The Threat of China's MSS: American Universities, Corporations, and Overseas Intelligence Operations

William Hubbell

william.hubbell@mycampus.apus.edu

The intelligence community in the United States is widely regarded as one of the most advanced in the world. The Central Intelligence Agency (CIA), the National Security Agency (NSA), and others have long played a vital role in protecting the nation's national security interests, especially amid growing totalitarianism and extremist worldwide. Unfortunately, several countries wish harm upon the United States and its allies, which means that their respective intelligence communities tend to be fixated upon objectives detrimental to American national security interests. In light of the current war in Ukraine, alongside longstanding tension from the Cold War, the Komitet Gosudarstvennoy Bezopasnosti (KGB), otherwise known as the principal intelligence agency of Russia, has understandably garnered substantive interest from scholars and analysts alike. However, the Ministry of State Security (MSS) in China should be of significant concern to the United States, especially when accounting for the insidious ways in which the MSS can harm vital national security interests. Dorfman (2020) notes that the ongoing battle regarding data, namely "who controls it, who secures it, who can steal it, and how it can be used for economic and security objectives," has gradually come to define the growing conflict between Washington and Beijing, which in turn underscores the growing threat MSS poses to the United States. As detailed in the following analysis, China's MSS poses a significant threat to United States national security in the short-term and long-term due to its exploitation of American universities, corporations, and overseas intelligence operations.

The American university system constitutes an increasingly weak link in national security, especially considering how deeply integrated many of its services and programs are with Chinese interests. In general, universities across the United States "have long played a leading role in relations between the United States and China" (Diamond & Schell, 2019), especially in terms of the numerous students and professors of Chinese origin present across universities today. In light of several highly publicized incidents regarding the theft of technology or other serious issues, fears have risen regarding MSS's propensity for "using American universities as vehicles through which to advance Chinese Community Party propaganda" (Diamond & Schell, 2019). It is import-

doi: 10.18278/gsis.8.1.2

ant to note that Chinese law is remarkably strict in terms of the information that it is allowed to collect from its citizens, which means that it has access to virtually all student data and information while they study in the United States. In several cases, students may willingly provide data to MSS, especially if they enrolled in American universities for espionage purposes in the first place.

For this reason, American university system has become an optimal "soft target" in terms of the "the global espionage war with China" (Dilinian, 2020). As observed by Bill Evanina, who serves as one of the top counterintelligence officials in the United States: "A lot of our ideas, technology, research, innovation is incubated on those university campuses … That's where the science and technology originates – and that's why it's the most prime place to steal" (Dilinian, 2020). Universities, in other words, are a valuable source of data for MSS, especially as it continues contributing information to the growing, vast apparatus of AI driven technologies. In essence, "data has already critically shaped the course of Chinese politics," which in return has started "altering the course of U.S. foreign policy and intelligence gathering around the globe" (Dorfman, 2020). In remarks to *Foreign Policy*, Evanina illustrates the grave threat China poses in that it is "one of the leading collectors of bulk personal data around the globe, using both illegal and legal means" (Dorfman, 2020), which has been evident in several different cases.

These cases entail both students and professors who have been accused of providing information to or otherwise taking actions to benefit MSS. For instance, a Boston University student failed to disclose her position as a lieutenant in the People's Liberation Army (Dilanian, 2020). In addition, at the Illinois Institute of Technology in Chicago, a Chinese student was charged for attempting "to recruit spies for his country's version of the CIA" (Dilanian, 2020). Bo Mao, who was a professor at the University of Texas, stole proprietary technology from an American Silicon Valley startup and subsequently passed it along to Huawei, the highly controversial Chinese telecommunications giant. Mao's affiliation with the university is precisely what enabled him to steal the technology: "By using his status as a university researcher to obtain the circuit board under the guise of academic testing" (Dilanian, 2020). In other words, academics have the ability to gain access to otherwise privileged or confidential information under the name of research. This information can be highly secretive for a reason, especially if it pertains to nuclear technology or other highly specialized information. Moreover, academics can also participate directly in helping Chinese bolster its intelligence, further weakening national security.

