The Heritage Foundation

CONGRESSIONAL TESTIMONY

"The PRC and Intelligence Gathering: Unconventional Targets and Unconventional Methods"

Testimony before Committee on the Judiciary

U.S. Senate

December 12, 2018

Dean Cheng
Senior Research Fellow
The Heritage Foundation

My name is Dean Cheng. I am a Senior Research Fellow at The Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

Since the founding of the People's Republic of China (PRC) in 1949, Chinese leaders have been intent on catching up with the West. This objective has, at times, led to catastrophic effects, such as the Great Leap Forward (1957–1960) when China experienced one of the worst famines of the 20th century, as it sought to achieve British levels of industrialization in less than a decade.

With the rise of Deng Xiaoping in 1978, China took a very different tack. Rather than ideologically driven campaigns that sought to overcome Chinese weaknesses in just a few years, Deng generally pursued a much more pragmatic line, under the rubric of "Reform and Opening." Communes and state ownership were replaced by a much greater reliance on the market for resource allocation and production decisions. At the same time, China lowered military spending, and made it clear that the People's Liberation Army (PLA) would have a far lower priority in access to national resources. Deng's policies laid the foundations for China's economic growth through the early 1990s.

Deng selected not only his immediate successor, Jiang Zemin, but also designated the *subsequent* successor, Hu Jintao. But while Jiang and his premier Zhu Rongji continued to push for Chinese economic liberalization in the 1990s, Hu and his premier Wen Jiabao first curtailed and then reversed Chinese economic reforms, beginning in the early 2000s. This shift in approach did not alter the overall Chinese goal, however, of catching up with, and eventually exceeding, the West. Indeed, with the promulgation of official programs such as "Made in China 2025," as well as various speeches by Chinese leaders such as Xi Jinping, it is very clear that Chinese leaders intend to establish China at the forefront of the world along many different metrics, including manufacturing, innovation, and military

capacity. The goal is to do this by 2049—the 100th anniversary of the founding of the PRC. This unswerving objective provides an essential context for understanding China's non-conventional approach to espionage. It is important to note here that "espionage" includes more than collecting military secrets. According to MI-5, "espionage is the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems). lt may also involve seeking to influence decision-makers and opinion-formers to benefit the interests of a foreign power."[1]

The PRC employs non-traditional means both for information collection and shaping foreign perceptions. Moreover, the PRC's intelligence-gathering efforts reflect both a very different approach to selecting intelligence *methods*, but also employing a different approach to *targets*. These two elements interact with each other, thereby posing a fundamentally different challenge to the targets of that espionage, including the United States.

Competing Across All Fields—Comprehensive National Power

If the PRC is intent upon catching up with the West, it is striving to do so along multiple lines of effort. This is because the Chinese leadership recognizes that in today's interconnected world, dominance in only one area or field is insufficient. Instead, the Chinese subscribe to the idea that nations are competing across a range of capabilities, embodied in the idea of "comprehensive national power (*zonghe guojia liliang*; 综合国家力量)."

Comprehensive national power (CNP) includes military power, but it goes beyond military and security forces and capabilities. Indeed, the experience of the Soviet Union serves as a cautionary tale that *over*-reliance on military elements of power can be as detrimental as insufficient capabilities. CNP therefore also includes economic power, which is seen as *potential* power, set against the actual power of military force. Without sufficient economic strength, military capability is brittle. Economic power, however, is also a key metric in its own right, and can also be used to influence, intimidate, and coerce others.

CNP also includes other elements, however. These include diplomatic influence and political unity. Without the former, states have limited ability to shape the international environment, including preventing the formation of an anti-China coalition. Without internal political unity, embodied within a powerful Chinese Communist Party (CCP), national resources (including human as well as industrial and financial) cannot be properly directed or mobilized.

The central place of the CCP, in this regard, is reinforced by its role as the "vanguard party," as set forth in Marxist-Leninist ideology. The CCP does not tolerate competition from alternative centers of political power (which might help coalesce resistance and dissent). Thus, there is no real room for civil society in the PRC, i.e., civic and social spaces that are beyond the reach of the CCP. This is why CNP also includes the component of "cultural security," which demands that the Chinese people be proud of their culture and political system.

