UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA v. JI CHAOQUN	CASE NUMBER: **UNDER SEAL**

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

From on or about August 28, 2013 to on or about September 21, 2018, in the Northern District of Illinois, Eastern Division, and elsewhere, JI CHAOQUN, the defendant violated:

Code Section	*Offense Description*
Title 18, United States Code, Section 951(a)	did knowingly act in the United States as an agent of a foreign government, specifically the People's Republic of China, without prior notification to the Attorney General, as required by law

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

ANDREW K. MCKAY
Special Agent, Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: September 21, 2018

Judge's signature

City and state: Chicago, Illinois

MICHAEL T. MASON, U.S. Magistrate Judge
Printed name and Title

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS | ss

AFFIDAVIT

I, ANDREW K. MCKAY, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately August 2014.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to espionage offenses, including the gathering or delivery of defense information to aid a foreign government or agent, in violation of Title 18, United States Code, Section 794(a), and individuals who act as a foreign agent without notice to the Attorney General, in violation of Title 18, United States Code, Section 951(a).

3. This affidavit is submitted in support of a criminal complaint alleging that JI CHAOQUN violated Title 18, United States Code, Section 951. The statements in this affidavit are based on my personal knowledge, and information I have received from other law enforcement personnel and persons with knowledge of relevant facts. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging JI with acting as an agent of a foreign government without notice to the Attorney General, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint.

Background

4. Title 18 of the United States Code, section 951 (Agents of Foreign Governments), makes it a criminal offense for any person, other than a diplomatic or consular official or attaché, to act in the United States as an agent of a foreign government without prior notification to the Attorney General, as required by law. For purposes of this law, the term "agent of a foreign government" includes an individual who agrees to operate within the United States subject to the direction or control of a foreign government or official.

People's Republic of China Ministry of State Security

5. Based upon my training and experience, and information obtained from publicly available sources, the Ministry of State Security ("MSS") for the People's Republic of China handles civilian intelligence collection and is responsible for counter-intelligence and foreign intelligence, as well as political security. The MSS consists of its primary central office, provincial departments, and a number of local and municipal bureaus. For example, the Jiangsu Province Ministry of State Security ("JSSD") is a provincial department of the MSS. These state and local bureaus report to both their national ministries and state and local governments and party committees. The MSS has maintained both a clandestine and overt human source collection capability through a network of defense attachés, academics, and spies operating in and out of China. The MSS's purview and intelligence collection capability has evolved over time, incorporating new missions as technology allows.

6. Based upon my training and experience, and information obtained from publicly available sources, I am aware that Chinese intelligence services conduct extensive overt, covert, and clandestine intelligence collection operations against U.S. national security entities, including private U.S. defense companies, through a network of agents within and outside of China.[1]

Southern District of Ohio Investigation

7. On or about October 16, 2017, a search warrant was executed on an email account (the "Email Account") in connection with an investigation in the Southern District of Ohio. Emails obtained pursuant to the search warrant showed the user of the account communicating, coordinating and directing an individual in the United States ("Individual A") to provide technical information from a U.S.-based Company (the "Company") without authorization, and providing the information as a benefit to the Chinese government. Individual A was employed at the Company as an engineer beginning in or around 2007 through in or around late 2017.

8. According to the Company, and publicly available information about the Company, the Company is among the world's top aircraft engine suppliers for both commercial and military aircraft and undertakes a significant amount of aviation research for U.S. military aircraft. The Company is a cleared defense contractor and

[1] Based upon my training and experience, and information obtained from publicly available sources, I am also aware that Chinese intelligence services typically recruit and employ agents to collect a wide range of information, including U.S. national security secrets. Chinese intelligence typically focus their efforts on recruiting ethnic Chinese, primarily because of cultural and language affinity.

maintains a U.S. Department of Defense security clearance; however, Individual A did not have a security clearance while employed at the Company.

9. The search warrant returns from the Email Account obtained in connection with the ongoing investigation in the Southern District of Ohio revealed that the user of the Email Account established an iCloud account. In fact, the Apple ID was the same as the individual's email address.

10. On or about December 8, 2017, a search warrant issued in the Southern District of Ohio was executed on the Apple iCloud account related to the same Apple ID. The contents of the iCloud account included a "Cadre Approval/Removal Appointment Application Form" for an individual known to law enforcement ("Intelligence Officer A"). This form identified Intelligence Officer A as currently holding the position of a Deputy Division Director of the JSSD and having held positions with the MSS since June 2003.

