How China Uses LinkedIn to Recruit Spies Abroad

Western intelligence officials say Chinese agents are contacting thousands of foreign citizens using LinkedIn, including former government officials.

Jonas Parello-Plesner, a former Danish Foreign Ministry official, reported an apparent recruiting attempt by the Chinese that began over LinkedIn.CreditCreditCarsten Snejbjerg for The New York Times

By Edward Wong

- Published Aug. 27, 2019 Updated Sept. 27, 2019

WASHINGTON — One former senior foreign policy official in the Obama administration received messages from someone on LinkedIn offering to fly him to China and connect him with “well paid” opportunities.

A former Danish Foreign Ministry official got LinkedIn messages from someone appearing to be a woman at a Chinese headhunting firm wanting to meet in Beijing. Three middle-aged men showed up instead and said they could help the former official gain “great access to the Chinese system” for research.

A former Obama White House official and career diplomat was befriended on LinkedIn by a person who claimed to be a research fellow at the California Institute of Technology, with a profile page showing connections to White House aides and ambassadors. No such fellow exists.

Foreign agents are exploiting social media to try to recruit assets, with LinkedIn as a prime hunting ground, Western counterintelligence officials say. Intelligence agencies in the United States, Britain, Germany and France have issued warnings about foreign agents approaching thousands of users on the site. Chinese spies are the most active, officials say.

“We’ve seen China’s intelligence services doing this on a mass scale,” said William R. Evanina, the director of the National Counterintelligence and Security Center, a government agency that tracks foreign spying and alerts companies to possible infiltration. “Instead of dispatching spies to the U.S. to recruit a single target, it’s more efficient to sit behind a computer in China and send out friend requests to thousands of targets using fake profiles.”

The use of social media by Chinese government operatives for what American officials and executives call nefarious purposes has drawn heightened scrutiny in recent weeks. Facebook, Twitter and YouTube said they deleted accounts that had spread disinformation about the Hong Kong pro-democracy protests. Twitter alone said it removed nearly 1,000 accounts.

It was the first time Facebook and Twitter had taken down accounts linked to disinformation from China. Many governments have employed similar playbooks to sow disinformation since Russia used the tactic to great effect in 2015 and 2016.

LinkedIn, owned by Microsoft, is both another vehicle for potential disinformation and, more important, an ideal one for espionage recruitment, American officials say.

That is because many of its 645 million users are seeking employment opportunities, often from strangers. To enhance their prospects, many former government employees advertise that they have security clearances.

LinkedIn is also the only major American social media platform not blocked in China because the company has agreed to censor posts containing delicate material.

Chinese agents often make offers over various channels, including LinkedIn, to bring the prospective recruit to China, sometimes through the guise of a corporate recruiting firm offering to pay them for speaking or consulting engagements or aid in research. From there, agents develop the relationship.

“The Chinese want to build these options with political, academic and business elites,” said Jonas Parello-Plesner, the former Danish Foreign Ministry official who reported the apparent recruiting attempt by the Chinese that began over LinkedIn. “A lot of this thrives in the gray zone or the spectrum between influence-seeking and interference or classical espionage.”

People who have just left government are especially vulnerable because they are often looking for new employment, he and other former officials say.

Nicole Leverich, a spokeswoman for LinkedIn, said the company proactively finds fake accounts to remove and has a team that acts on information from a variety of sources, including government agencies.

“We enforce our policies, which are very clear: The creation of a fake account or fraudulent activity with an intent to mislead or lie to our members is a violation of our terms of service,” she said.

Some photographs on fake accounts are generated by artificial intelligence, The Associated Press reported.

In multiple recent cases, LinkedIn proved to be an effective recruiting tool. A former employee of the C.I.A. and Defense Intelligence Agency, Kevin Patrick Mallory, was sentenced in May to 20 years in prison for spying for China. The relationship began after he replied in February 2017 to a LinkedIn message from a Chinese intelligence agent posing as a think tank representative, the F.B.I. said.

The Justice Department last October charged a Chinese intelligence agent, Yanjun Xu, with economic espionage after he recruited a GE Aviation engineer in a relationship that began on LinkedIn, according to the indictment.

Mr. Evanina, the counterintelligence chief, told Reuters last year that Chinese agents were contacting thousands of people at a time on LinkedIn. “It’s the ultimate playground for collection,” he said.

That level of activity has not dropped, though Mr. Evanina declined to give statistics.

“People in the private sector and academia are also being targeted this way,” he said this month. “Foreign intelligence services are looking for anyone with access to the information they want, whether classified or unclassified, including corporate trade secrets, intellectual property and other research.”

The Chinese Foreign Ministry did not respond to a request for comment.