Given this broad range of components incorporated within it, the Chinese leadership faces a major challenge to improve China's overall level of CNP. However, their task is simplified because of the extensive control of

[1]Security Service MI-5, Espionage, https://www.mi5.gov.uk/espionage (accessed December 10, 2018).

the CCP, and the Chinese government that it operates, over the entire nation.

"Market Socialism"—Facilitating Economic Competitiveness

Not only are the lines blurred between the government and civil society, but also between the state-run sector and the private sector (i.e., companies not run by the government). The CCP controls the careers of senior state-owned enterprise (SOE) managers, as well as the bureaucrats who oversee and coordinate them. Similarly, since there are Party committees even in non-SOEs, Beijing has an important means of monitoring developments in private companies. Coupled with government regulations, there is a pervasive CCP presence that ensures that even private companies cannot easily escape governmental directives, "suggestions," and general policy direction.

This is especially true in the realm of information and communications technology (ICT). Regarding ICT companies, as well as Internet Service Providers (ISPs) and telecommunications-related firms, the Chinese have enacted laws and regulations to make clear that companies in this area *must* cooperate with the state. Cybersecurity, for example, has become ever more explicitly linked to national security. Article 25 of the Chinese National Security Law, enacted in July 2015, specifies that one of the state's national security responsibilities is maintaining national network and information security, stopping "unlawful and criminal activity," including "dissemination of unlawful and harmful information," as well as "maintaining cyberspace sovereignty, security, and development interests." To this end, it is specifically noted that there will be national security reviews and oversight management of "Internet information technology products and services."[2]

Meanwhile, the Chinese cybersecurity law that came into effect on January 1, 2016, reinforces this. The legislation requires all telecommunications and Internet companies operating in the PRC to cooperate with Chinese law enforcement and security organizations in controlling information flow in defense of cyberspace sovereignty, as well as information network security and development efforts. The legislation requires such companies to provide "technical assistance," including the decryption of user data, in support of "counter-terrorist" activities.[3]

Governmental control is further facilitated by the reality that China's banking system is almost entirely state-owned as well. This has several effects. On the one hand, this means that certain companies, especially state-owned enterprises but also companies with links to key individuals within the CCP, "have long received credit disproportionately to their profitability" from state-run banks.[4] As a result, SOEs have access to essentially the financial resources of the state, whether to cover operating deficits or to obtain funding to acquire foreign technology and even foreign companies.

Conversely, it suggests that private Chinese companies may find their access to capital curtailed, should they refuse to cooperate with the Chinese government on any given issue. This, in turn, affects their ability to expand their business, develop new product lines, or otherwise improve. The idea that a Chinese

[2]"People's Republic of China National Security Law," *China Daily*, July 1, 2015, http://www.chinadaily.com.cn/hqcj/zgjj/2015-07-01/content_13912103.html (accessed December 10, 2018).

[3]Bruce Einhorn, "A Cybersecurity Law in China Squeezes Foreign Tech Companies," Bloomberg News, January 21, 2016), http://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies (accessed December 10, 2018).

[4]Robert Cull, Maria Soledad Martinez Peria, and Jeanne Verrier, "Bank Ownership: Trends and Implications," IMF Working Paper WP/17/60, p. 28.

company could refuse to cooperate with the PRC government, especially in matters of national security, as Google has with regards to Project Maven or Apple with the San Bernardino shooting incident, is therefore almost impossible to imagine.

For Chinese leaders, this hybrid structure is a feature. Chinese leaders have long described the PRC economy as a "socialist market economy," where the state sets broad policies and retains control of key parts of the economy, yet reaps the benefits and efficiencies of the market in resource allocation and demand signals. However, this outsize government role, which far exceeds that present in places like Western Europe, means that the PRC is not a market economy, an assessment reached by a variety of authorities including the EU and the International Monetary Fund. [5] China's companies, then, are not only economic entities, but also another part of the state, prepared to further PRC interests as well as generate profits. Similarly, the Chinese state can and will support Chinese companies in ways that go beyond subsidies and non-tariff barriers to aiding the acquisition of intellectual property, business plans, and other traditionally private corporate information.