11. On or about November 1, 2017, a search warrant was executed at the residence of Individual A in the Southern District of Ohio. During that search, agents seized a business card for an individual purportedly employed by an Association for Science and Technology, located in China. The search warrant return for the iCloud account contained a text message conversation from December 2013 in which Intelligence Officer A wrote in sum and substance, "the customer does not know our identity. I approached him with the identity of the Deputy Secretary-General

employed by an Association for Science and Technology."[2] Based on this message, my training and experience, as well as conversations with other law enforcement agents familiar with the investigation in the Southern District of Ohio, I believe that Intelligence Officer A uses aliases and false claims of employment when Intelligence Officer A does not want to disclose an affiliation to the JSSD.

JI CHAOQUN and Intelligence Officer A

12. According to immigration records, JI CHAOQUN was born in China and arrived in the U.S. from Beijing, China on or about August 28, 2013, on an F1 Visa, for the purpose of studying in the U.S. He received his Master's Degree in Electrical Engineering at the Illinois Institute of Technology in Chicago in December 2015. In his F1 Visa Application, JI listed his primary phone number as "152XXXXXX87" (the "JI Phone").[3]

13. Certain text messages from the SMS database from the Apple iCloud account referenced above suggest that JI was introduced to Intelligence Officer A by

[2] Certain email and text message communications have been quoted or summarized in this Affidavit (the "communications"). The communications are based upon draft—not final—English translations of Chinese communications completed by interpreters employed by the FBI. The summaries do not include all statements or topics covered during the course of the communications.

At various points in the Affidavit I have included my interpretation of words and phrases used in the communications. My interpretations are based on the contents and context of the communications, events occurring before and after the communications, my knowledge of the investigation as a whole, my experience and training, and the experience and training of other law enforcement agents in this investigation.

[3] The complete phone number is redacted because this will be a public filing.

Intelligence Officer B.[4] On or about November 29, 2013, Intelligence Officer B asked Intelligence Officer A "Can Little JI use his/her real name to fill out forms?" On or about December 18, 2013, Intelligence Officer B provided the following information to Intelligence Officer A, "[the JI Phone], JI Chaoqun" and informed Intelligence Officer A that JI would be on High Speed Rail G203 arriving at Nanjing South Station at 22:37. Intelligence Officer A replied to Intelligence Officer B, "Got it. Tell him that I'm a professor at Nanjing University of Aeronautics and Astronautics."

14. The Apple iCloud SMS database included approximately 36 messages between Intelligence Officer A and JI, from on or about December 19, 2013 to July 9, 2015.

15. According to his travel records, JI traveled to and from China on three occasions since his arrival in the U.S. JI traveled to Beijing on or about December 9, 2013, and returned to Chicago on or about January 15, 2014. JI again traveled to Beijing on or about May 19, 2014, and returned to Chicago on or about July 6, 2014. JI's last trip to China was when he traveled to Beijing on or about December 22, 2014, and returned to Chicago on or about February, 3, 2015.

[4] The search warrant return for the iCloud account included an entry for Intelligence Officer B in Intelligence Officer A's contact list. The iCloud account also included a database of SMS text messages. Intelligence Officer A's messages with Intelligence Officer B, from the SMS database for Intelligence Officer A's Apple iCloud Account, show that in or around January through April 2014, Intelligence Officer B referred to Intelligence Officer A as "Section Chief" and that Intelligence Officer B provided passwords to Intelligence Officer A. Intelligence Officer B is therefore believed to be a colleague of Intelligence Officer A's in the JSSD.

16. According to the Apple iCloud records, on or about December 18, 2013, JI sent the following message to Intelligence Officer A, stating, "Hi Big Brother, I'm JI Chaoqun. I'm taking the G203 [train] and will arrive at Nanjing South Station at 22:37." JI and Intelligence Officer A then exchanged several more messages in which Intelligence Officer A appeared to arrange to meet JI for the first time.

17. According to text messages from the SMS Database, on or about January 3, 2014, Intelligence Officer A asked JI if he could meet the following week. On or about January 10, 2014, JI informed Intelligence Officer A that he was on the subway. Intelligence Officer A then instructed JI where to get off the subway. Approximately five hours after this conversation, Intelligence Officer A informed his wife via text message that he had a suite in a hotel and asked her if she would like to stay. Based upon these communications and my training and experience, Intelligence Officer A and JI's second meeting likely occurred in a hotel room. Based upon my training and experience, conducting meetings in hotel rooms is an indication of intelligence officer tradecraft because meetings in hotel rooms provide a discreet, private place for the intelligence officer to recruit or debrief his/her intelligence asset.