One of the most egregious cases included that of Dr. Charles Lieber, the former Chair of Harvard University's Chemistry and Chemical Biology Department, who was charged alongside two Chinese nationals for aiding the People's Republic of China. Lieber's arrest occurred after it emerged that he had lied about his involvement with the Thousand Talents Plan, which has drawn increased scrutiny from the American intelligence community (Department of Justice, 2020). According to the Department of Justice (2020), China's Thousand Talents Plan constitutes "one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent," chiefly to further "China's scientific development, economic prosperity and national security." In essence, this talent program "[seeks] to lure Chinese overseas talent and foreign experts to bring their knowledge and experience to China," as well as "reward individuals for stealing proprietary information" and providing it to Chinese intelligence authorities (Department of Justice, 2020). The program has drawn the great ire of American agencies, who have viewed it as a vehicle for the MSS to obtain information for purposes of furthering China's power. Lieber was involved in the Wuhan University of Technology, which paid him exorbitant compensation for his services: "WUT paid Lieber $50,000 USD per month, living expenses of up to 1,000,000 Chinese Yuan (approximately $158,000 USD at the time) and awarded him more than $1.5 million to establish a research lab at WUT" (Department of Justice, 2020). The level of greed exhibited by Lieber illustrates precisely how the MSS is able to exploit weak links in the American university system, and it continues this exploitative practice with regards to American corporations and their innovative technologies.

Whereas two decades ago a major concern was the targeted attack on classified Department of Defense websites, the major concern now includes "the shift [in espionage efforts] to private sector intellectual property research and development, particularly by China, who has been the most egregious one in stealing those technologies" (CBS News, 2021). Consequently, corporations, like universities, have become of great interest to MSS, especially since "another way to get the tiger is to circumvent the developmental process altogether by stealing the product" (Hannas et al., 2013). The espionage capabilities exhibited by MSS illustrate precisely why the NSA finds cyber espionage to be particularly damaging in terms of monetary loss. On July 26, 2012, General Keith Alexander of the NSA informed the Aspen Security Forum that cyber espionage constituted "the greatest transfer of wealth in history" (Hannas et al., 2013). Per the American government, U.S. corporations routinely "lose billions of dollars' worth of technological innovation each year to China" (Schnell, 2022), a staggering figure not only from the massive amount alone, but also the implications of that much proprietary technology being lost to China through its nefarious spy agencies' efforts. In other words, the real losses may be even greater if the United States loses its edge in innovation relative to China.

Multiple cases of Chinese executives or professionals engaging in crime on behalf of Chinese intelligence have abounded, especially when incentivized. For example, Xiangdong Yu had previously worked as a product engineer for Ford Motor Company, where he copied approximately 4,000 Ford documents into an external hard drive for purposes of obtaining a job with an automotive company in China (Hannas et al., 2013). However, Yu was captured in October 2009 and pled guilty to one count of theft of trade secrets (Hannas et al., 2013). In one especially remarkable case, an actual MSS officer managed to penetrate an American corporation and attempt to obtain highly sensitive information. Yanjun Xu, under the direction of the MSS, was "accused of seeking to steal General Electric/Aviation jet engine technology" (Schnell, 2022), which, given the potential military applications, constitutes a serious issue. Moreover, Xu's case was highly unique in the sense that it employed remarkable cyber subterfuge efforts: "A unique feature of his case is that it he allegedly did so without ever setting foot in the [United States]" (Schnell, 2022). In other words, as Chinese capabilities in cyber espionage continue to advance, the technology of American companies is increasingly threatened. This threat is compounded by the reality that Americans and Chinese are deeply integrated in technological innovation and production, which is why Former Secretary of Defense Robert Gates advocated a "small yard, high fence" approach for protecting American corporations. Specifically, Gates called for "selectively protecting key technologies, and doing so aggressively" (Hass & Balin, 2019) in an effort to protect American security interests.

While MSS can cause havoc internally in the United States, it can also create havoc for U.S. intelligence agencies externally, or over the course of their overseas intelligence operations. This level of disruption, along with domestic disturbances, is precisely why "the FBI opens a new China-related counterintelligence investigation every 12 [hours]" (Schnell, 2022) As of 2020, at least 5,000 cases were active (Wray, 2020). These cases also account for the fact that the MSS and its support have access to highly sophisticated technologies that cause a serious threat to United States operations overseas. For example, in 2013, American intelligence agencies discovered a highly troubling trend: "Undercover CIA personnel, flying into countries in Africa and Europe for sensitive work, were being rapidly and successfully identified by Chinese intelligence," and "in some cases as soon as the CIA officers had cleared passport control" (Dorfman, 2020). In general, American intelligence attempts to recruit "Russians and Chinese hard in Africa" (Dorfman, 2020) per one former official, which is precisely why the exposure of these agents is highly problematic in terms of their safety.

