FBI COUNTERINTELLIGENCE BULLETIN

02 September 2020

China’s People’s Liberation Army (PLA) Continues to Abuse US Intellectual Freedom to Advance Its Military Capabilities

Summary

The FBI’s Counterintelligence Division prepared this bulletin to inform academia, specifically faculty and administration at US universities, regarding the People’s Republic of China’s (PRC) information collection activities targeting intellectual property, sensitive information, and research at US academic institutions.

Recent criminal prosecutions clearly demonstrate that the PRC is exploiting visa programs to covertly send its military officials to the United States posing as visiting scholars or students to collect information. The FBI is urging US academic institutions to become aware of the threat and remain vigilant of foreign adversaries’ ulterior motive(s) while continuing to ensure an exchange of ideas in an open and transparent environment. Following are some recent case examples.

Details

Ye Yanqing is a PRC People’s Liberation Army (PLA) officer who lied about her PLA connection on her visa application to get into a Boston area university as a visiting scholar from 2017 to 2019 researching knowledge graph construction, analysis, and application based on data mining. Being enrolled at the university allowed her access to US military websites, research data, and personal information of experts in the field, information that she routinely sent to her contacts in China. Ye also gave her university user name and password to military colleagues in China for them to use. Additionally, Ye used her US research to advance her Ph.D. studies at the PRC’s National University of Defense Technology, a military academy responsible for modernizing China’s military and designing advanced weapons. Ye was able to return to China in 2019 before US authorities could arrest her for acting as an agent of a foreign government, visa fraud, conspiracy, and making false statements.[i]

Xin Wang allegedly was still working for a PLA lab when he entered the United States in March 2019 for the stated purpose of conducting research at a northern California university, but he claimed on his visa application that his employment with the PLA had ended in 2016. Wang was tasked to replicate the layout of the university’s lab in China, and he admitted to reproducing some of the university lab’s work—which was funded by the National Institutes of Health and the US Department of Health and Human Services—at the lab in China. The FBI arrested Wang in June 2020 for visa fraud.[ii]

Juan Tang, according to the criminal complaint charging her with visa fraud, answered “No” on her visa application to the question, “Have you ever served in the military?” and entered the United States in December 2019 to conduct research at a California university. As set forth in the complaint, the FBI found photos of Tang in two different PLA Air Force (PLAAF) uniforms and references to her current employment with a PLAAF medical university. Tang sought refuge at the PRC consulate in San Francisco in July 2020 but was taken into custody shortly afterward.[iii]

Chen Song, according to the criminal complaint charging her with visa fraud, lied on her J-1 visa application in response to the question, “Have you ever served in the military?” She allegedly responded that she had previously served in the PLA but separated in 2011 and that she is currently a neurologist employed by a non-military-affiliated hospital in China coming to the

United States to conduct brain disease research at a northern California university. An affidavit supporting the complaint alleges that these were lies, having identified research articles she co-authored describing her as affiliated with PLAAF institutions and a website with a photo of her in what appears to be a PRC military uniform well after 2011. Also according to the affidavit, a search of Song's external hard drive turned up a deleted letter from Song to the PRC consulate in New York explaining her one-year extension in the United States. She stated in the letter that the hospital in China listed as her employer is a false front and that she could not transmit her military approval documents via the Internet because they are classified. The FBI arrested Song in July 2020.[iv]

Kaikai Zhao was a graduate student at a university in Indiana studying machine learning and artificial intelligence. According to the criminal complaint charging him with visa fraud, Zhao lied on his F-1 visa application when he responded "No" to the question, "Have you ever served in the military?" Zhao allegedly served in the PLA's National University of Defense Technology and attended the Aviation University of the Air Force (AUAF). The AUAF is the PRC's equivalent of the US Air Force Academy, in which students are active military service members who receive military training while conducting their studies. According to the complaint, the FBI also located an online photo of Zhao wearing a PLAAF uniform. The FBI arrested Zhao in July 2020.[v]

Potential Indicators

These cases demonstrate the PLA's willingness to lie and omit affiliation on their academic applications in order to obtain access to programs of interest. Universities and research organizations should remain vigilant against foreign adversaries' ulterior motive(s), working with their local FBI offices for guidance as they conduct appropriate due diligence in making hiring and admissions decisions.

Some potential indicators of someone hiding his or her affiliation or intentions are:

- Failing to disclose funding from China for scholarships or projects
- Trying to obtain sensitive information from research projects outside of their expertise
- Attempting to circumvent security protocols or use credentials of other students/employees
- Claimed affiliation with a foreign institute or school that is very new without established credentials
- Taking sensitive information home without authorization

What is sensitive information? Sensitive information can include many things, such as pre-publication research data, prototypes or blueprints, provisional patent application data, software and source codes, confidential research notes, products or data that are export controlled, and proprietary materials shared under the guise of research partnerships. Other types of sensitive information include classified US Government information handled under government grants or contracts and reports on US Government foreign policy plans or intentions. Even the physical layout of a laboratory or a list of equipment in a laboratory can be sensitive information.

Risk Mitigation Strategies

These cases represent just a small part of the PRC's increased efforts to take advantage of the openness of universities in the United States to strengthen its military. Academic institutions can take steps—such as conducting a compliance review; training faculty, staff, and students; and engaging with the FBI—to help minimize the risks to our national security through theft of intellectual property and trade secrets by foreign adversaries.

In 2020, the Association of American Universities (AAU) and the Association of Public and Land-grant Universities (APLU), in collaboration with the Council on Governmental Relations (COGR), updated recommendations for universities and research organizations to address risks from foreign government influence. COGR also produced a report that helps institutions assess potential research security risks and develop strategies for mitigation. A link to the full report may be found in the "Resources" section of this bulletin. The following risk mitigation strategies are taken from those recommendations.

- Build awareness and communicate.
- Train faculty, students, and visiting researchers.
- Interact with federal security and intelligence agencies.
- Protect electronic data.
- Protect intellectual property and use technology control plans.
- Review collaborations, contracts, and foreign gifts.
- Review, update, and enforce conflict-of-interest policies.
- Develop international travel policies.
- Build a program to securely vet and host foreign visitors.
- Strengthen policies and programs to ensure full compliance with export control requirements.

Resources

AAU and APLU risk mitigation strategies for universities: *University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus*

COGR "*Framework for Review of Individual Global Engagements in Academic Research*"

Effective practices for developing a foreign visitor program are available at the Academic Security & Counter Exploitation Program at Texas A&M University.

Additional information regarding the PRC's economic espionage efforts and their Military-Civil Fusion plan can be found at https://www.fbi.gov/investigate/counterintelligence/the-china-threat and https://www.state.gov/military-civil-fusion.

Contact

If you become aware of any misuse of institutional resources that may violate US laws, or if you have any requests or questions, please contact your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices or email Academia@FBI.Gov.

[i] DOJ | Press Release | "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases" | https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

[ii] DOJ | Press Release | "Researchers Charged with Visa Fraud After Lying About Their Work for China's People's Liberation Army" | https://www.justice.gov/opa/pr/researchers-charged-visa-fraud-after-lying-about-their-work-china-s-people-s-liberation-army

[iii] DOJ | Press Release | "Statement on the arrest of Juan Tang" | https://www.justice.gov/usao-edca/pr/statement-arrest-juan-tang

[iv] DOJ | Press Release | "Researchers Charged with Visa Fraud After Lying About Their Work for China's People's Liberation Army" | https://www.justice.gov/opa/pr/researchers-charged-visa-fraud-after-lying-about-their-work-china-s-people-s-liberation-army

[v] *Ibid*