18. According to text messages from the SMS Database, on or about January 11, 2014, JI asked Intelligence Officer A to order him a train ticket leaving Nanjing traveling to Beijing for the following day. Intelligence Officer A instructed JI to send the train ticket back to Intelligence Officer A when JI returned home. On or about January 12, 2014, Intelligence Officer A instructed JI to send the tickets to Intelligence Officer A at an address in Nanjing City, China. Based upon my training

and experience, Chinese intelligence agencies often require intelligence officers to produce itemized receipts for expenditures related to intelligence assets.

19. Open source research on the Nanjing City address revealed multiple images identifying the address as the location for the Jiangsu State Security Department.

20. Additional text messages obtained from Intelligence Officer A's Apple iCloud SMS database revealed that on or about June 11, 2014, Intelligence Officer A and JI coordinated a third meeting in China.

21. Based upon my training and experience, MSS officers often use aliases or alternate identities when initially meeting potential intelligence assets. Intelligence Officer A employed this tradecraft by initially using an alias with Individual A and assuming the identity of a professor with JI. While JI was initially told that Intelligence Officer A was a professor, it appears that JI learned of Intelligence Officer A's affiliation with the JSSD because Intelligence Officer A told JI to send items to the JSSD address, which is listed on public Chinese-language websites. As explained below, JI later acknowledged in a meeting with an undercover agent that he believed Intelligence Officer A was part of a "confidential unit" with Intelligence Officer B, and that Intelligence Officer B told him stories about espionage.

22. On or about March 29, 2018, Magistrate Judge Daniel G. Martin issued a search warrant for the email account pricebidXXX@gmail.com ("Subject

Account 1").[5] According to the search warrant return, on or about August 30, 2015, an email was sent from JI, using Subject Account 1, to an email address hosted by "qq.com," stating, "eight sets of the midterm test questions for the last three years," which email was forwarded from Subject Account 1 to Intelligence Officer A.[6] The subject line for the email was "Midterm test questions." Eight separate pdf documents were attached to the email. The eight separate pdf documents are background reports on eight U.S.-based individuals generated by U.S.-based companies Intelius, Inc., Instant Checkmate, and Spokeo.[7]

23. According to JI's Discover credit card statements obtained via subpoena, on or about August 30, 2015, JI's credit card authorized charges in the total amount of $34.85 from Spokeo. On the same date, JI's credit card authorized charges totaling $277.35 from Intelius, Inc. According to the JP Morgan Chase records for JI's debit card obtained via subpoena, JI made multiple purchases totaling $84.82 on or about August 30, 2015; and one purchase totaling $19.95 on or about September 18, 2015,

[5] The complete email account is redacted because this will be a public filing.

[6] According to its website, QQ is an email and instant messaging service developed and maintained by China-based company Tencent Holding, Ltd.

[7] According to their websites, Intelius, Instant Checkmate, and Spokeo are each U.S.-based companies that offer, among other services, online services for consumers to purchase background reports about any individual. According to a representative from Intelius, and its Terms and Conditions, Intelius's services are intended only for U.S.-based consumers, and it utilizes a tool that restricts access to the Intelius website from China, among other locatiosn outside the U.S. According to a representative from Instant Checkmate, and its Terms of Use, purchases from outside the U.S. are strictly prohibited. According to a representative from Spokeo, and its Terms and Conditions, Spokeo's services are intended only for U.S.-based consumers, and Spokeo only accepts payment from U.S.-based credit cards with valid U.S. billing zip codes.

from Instant Checkmate. According to Spokeo records obtained via subpoena, Subject Account 1 was the email account associated with JI's Spokeo account.

24. According to the IP records associated with JI's account registrations with the background check companies obtained via subpoena, JI registered his accounts at Spokeo, Instant Checkmate and Intelius on August 30, 2015, from IP address 73.51.23.94, which, according to Comcast, is a US-based Comcast IP.