Moreover, when recalling the troves of data MSS and other agencies have managed to obtain via hacks, it is important to note that, "compounding the threat, the data China stole is of obvious value as they attempt to identify people for secret intelligence gathering" (Wray, 2020). Specifically, with regards to MSS's ability to identify CIA agents as soon as they cleared passport control, "U.S. officials believed Chinese intelligence operatives had likely combed through and synthesized information from these massive, stolen caches to identify the undercover U.S. intelligence officials" (Dorfman, 2020). A former intelligence official referred to the "suave and professional utilization" of these data sets as neither "random," nor "generic," but rather "a big data problem" (Dorfman, 2020). This situation illustrates precisely why "rapid escalation [constitutes] an acute risk, particularly if the pace of technological advancements in capabilities exceeds the development of protocols for maintaining human agency in decision-making loops" (Hass & Balin, 2019). In other words, whereas intelligence agencies could try to root out moles in the past, big data analytics, which may be more effective than moles, is a far more difficult foe to defeat.

In general, China arguably poses the biggest threat, or clearly one of the biggest threats, to the United States in a number of ways: Per Joseph Bonavolonta, an agent with the FBI, "no country poses a greater, more severe or long-term threat to our national security and economic prosperity than China" (Dilianian, 2020). Thus, its premiere intelligence agency, MSS, is a huge threat due to its ability to exploit American universities, corporations, and overseas intelligence operations. Theft of proprietary information from universities and corporations is commonplace, among other behaviors, some of which are directly executed by MSS officers themselves. Moreover, advancements in artificial intelligence are enabling the MSS to become an even fiercer opponent in overseas intelligence operations. As noted by Bonavolonta, "China's communist government's goal, simply put, is to replace the U.S. as the world superpower, and they are breaking the law to get there" (Dilianian, 2020). However, it is important to note that "China's appetite for foreign technology and its network for informal technology acquisition extend well beyond the United States," including attacks on the UK and other allies as well (Hannas et al., 2013). Consequently, it is crucial for interagency collaboration to attempt countering the growing China threat posed through its intelligence agency, MSS.

To strengthen cybersecurity measures, there are several methods to counter China from posing threats in America. These include enhancing cybersecurity protocols within universities, corporations, and government agencies to safeguard against cyber threats and intellectual property theft. International cooperation to prevent China's MSS from taking over American universities requires a multi-faceted approach. Countries need to establish effective information sharing mechanisms, exchanging intelligence on MSS activities and individuals or organizations with suspected ties to the MSS. This collaborative effort can aid in identifying potential threats and devising countermeasures. Additionally, policy coordination is vital to safeguard the independence and integrity of academic institutions. By developing unified guidelines and regulations, countries can address vulnerabilities, increase transparency in research funding, and protect academic freedom, reducing the MSS's ability to exploit loopholes in the system.

Bolstering cybersecurity measures is essential in preventing MSS-related cyber espionage and intellectual property theft. International cooperation should focus on sharing best practices, conducting joint cybersecurity drills, and coordinating responses to cyber threats originating from MSS-affiliated entities. By leveraging collective expertise and resources, universities can enhance their cybersecurity infrastructure, minimizing the risk of MSS interference. Furthermore, academic exchanges and collaborations should continue, but with increased transparency and scrutiny. Establishing guidelines for vetting partnerships and research collaborations, particularly in sensitive areas, can help mitigate the risk of undue influence. Overall, international cooperation plays a crucial role in fortifying American universities against MSS infiltration while promoting academic freedom and knowledge sharing (Jinghua, 2019).

Another method is by encouraging China to adhere to international norms and rules governing cybersecurity and intellectual property protection. This involves a two-fold approach. Primarily, diplomatic engagement is essential. Open and constructive dialogue should be established to foster mutual understanding and emphasize the benefits of compliance. Diplomatic efforts should stress the significance of cybersecurity and intellectual property protection for global economic growth and stability, emphasizing the advantages of a level playing field and fair competition. Through sustained diplomatic engagement, China can be encouraged to recognize the importance of adhering to these norms.

Furthermore, incentives and cooperation are key. Positive incentives can motivate China to align its practices with international standards. These incentives may include trade and economic benefits tied to compliance, such as enhanced market access and preferential treatment. Bilateral and multilateral cooperation can facilitate collaboration on cybersecurity and intellectual property protection. Sharing best practices, expertise, and technology, as well as jointly addressing common challenges, can demonstrate the advantages of adhering to international norms. By fostering public-private partnerships and providing technical assistance, capacity-building initiatives can be undertaken to assist China in effectively addressing these issues. These combined efforts, encompassing incentives, cooperation, and capacity-building, can contribute to the gradual adoption of international norms and rules by China.