At the same time, however, all Chinese companies, state-owned or not, are subject to government supervision and pressure. Therefore, those same companies can, and do, engage in information collection. China Aerospace Science and Technology Corporation (CASC) is one of the main SOEs involved in China's space program. Many of its subsidiary academies have research institutes dedicated to collecting information about foreign space programs and aerospace manufacturers. The information that this economic entity collects is presumably available to the entire government, including intelligence agencies and the PLA.

Political Warfare and Public Opinion Warfare—Influencing Global Perceptions

While economics play a central role in improving China's CNP, another element is improving China's international political standing. This entails the undertaking of not only traditional diplomacy, but also political warfare, and especially "public opinion warfare."

The Chinese conception of political warfare involves the use of information to undertake sustained attacks against the enemy's thinking and psychology, so as to eventually subvert their will. [6] Chinese leaders see themselves reacting to foreign pressures in this regard. From Beijing's perspective there is a constant threat of "westernization" and "splittism," reflected by Western calls for greater democratization and liberalization, which endangers the nation's political security and the Party's hold on power.

Although the tools for political warfare are mainly forms of strategic communications, including television, radio, the Internet, and news organizations, it is nonetheless seen *as a form of warfare*. It is envisioned as the use of information as a weapon to attack opponents, by eroding will, imposing psychological pressure, and influencing cognitive processes and the framework of perceptions. Because of

[5]Philip Blenkinsop, "EU Singles Out China as Distorted State-Run Economy," Reuters, December 20, 2017, https://www.reuters.com/article/us-eu-china-trade/eu-singles-out-china-as-distorted-state-run-economy-idUSKBN1EE1YY (accessed December 10, 2018), and Frank Tang, "Is China an Open Economy? Beijing Says It Is but IMF Differs," *South China Morning Post*, August 24, 2018, https://www.scmp.com/news/china/economy/article/2161265/china-open-economy-beijing-says-it-imf-differs (accessed December 10, 2018).

[6]YANG Chunchang, SHEN Hetai, Chief Editors, *Political Warfare/Operations Under Informationized Conditions* (Beijing, PRC: Long March Press, 2005), p. 15.

the informationized condition of the global economy, political warfare efforts are no longer limited to front-line military forces, but can now be applied against the adversary's population and leadership. It is the weaponization of soft power.

Similarly, because modern information technology blurs the lines between peacetime and wartime, between military and civilian, and among strategy, operations, and tactics, political warfare is not limited to when hostilities have formally commenced, and is not focused solely on military targets.[7] Instead, informationized warfare includes activities that are undertaken in peacetime, many of which are aimed at the adversary's political leadership and broad population. Informationized warfare, even more than Industrial-Era mechanized warfare, encompasses the entire society of both sides.

Chinese analysts see public-opinion warfare (*yulun zhan*; 舆论战) as the effort to shape an intended audience through the application of information derived and propagated by various types of mass information channels, including the Internet, television, radio, newspapers, movies, and other forms of media. In particular, it involves transmitting selected news and other materials with a consistent message to the intended audience in accordance with an overall plan, so as to guide and influence their public opinions towards views and conclusions that are beneficial to oneself and detrimental to the adversary. Public-opinion warfare is therefore also sometimes termed "media warfare" or "consensus warfare."

In many ways, both public-opinion warfare and legal warfare support psychological warfare. Public-opinion warfare, in particular, is a key means of influencing a variety of audiences, preparing them for the messages embodied in psychological warfare efforts.