25. In addition, JI's financial and travel records also indicate JI was in the United States in August and September 2015, when he purchased and sent the above-referenced background check reports. According to JI's Discover and JP Morgan records, his accounts are maintained in the U.S. According to the JP Morgan Chase records, JI made a debit card purchase at Chicago Ventra on or about August 25, 2015, five days prior to his August 30, 2015 purchases from Instant Checkmate. On or about September 9, 2015, JI made a debit card purchase at the Potsticker House in Chicago, Illinois, nine days prior to his September 18, 2015 purchase from Instant Checkmate. According to JI's Treasury Enforcement Communications System (TECS) records, JI's last international travel was the trip from Chicago to Beijing from December 22, 2014 to February, 3, 2015, noted above.

26. According to information obtained from law enforcement databases, all eight individuals referenced in the background check documents were naturalized U.S. citizens born in Taiwan or China now living in the United States. All eight individuals either currently worked in or were recently retired from a career in the science and technology industry, including several individuals specializing in

aerospace fields. Open source research indicated that as of approximately January 2018, at least seven of the eight individuals worked for, or had recently retired from, cleared U.S. defense contractors.

27. Based upon my training and experience, it appears that JI was tasked by Intelligence Officer A to provide him with biographical information on eight individuals for possible recruitment by the JSSD. JI attempted to cover up the work he was doing on behalf of Intelligence Officer A by misrepresenting the contents of the attachments calling them "Midterm Test Questions" rather than stating the true contents of the email – background checks on ethnic Chinese working as engineers and scientists, including for cleared U.S. defense contractors. In my training and experience, it is typical tradecraft for Chinese intelligence officers to instruct their U.S. assets to conceal information they are providing to their handlers in China in order to protect that information, the asset, and the intelligence officer.

Undercover Meeting with JI CHOAQUN

28. On or about April 25, 2018, JI met with an individual who, unbeknownst to JI, was an FBI Special Agent working undercover (the "UC"). During the audio and video recorded first meeting between JI and the UC, the UC introduced himself to JI as someone directed to meet with JI by Intelligence Officer C in light of Intelligence Officer A's arrest.[8]

[8] Based upon the review of the SMS database text messages, agents believe that Intelligence Officer C is the direct supervisor of Intelligence Officer A at the JSSD. More specifically, in the majority of messages in which Intelligence Officer A either communicates directly with or references Intelligence Officer C, he uses Intelligence Officer C's formal title.

29. On or about May 17, 2018, JI met with the UC a second time. During the audio and video recorded meeting, JI made multiple statements that corroborated the information revealed during the course of the investigation and detailed above.

30. For example, JI explained that he was first introduced to Intelligence Officers A and B via Intelligence Officer C, who he met during a recruitment fair while in school in China. He stated he believed Intelligence Officers A, B, and C were in the same "confidential unit" and further explained as follows:

> Initially when I met [Intelligence Officer C], it was during a recruitment fair in the IM [phonetic] school. There was not much advertising. They were asking if anyone was interested in joining the organization. They said it was a confidential unit but they did not elaborate. Therefore, I went there and met [Intelligence Officer C]. Afterwards, [Intelligence Officer C] asked [Intelligence Officer B] to contact me in Beijing because [Intelligence Officer B] was in Beijing during that period of time. It was during my Nanjing trip that I met [Intelligence Officer A] for the first time when he was together with [Intelligence Officer C]. . . It was when I was in Beijing I contacted [Intelligence Officer B] for a few times. I often dined with him. He told me stories such as Long-Tan-San-Jie the three covert CCP agents inside KMT. Afterwards, I went to Nanjing to look for and meet [Intelligence Officer A]. Afterwards, when I first left China, it was [Intelligence Officer B] who contacted me using my undergraduate name and my newly registered email address.[9]

Based on my training and experience, using the formal title is a sign of respect and indicates that Intelligence Officer C holds a higher rank than Intelligence Officer A.

[9] Based on my training and experience, and information obtained from publicly available sources, "Long Tan San Jie" verbatim translates to "three heroes of the dragon's lair," but is colloquially a reference to a Chinese intelligence operation conducted in the late 1920s. Considered one of the earliest modern examples of a Chinese "seeding operation," the Chinese Communist Party (CCP) directed three spies to infiltrate the CCP's main rival political party, the Kuomintang (KMT). The three spies successfully gained employment with and access to sensitive KMT information and provided crucial warning to the CCP during the peak of the KMT's violent suppression of the CCP in 1931.

31. JI further explained that he had more contact with Intelligence Officer B at first because he went to undergraduate school in Beijing, which is where he understood Intelligence Officer B was based. He began communicating with Intelligence Officer A because, according to Intelligence Officer A, Intelligence Officer B was transferred to a different department.