The 2020 Annual Report to Congress highlights the importance of industry-government partnerships in fostering closer collaboration between the government and private sector entities, particularly universities and corporations, to exchange information, insights, and technological expertise. These partnerships can facilitate the sharing of knowledge and resources, enabling the government to leverage the expertise and innovation of the private sector. By establishing robust channels for communication and cooperation, such partnerships can enhance the exchange of critical information on emerging technologies, cybersecurity threats, and best practices. The collaboration between universities and corporations can facilitate joint research initiatives, technology transfer, and workforce development programs, fostering innovation and driving economic growth. Ultimately, these industry-government partnerships can create a dynamic ecosystem that harnesses the strengths of both sectors, promoting information sharing, innovation, and technological advancement for the benefit of society as a whole. (Congress, 2020).

Lastly, engaging in international discussions and negotiations is vital to establish norms and agreements governing cyber operations, intelligence activities, and the protection of intellectual property. By participating in these discussions, countries can collectively address the challenges posed by China's non-traditional espionage activities. International discussions provide a platform for countries to exchange perspectives, share experiences, and develop common understandings of the threats posed by cyber operations and intellectual property theft. These discussions aim to establish international norms and agreements that outline acceptable behavior in cyberspace, define the boundaries of intelligence activities, and promote the protection of intellectual property rights. Through negotiations, countries can work towards consensus on these issues, seeking to establish legally binding agreements or frameworks. These agreements can serve as a guide for responsible behavior in cyberspace, discourage malicious activities, and outline consequences for non-compliance. Additionally, discussions and negotiations can help shape the development of international standards and guidelines to address emerging threats and challenges. (Department of Justice, 2020).

It is important to note that these counter strategies should be tailored to the specific challenges posed by China's MSS and regularly evaluated and adapted to address evolving threats in the intelligence and cybersecurity landscape. Also, a holistic approach that combines technological advancements, intelligence sharing, public-private partnerships, and international cooperation to effectively counter the MSS threat. Constant vigilance, proactive measures, and adaptability are also key to mitigating risks and safeguarding national security interests in the face of evolving intelligence challenges from China.

References

Diamond, L. & Schell, O. (2019). *China's Influence and American Interests: Promoting Constructive Vigilance*. Hoover Institution Press. Dilanian, K. (2020). American universities are a soft target for China's spies, say U.S. intelligence officials. *NBC News*. https://www.nbcnews.com/news/china/american-universities-are-soft-target-china-s-spies-say-u-n1104291

Dorfman, Z. (2020). China Used Stolen Data to Expose CIA Operatives in Africa and Europe. *Foreign Policy*. https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/

Jinghua, L. (2019, March 22). *What are China's cyber capabilities and intentions?* IPI Global Observatory. https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/

Hannas, W.C., Mulvenon, J., Puglisi, A.B. (2013). *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*. Taylor & Francis.

Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases. (2020). *Department of Justice*. https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

Hass, R. & Balin, Z. (2019). US-China relations in the age of artificial intelligence. *Brookings*. https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/

Schnell, J. (2022). Cultural Variables Within Prosecution of Chinese Corporate Espionage: The Case of USA Versus Yanjun Xu. *Fudan J. Hum. Soc. Sci.* https://doi.org/10.1007/s40647-022-00350-0

The Strategic Competition Act of 2021, 117th Cong., 1st Sess. (2021). https://www.foreign.senate.gov/imo/media/doc/DAV21598%20-%20Strategic%20Competition%20Act%20of%202021.pdf

Top counterintelligence official Mike Orlando on foreign espionage threats facing U.S. (2021). *CBS News*. https://www.cbsnews.com/news/foreign-espionage-threats-u-s-intelligence-matters-podcast/

U.S.-China Economic and Security Review Commission. (2020). *2020 annual report to Congress*. Retrieved May 26, 2023, from https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf

U.S. Department of Justice. (2018, December 12). *China's non-traditional espionage against the United States: The threat and potential policy responses.* https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2018/12/18/12-05-2018_john_c._demers_testimony_re_china_non-traditional_espionage_against_the_united_states_the_threat_and_potential_policy_responses.pdf

Wray, C. (2020). The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States. *FBI*. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states