Chinese analysts see public-opinion warfare as a special part of informationized warfare. Because of the wide permeation of information technology, public opinion warfare has global reach, extends to every part of society, and has an especially wide impact. The goal of public-opinion warfare is to shape public and decision-maker perceptions and opinion, so as to shift the perception of overall balance of strength between oneself and one's opponent.[8] To this end, it is especially important that communications efforts associated with public opinion warfare be mutually reconciled and coordinated, so that specific messages are clearly transmitted, in support of specific goals. While the news media plays an important role in the Chinese conception of public opinion warfare, it is only a subset of the larger set of means available for influencing public opinion.[9]

Successfully conducted public-opinion warfare will influence three audiences: the domestic population, the adversary's population and decision makers (both military and civilian), and neutral and third-party states and organizations. It will preserve friendly morale, generate support at home and abroad for oneself, weaken the enemy's will to fight, and alter the enemy's situational assessment. Public-opinion warfare is both a national and a local responsibility, and it will be undertaken

[7]YUAN Wenxian, *The Science of Military Information* (Beijing, PRC: National Defense University Publishing House, 2008), pp. 77–79.

[8]Academy of Military Sciences Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November, 2005), p. 405, and LIU Gaoping, *Study Volume on Public Opinion Warfare* (Beijing, PRC: NDU Publishing House, 2005), pp. 16–17.

[9]LIU Gaoping, *Study Volume on Public Opinion Warfare*, p. 5.

not only by the PLA's own assets, but through the People's Armed Police, national and local media, spokespeople, netizens, among others.[10]

Public-opinion warfare is an autonomous activity, in the sense that it can be undertaken independent of an actual, formal conflict; consequently, it is a central element of political warfare. According to Chinese analyses, the side that plants its message first enjoys a significant advantage influencing public opinion. Indeed, Chinese analyses of public-opinion warfare repeatedly emphasize that the "the first to sound grabs people, the first to enter establishes dominance (*xian sheng duoren, xianru weizhu*; 先声夺人， 先入为主)."

Essentially, the objective of public opinion warfare is to establish the terms of the debate and define the parameters of coverage. By presenting one's message first, the PLA expects to shape all others' views of a conflict. Thus, the Chinese side can underscore the justice and necessity of its operations, better display national strength, exhibit the superiority of its forces, and shake an opponent's will to resist. [11] By contrast, adversaries must overcome the ideas that are already planted and taking root by Chinese public-opinion warfare efforts. Therefore, in a very real way, Chinese decision makers see public-opinion warfare as being waged even in peacetime, as part of the larger effort to shape peoples' perceptions of the PRC. There is a constant effort to influence audiences to accept China's narrative and perceptual framework.

To maximize the effectiveness of public-opinion warfare, it is essential to exploit all possible channels of information dissemination, so that a given message is reiterated, reinforced by different sources and different versions. Public-opinion warfare efforts, then, will embody the ideals of "combining peacetime and wartime operations; civil-military integration of resources; military and local resources unified (*pingzhan jiehe, junmin jiehe, jundi yiti*; 平战结合, 军民结合, 军地一体)."

To successfully conduct public-opinion warfare requires careful preparation of the public opinion battleground in peacetime. That is, there must be extensive research into tactics and methods for undertaking public opinion warfare, understanding potential opponents' psychology and national moods, and the nurturing of public-opinion warfare specialists. This is not limited to the news media; in the Iran–Iraq War, for example, Chinese analysts note that Iran linked news-based propaganda with religious outlets. This helped bolster public morale, employing religious fervor in support of the state.[12] Such efforts, however, can only succeed with a thorough understanding of the target audience. For this reason, PLA writings consistently invoke the saying, "Before the troops and horses move, public opinion is already underway (*bingma weidong, yulun xianxing*; 兵马未动，舆论先行)," emphasizing that the preparation for public-opinion warfare must begin far in advance of the actual outbreak of hostilities.[13]

[10]The People's Armed Police are part of the Chinese armed forces, along with the PLA and the reserve forces.

