science of Military Strategy*, trans. Chinese Academy of Military Science (Beijing: Military Science Press, 2013), 17.

25. Ibid., 3

26. Ibid., 247–48.

27. The White House, *National Security Strategy*, 21.

28. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 25.

29. Ibid., 23–28.

30. Ibid., 24.

31. Ibid.

32. Defang He, "As for Indigenous Innovation, Information Should Go Ahead of Rest," *China Information Review* 10 (2006): 12-13, quoted in Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 38.

33. "Contracts," DOD, accessed 15 May 2020, https://DOD.defense.gov/News/Contracts/.

34. Chunlin Zhang, *How Much do State-Owned Enterprises Contribute to China's GDP and Employment* (Washington, DC: World Bank, 15 July 2019), 10, accessed 15 May 2020, http://documents.worldbank.org/curated/en/449701565248091726/pdf/How-Much-Do-State-Owned-Enterprises-Contribute-to-China-s-GDP-and-Employment.pdf.

35. Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, 17–19.

36. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 93–94, 111.

37. Ibid., 79–80, 95.

38. "National High-tech R&D Program (863 Program)," Ministry of Science and Technology of the People's Republic of China, accessed 15 May 2020, http://en.most.gov.cn/eng/programmes1/200610/t20061009_36225.htm; "Chinese Scientist Huang Kexue Jailed for Trade Theft," BBC News, 22 December 2011, accessed 15 May 2020, https://www.bbc.com/news/business-16297237.

39. "Made in China 2025," The State Council, 8 May 2015, accessed 15 May 2020, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

40. Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, 16.

41. Ibid., 17–20.

42. "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018,"

U.S. Department of Justice, accessed 15 June 2020, https://www.justice.gov/opa/page/file/1223496/download.

43. Senate Comm. on Armed Services, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, S. Rep. No. 112-167, at vi–viii (2012), accessed 15 May 2020, https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf.

44. Ibid., ii–iv.

45. Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," Bloomberg Businessweek, 4 October 2018, accessed 15 May 2020, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

46. Jacob Kastrenakes, "Trump Signs Bill Banning Government Use of Huawei and ZTE Tech," The Verge, 13 August 2018, accessed 15 May 2020, https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump.

47. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 12.

48. Ibid., 136–37.

49. Alexander Bowe, *China's Overseas United Front Work: Background and Implications for the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, 2018), 12, accessed 10 June 2020, https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf.

50. Ibid., 10, 12.

51. Ibid., 10.

52. Michael Barr, *Who's Afraid of China?: The Challenge of Chinese Soft Power* (London: Zed Books, 2011), 67.

53. *China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses, Before the Senate Judicary Committee*, 115th Cong. (2018) (statement of E. W. "Bill" Priestap, Assistant Director of Counterintelligence Division, Federal Bureau of Investigation), accessed 18 May 2020, https://www.fbi.gov/news/testimony/chinas-non-traditional-espionage-against-the-united-states.

54. U.S. Department of Justice, "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," news release no. 20-99, 28 January 2020, accessed 15 June 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

55. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 156–57.

56. Ibid., 157.

57. Ibid., 188.

58. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: DOD, 2019), 65, accessed 18 May 2020, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

59. Ibid.

60. Verizon RISK Team, *2013 Data Breach Investigations Report* (New York: Verizon, 2013), 21, accessed 18 May 2020, https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/data-breach-investigations-report-2013.pdf.

61. National Bureau of Asian Research, *Update to the IP Commission Report*, 11.

62. "Gen. Alexander: Greatest Transfer of Wealth in History," YouTube video, posted by "American Enterprise Institute," 9 July 2012, 1:27, accessed 18 May 2020, https://www.youtube.com/watch?v=JOFk44yy6IQ.

63. U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," news release no. 14-528, 19 May 2014, accessed 18 May 2020, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

64. Ibid.

65. FireEye iSight Intelligence, *Red Line Drawn: China Recalculates its Use of Cyber Espionage* (Milpitas, CA: FireEye, June 2016), 3 and 15, accessed 18 May 2020, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

66. Elsa Kania and John Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3, no. 1 (Spring 2018): 106–7.

67. U.S.-China Economic and Security Review Commission, *2016 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: U.S. Government Publishing Office, 2016), 57, accessed 10 June 2020, https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf.

68. Edward Wong, "How China Uses LinkedIn to Recruit Spies Abroad," *New York Times* (website), 27 August 2019, accessed 18 May 2020, https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.

69. DOD 5220.22-M, *National Industrial Security Program Operating Manual* (Washington, DC: DOD, 2006, incorporating change 2, 18 May 2016), accessed 18 May 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODm/522022M.pdf.

70. Ibid.; "FAR [Federal Acquisition Regulation]," Acquisition.gov, last updated 15 May 2020, accessed 18 May 2020, https://www.acquisition.gov/browse/index/far; "Defense Federal Acquisition Regulation Supplement [DFARS]," Acquisition.gov, last updated 18 May 2020, accessed 18 May 2020, https://www.acquisition.gov/dfars.

71. Ron Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171, rev. 2 (Gaithersburg, MD: National Institute of Standards and Technology, February 2020), accessed 18 May 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

72. "DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)," Office of the Under Secretary of Defense for Acquisition, 31 December 2019, 252.204-7012(m)(2), accessed 10 March 2020, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

73. "DFARS 252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services (Dec 2019)," Office of the Under Secretary of Defense for Acquisition, 31 December 2019, 252.204-7018, accessed 18 May 2020, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7018.