32. JI further explained that Intelligence Officer A asked him to purchase background checks on a few people from the internet. He explained that "they just wanted me to purchase some documents on their behalf. Their reason was just because it was inconvenient for them to make payments from China." Based on my training and experience, I believe that Intelligence Officer A tasked JI with purchasing these background check reports because Intelligence Officer A was (a) using operational security tradecraft by not generating a subscriber and payment trail in China with the U.S.-based background check companies; and (b) was testing JI's skills as a potential asset by tasking him to purchase these background check reports.

33. JI further explained that the "people search website would tell you the price of a report per person," which appeared to be a reference to the background check reports JI purchased from Intelius, Instant Checkmate, and Spokeo. JI stated that he "purchased the documents after [he] came to the U.S," and that he paid approximately $700 for the reports. He further stated that Intelligence Officer A asked how he could send the money to JI after JI purchased the background check

documents, and JI provided Intelligence Officer A with an account number. He further stated that sometime thereafter he was reimbursed approximately $1,000.

34. JI further stated that he labeled the file containing the reports "Mid Term Quiz Questions," and sent the reports to both Intelligence Officers A and B via email, which is consistent with the emails discovered in Subject Account 1.

35. According to records checks conducted by the Department of Justice Foreign Agents Registration Unit, as of June 14, 2018, JI did not provide notice to the Attorney General of the United States of his actions or intentions to act as an agent of a foreign government or foreign official.

36. Based on the foregoing, I believe that JI acted as an agent of the Chinese government by agreeing to taskings from Chinese intelligence officers, and in particular, by obtaining background checks in the United States on ethnic Chinese individuals working for cleared U.S. defense contractors in the United States at the request of Intelligence Officers A, B, and C. By collecting this information for an arm of the Chinese government while in the United States, JI knowingly and unlawfully acted as an agent of a foreign power.

JI CHAOQUN and the MAVNI Program

37. In May 2016, JI enlisted in the U.S. Army Reserves as an E4/Specialist under the Military Accessions Vital to the National Interest program ("MAVNI") program.[10]

[10] The MAVNI program authorizes the U.S. Armed Forces to recruit certain legal aliens whose skills are considered to be vital to the national interest. Individuals such as physicians,

38. On or about June 6, 2016, as part of the process for his application to participate in the MAVNI program, JI electronically submitted Standard Form 86 ("SF-86"), a Security Clearance Application.

39. In Section 20B of the SF86, JI answered "No" to the following question:

> Have you or any member of your immediate family in the past seven years had any contact with a foreign government, its establishment (such as embassy, consulate agency, military service or security service, etc.) or its representatives, whether inside or outside the U.S.? (Answer 'No' if the contact was routine visa applications and border crossings related to either official U.S. Government travel or foreign travel on a U.S. passport.)

40. On or about December 6, 2017, also as part of the process for his MAVNI application, JI underwent a Single Scope Background Investigation ("SSBI") interview with a U.S. Army officer. As part of the interview, the officer reviewed JI's responses in the SF-86 with JI. During the interview, JI again failed to disclose his relationship and contacts with Intelligence Officers A, B, or C. At the conclusion of the interview, JI signed a Department of the Army Form 2823, which is a sworn statement affirming to the truthfulness of the information JI provided during his interview.

---

nurses, and experts in certain languages with associated cultural background become eligible if they meet the following requirements: candidates must be in the country legally, must have been in valid status for at least two years immediately prior to the enlistment date, and applicants who may be eligible on the basis of a nonimmigrant status category must not have any single absence from the United States of more than 90 days during the two-year period immediately preceding the date of enlistment. Once the immigrant enlistees complete the 10-week Basic Combat Training, their citizenship application will be expedited without first obtaining lawful permanent residence.

41. Based upon the above-described contacts between JI and Intelligence Officer A in China and via e-mail, JI's responses to the SF86 Section 20B question and during his SSBI interview were materially false representations.

Conclusion

42. Based on the foregoing, I believe there exists probable cause to believe that from on or about August 28, 2013, through on or about September 21, 2018, JI CHAOQUN, did knowingly act in the United States as an agent of a foreign government, specifically the People's Republic of China, without prior notification to the Attorney General, as required by law, in violation of Title 18, United States Code, Section 951(a).

FURTHER AFFIANT SAYETH NOT.

ANDREW K. MCKAY, Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me on September 21, 2018.

MICHAEL T. MASON
United States Magistrate Judge