[11]YAO Fei, "Some Thoughts Regarding Our Military's Anti-Secessionist Public Opinion and Propaganda Policies," *Military Correspondent* (PRC) No. 5 (2009), http://www.chinamil.com.cn/site1/jsjz/node_22972.htm (accessed December 10, 2018), and JI Chenjie, LIU Wei, "A Brief Discussion of Public Opinion Warfare on the Web," *Military Correspondent* (PRC) No. 1 (2009), http://www.chinamil.com.cn/site1/jsjz/2009-01/14/content_1619064.htm (accessed December 10, 2018).

[12]JI Peilin and JI Kaiyun, "The Iran-Iraq War and Psychological Warfare," *Journal of Shangluo University*, Vol. 28, No. 3 (June 2014), p. 31.

[13]Nanjing Political Academy Military News Department Study Group, "Study of the Journalistic

The PRC employs not only its news media to shape foreign perceptions, but also non-traditional methods such as tourists. When Beijing was displeased with South Korea's decision to deploy the Theater High Altitude Air Defense System (THAAD) for protection against North Korean missiles, one response was to ban Chinese tourism in South Korea. This apparently led to a $15.6 billion loss in revenue for the South Korean economy, and helped persuade South Korean president Moon Jae-in to adopt a much more conciliatory policy towards China. While the deployment of the THAAD battalion has been completed, Seoul has agreed to the "three nos":

1) No further THAAD deployments to South Korea,
2) No Republic of Korea participation in any regional missile defense network, and
3) No trilateral military alliance with the U.S. and Japan.[14]

In effect, Beijing has succeeded in creating "weaponized tourism."

Implications for Intelligence Gathering and Espionage

The intimate and extensive linkage among all aspects of China's economy and society with the instruments of the state and the CCP means that Chinese intelligence activities and resources can and will be employed to support improvements in Chinese CNP. This may be seen as non-traditional espionage *methods*, where academic, journalistic, and economic entities may engage in activities that are typically associated with state intelligence roles and missions.

At the same time, the Chinese security apparatus can call upon economic, social, and other elements to supplement information and intelligence gathering in ways that have no parallel in the West. This may be seen as non-traditional espionage *targets*, where state intelligence entities gather information about foreign companies, organizations, and people that have no obvious national security role.

Non-traditional Espionage Methods

Chinese concepts of national security are very broad and comprehensive. Consequently, ensuring national security requires comprehensively applying "political, economic, military, diplomatic, cultural, and propaganda techniques."[15] This means that the PRC's intelligence services can call upon a much broader range of organizations and entities to support and supplement governmental information collection. The latest edition of the *PLA Encyclopedia*, for example, specifically notes that military intelligence should coordinate with non-military intelligence, under a unified plan, when implementing strategic intelligence responsibilities.[16]

Because the PRC is not a market economy, government-industry relations work along very different lines. As noted previously, some SOEs even have information-gathering institutions and organizations, which likely operate not only akin to state intelligence services, but at their direction and certainly in

Media Warfare in the Iraq War," *China Military Science*, No. 4 (2003), p. 28.

[14]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 December 10, 2018).

[15]XIE Xiang, *National Security Strategy Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 111.

[16]Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, 2nd Edition, *Military Intelligence* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 27.

coordination. Thus, entities such as the China Great Wall Industries Corporation, which is a subsidiary of CASC, may have an information-collection function, even as they serve as the main point of contact for Chinese exports of satellites and launch services.

As important, it now appears that the Chinese are prepared to employ financial institutions and entities in pursuit of intelligence. A recent report on a company buying a Boeing satellite suggests that the Chinese sought to circumvent Committee on Foreign Investment in the United States (CFIUS) and International Trade in Arms Regulations (ITAR) restrictions and access a Boeing satellite. What is striking is that the Chinese apparently exploited their position on the board of an American company (Global IP) to access information that was perfectly legal for the company to possess. As important, they secured these positions on the board by providing financing to the American start-up. That funding, moreover, was channeled through an offshore company based in the British Virgin Islands, and was undertaken by a Hong Kong passport holder.[17] In essence, the Chinese employed a number of financial subterfuges to gain access to aerospace technology.

This intertwining is not just one way, however, with Chinese industry supporting Chinese military and intelligence organizations. Because of the comprehensive Chinese view of national security, as embodied in CNP, the military is also likely to help secure business information. The apparent employment of Chinese military units in economic cyber espionage likely reflects this comprehensive approach.

Indeed, in the realm of computer network operations, the PLA quite clearly expects to operate closely with non-military and even non-governmental forces. PLA cyber units appear to operate specifically in conjunction with other parts of the Chinese government, especially those parts responsible for various aspects of information security. These include the State Council's Ministry of Science and Technology, the State Secrecy Bureau, the Ministries of Public Security and State Security, and the National Cryptologic Management Center.[18]

This apparent integration of civilian and military efforts, at least in the realm of computer network operations, is supported by the observation in the 2013 edition of *The Science of Military Strategy* that there are three broad categories of Chinese computer network warfare forces. These are comprised of:

1) Specialized network warfare strength, which are specialized military units specifically tasked for implementing network offensive and defensive operations;
2) Authorized strength, which are specialist units organized with military permission, drawn from local capabilities (e.g., from within a military region or war zone), including the Ministry of State Security and the Ministry of Public Security, and other relevant government departments;
3) Civilian strength, comprised of voluntary civilian participants who can

[17]Brian Spengele and Kate O'Keeffe, "China Maneuvers to Snag Top Secret Boeing Satellite Technology," *Wall Street Journal*, December 4, 2018, https://www.wsj.com/articles/china-maneuvers-to-snag-top-secret-boeing-satellite-technology-1543943490 (accessed December 10, 2018).

[18]Mark Stokes and L. C. Russell Hsiao**,** *Countering Chinese Cyber Operations: Opportunities and Challenges for US Interests* (Arlington, VA: Project 2049, 2012), p. 4, http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf (accessed December 10, 2018).

> conduct network operations after being mobilized and organized.[19]

It should therefore not be a surprise that Chinese computer network operations should include military and non-military units and organizations, all targeting the same array of targets. The line separating military, government, and civilian roles in the PRC, at least in the realm of computer network operations, is almost certainly thin at best.

A recent study from professors at the U.S. Naval War College and Tel Aviv University outline how China has been redirecting entire portions of the Internet to transit through Chinese portals—and thereby provide an opportunity for the data to be copied on a wholesale basis. By exploiting the Border Gateway Protocol, a "Tier 1" Internet Service Provider, has the ability to redirect traffic. In this case, China Telecom, a Tier 1 provider with "points of presence" in the North American telecommunications backbone, has apparently exploited this role to redirect Internet traffic from North America to China.[20] Not surprisingly no American Tier 1 provider is allowed to operate in the PRC.

Non-traditional Espionage Targets

The same broad Chinese concepts of national security means that the PRC's intelligence effort will target a much broader range of organizations and entities, including businesses and non-governmental elements of civil society, as well as traditional military and security organizations.

Given the Chinese military's emphasis on establishing "information dominance" in order to fight and win future wars, a top priority for PLA espionage is military and security-related information. But this goes beyond traditional issues such as weapons blueprints, cryptographic keys, and war plans. The emphasis on both electronic warfare and network warfare (which encompasses cyber operations) means that the PLA will want to have insight into all aspects of adversary information and communications technology, including mapping out various networks. Indeed, the tasks of the newly established PLA Strategic Support Force (which encompasses electronic, network, and space warfare) give some indication of likely Chinese espionage priorities.

At the same time, Chinese security extends to broader areas of economic, scientific, and technological endeavor. Not surprisingly, Chinese military writings make clear that the PRC's intelligence community is expected to obtain not only traditional military and security secrets such as military plans and equipment designs, but also economic, industrial, and financial data. The PLA's volume on military terminology, for example, notes that "strategic intelligence" includes "military thought, strategic guidelines, war plans," but also "potential combat power (*zhanzheng qianli*; 战争潜力)," which is a term generally associated with military industrial capacity. It also specifically notes the need to collect "political, diplomatic, economic, scientific and technical, geographic, and other information."[21]

This suggests that not only will SOEs and perhaps private companies engage in

[19]Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 196.

[20]Chris Demchak and Yuval Shavitt, "China's Maxim—Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs*, Vol. 3, No. 1 (2018), https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca (accessed December 10, 2018).

[21]All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 226.

cooperative and coordinated information gathering, but companies may also designate key information targets. They may, for example, seek not only technical information, but also business development plans, marketing plans, and acquisition and merger targets. The array of Western companies and entities that have been targeted by what are believed to be Chinese hackers, including military units, suggests that this may indeed be the case. The PLA's Unit 61398, for example, is said to have targeted Coca-Cola in 2009, when the firm attempted to acquire China Huiyuan Juice Group.[22]

Chinese espionage efforts have also included efforts to secure information in key technologies not typically associated with military and defense. For several years, Chinese nationals have been found trying to smuggle advanced hybrid seeds from the United States.[23] As the PRC is a net food importer, it views food security as a vital national concern, comparable to energy security.

Finally, because of the role of influencing others in the realm of espionage, it is also useful to consider the Chinese targeting of academia. It is clear that the Chinese wish to project a particular image of the PRC, and this means shaping academic study of that nation. Scholars are actively discouraged from investigating certain topic areas. Xinjiang, the large Chinese northwest province with a large Uighur population, is a case in point. Even before the current repression of the Uighurs, Western scholars interested in Xinjiang faced significant obstacles to studying the region. When Routledge (a long-standing academic publisher) published an anthology examining a wide variety of aspects of Xinjiang, including ethnicity, history, and economy, many of the contributing authors found they could no longer obtain visas to China.[24] The implication seems clear: if you pursue even academic studies of issues that Beijing does not support, there will be consequences.

This appears to be an ongoing effort. In 2017, it came to light that Cambridge University Press, under great pressure from the PRC, had agreed to censor digital back issues of *China Quarterly*, one of the premier journals of the China studies field. The Chinese General Administration of Press and Publications had pushed for the removal of articles relating to Xinjiang, Tibet, Taiwan, the Great Proletarian Cultural Revolution, and the events of June 1989. The PRC had apparently also pressed for the removal of a thousand e-books from the publisher's website.[25] While the publisher eventually backed down, their willingness to cave to Chinese pressure highlights how far-reaching China is willing to go to ensure that its version of history and perceptions dominates.

[22]David E. Sanger, David Barboza, and Nicole Perlroth, "China's Army Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013, https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html (accessed December 10, 2018).

[23]Ted Genoways, "Corns Wars," *The New Republic*, August 16, 2015, https://newrepublic.com/article/122441/corn-wars (accessed December 10, 2018), and "Chinese Scientist Gets Ten Years in U.S. Prison over Theft of GMO Rice," Reuters, April 4, 2018, https://www.reuters.com/article/us-kansas-court-china/chinese-scientist-gets-10-years-in-u-s-prison-over-theft-of-gmo-rice-idUSKCN1HB36A (accessed December 10, 2018).

[24]Daniel deVise, "U.S. Scholars Say Their Book on China Led to Travel Ban," *Washington Post*, August 20, 2011, https://www.washingtonpost.com/local/education/us-scholars-say-their-book-on-china-led-to-travel-ban/2011/08/17/gIQAN3C9SJ_story.html?noredirect=on&utm_term=.93c7cbe9b08d (accessed December 10, 2018).

[25]Elizabeth Redden, "Outrage Over University Press Caving in to Chinese Censorship," *Inside Higher Ed*, August 21, 2017, https://www.insidehighered.com/news/2017/08/21/cambridge-university-press-blocks-access-300-plus-articles-request-chinese-censors (accessed December 10, 2018).

Recommendations

Because the Chinese engage in both non-traditional methods of espionage, and employ them against non-traditional targets, it is important for the United States to think beyond military and intelligence aspects. American planners, including Congress, need to think beyond military and intelligence means and ends, not only in assessing what the Chinese are doing, but also how to counter them.

Two key issues, then, should be how to prevent technology from reaching the PRC, and how to discourage and punish ongoing efforts.

Preventing technology from reaching the PRC. Clearly, it is in the American interest to limit the illegal flow of controlled or otherwise sensitive technology to the PRC, and any other unauthorized destination. To this end, there is already a range of restrictions, including ITAR and CFIUS. But the recent Chinese effort to access Boeing satellite technology through third-party funding of an American start-up indicates that the PRC is continuing its efforts to circumvent these efforts.

Increase the Resources Available for Investigations. The Foreign Investment Risk Review Modernization Act (FIRRMA) of August 2018 is a step towards countering such subterfuge. One of the provisions, for example, is the review of minority investments that might provide access to sensitive information or technology, even if the minority investor does not have a controlling share. But the resources available to conduct such reviews are limited. Therefore, it is vital that Congress consider increasing the resources available for such investigations. As Silicon Valley increases its interactions with the PRC, and actively seeks business there, this will become a more pressing requirement.

Ensure that the Information It Already Has Can Be Shared Smoothly and Rapidly. This means mandating increased interaction among not only intelligence and law enforcement agencies, but also regulatory bodies, such as the Securities and Exchange Commission, as well as the Department of Treasury and Department of Commerce. It also should entail increased information sharing with American companies in effected technology areas. The private sector is the main target for Chinese non-traditional espionage methods; only by cooperating with them can the U.S. hope to stanch the outflow of sensitive information. In the face of the comprehensive Chinese threat, the U.S. can ill-afford self-imposed stovepiping of the various relevant agencies, organizations, and companies. At the same time, however, there must also be proper provisions kept in place to ensure that such information sharing does not lead to abuse or violations of Americans' civil liberties.

Limit Chinese Access to American Technology. In key areas such as aerospace and information and communications technology, safeguarding America's technology argues for limiting interactions with the PRC. The limits placed on NASA's interactions with their Chinese counterparts, for example, arguably helps prevent inadvertent disclosures to the PRC. This is especially important, given the outsize PLA role in China's space program, as well as the fused nature of China's aerospace industry, which serves military, civilian, and commercial users.

Discouraging Chinese Non-traditional Activities. American efforts can only have so much effect so long as the Chinese believe that they can operate with impunity. The issuing of indictments, such as of the five PLA officers in 2014, signals American unhappiness, but the likelihood that those officers would be extradited, or even accessible, is questionable. Indeed, the issuance of a public indictment makes it unlikely that they will even transit through countries with extradition treaties with the

U.S., such as occurred with Huawei's CFO Meng Wanzhou.

It is therefore essential that more proactive measures be incorporated into the quiver of American response options.

Apply Current U.S. Laws Governing the Trafficking and Use of Stolen Goods. These laws have typically been formulated with physical goods in mind. However, if Chinese companies are exploiting stolen intellectual property, then it is possible that current statutes could be applied to those companies.

Apply the Racketeer Influenced and Corrupt Organizations (RICO) Act, Regarding the Activities of Criminal Organizations. If Chinese companies are knowingly exploiting stolen intellectual property, obtained in cooperation with the Chinese government, then those activities should be reviewed as more than just the actions of certain individuals, but reflect a broader, organized effort.

Ensure a Comparable Level of Proof, as Mandated in the American Legal Process. This would include being able to achieve a suitable standard of evidence, which may be difficult given the sources of information. The precedent set in the wake of 9/11 may offer a useful model. The intelligence community and various federal, state, and local law enforcement agencies seem to be better able to share information to counter various terrorist plots. A similar facilitation should be undertaken across the same bodies, as noted previously.

Such an effort, if successful, could reap significant benefits. The political gains of being able to demonstrate, in a court of law, beyond a reasonable doubt, that Chinese companies are acting in an illegal manner would be substantial, not only in the U.S., but globally. Moreover, it would strongly reinforce American arguments at the World Trade Organization and in other forums that China is acting against the international rules–based order.

* * * * * * * * * * * * * * * * * * *