The former Obama senior foreign policy official, speaking on the condition of anonymity for fear of jeopardizing future interactions related to China, described in interviews a monthslong recruitment effort by someone who appeared to be a Chinese spy.

In May 2017, five months after the official left his government job and just after he made a trip to China, someone called Robinson Zhang reached out via LinkedIn.

Mr. Zhang's profile photograph features the Hong Kong skyline, and he identifies as a public relations manager for a company called R&C Capital. In a message to the former official, Mr. Zhang described R&C as "an international consulting company based in Hong Kong" that specializes in "global investment, geopolitical issues, public policy, etc."

"I'm quite impressed by your CV and think you may be right for some opportunities, which are all well paid," Mr. Zhang wrote, according to screenshots of the exchanges.

The words struck him as strange, the former official said, so he asked Mr. Zhang for a website. Mr. Zhang directed him to a home page with an image of the Eiffel Tower but little information about R&C Capital. It appeared to be "something he made up on the fly," the former official said. (The New York Times viewed the site, which was deleted sometime after The Times emailed the company for an interview request.)

Mr. Zhang repeatedly indicated that his company could pay for a trip to China. The former official asked multiple times for more detail on the company but did not get any substantive responses.

In a message in August 2017, Mr. Zhang said that Zhejiang University had "already determined a candidate" for a conference on China's Belt and Road infrastructure projects before suggesting other opportunities — even though the two had not shared any earlier exchanges about this or any other event.

The former official referred Mr. Zhang to a speakers' agency representing him and has not heard from Mr. Zhang since.

Although the site for R&C Capital listed its address as No. 68 Mody Road in Hong Kong, there is no company by that name there. The company is also not included in the Hong Kong corporate registration database.

Mr. Parello-Plesner, the Danish official, had similar exchanges on LinkedIn with a user by the name of Grace Woo who contacted him in 2011.

Ms. Woo said she worked for DRHR, a headhunting company in Hangzhou, China. When she learned Mr. Parello-Plesner was visiting Beijing in 2012, she suggested he stop by Hangzhou to meet with the company. She asked for an image of his passport so she could make travel arrangements, but he declined.

Mr. Parello-Plesner agreed to meet in the St. Regis Hotel in Beijing. Ms. Woo never appeared, but a young man who said he was from DRHR guided Mr. Parello-Plesner to a conference room, where three middle-aged men welcomed him. They said they were from a government research organization, but they did not have business cards.

“I thought, ‘This meeting is very dodgy,’” Mr. Parello-Plesner said.

The men told Mr. Parello-Plesner they could fund his research if he worked with them, promising “‘really great access to the Chinese system,’” he said.

Mr. Parello-Plesner, suspecting the men were intelligence or security officials, reported the meeting to British officials when he returned to London, where he lived at the time.

“If I were LinkedIn, I would proactively do my homework now,” said Mr. Parello-Plesner, who has researched China’s foreign interference operations as a senior fellow at the Hudson Institute and wrote about his encounter last year. “This was just the tip of the iceberg.”

DRHR was one of three companies German domestic intelligence officials singled out in December 2017 as front organizations for Chinese agents. Those officials concluded that Chinese agents had used LinkedIn to try to contact 10,000 Germans, and LinkedIn shut down some accounts, including those of DRHR and Ms. Woo.

Last October, French intelligence agencies told the government that Chinese agents had used social networks — LinkedIn in particular — to try to contact 4,000 French individuals. Targets included government employees, scientists and company executives, according to Le Figaro, the French newspaper.

It can be hard to pinpoint the origins of the people behind fake social media accounts. The former Obama White House official and career diplomat, Brett Bruen, said a user by the name of Donna Alexander contacted him in 2017 on LinkedIn. Her profile says she is a research fellow at the California Institute of Technology, but the photograph is of an actress.

A spokeswoman for the university said it has no record of an employee by that name.

Ms. Alexander’s network on LinkedIn includes White House officials and former ambassadors, according to screenshots seen by The Times. “This person seems to have ingratiated herself with or gotten accepted by a lot of people in the foreign policy structure of U.S. government,” Mr. Bruen said.

At the same time, Western intelligence agencies are discovering another potential issue with LinkedIn — some of their operatives have no account there at all, which might raise questions about a person’s true identity among foreign officials or counterintelligence agents. Mr. Bruen said one European official told him that his country’s intelligence

agency was creating “the most boring LinkedIn profiles possible — a shallow cover so it doesn’t arouse suspicion.”

Cao Li contributed reporting from Hong Kong.

Edward Wong is a diplomatic and international correspondent who has reported for The Times for more than 20 years, 13 of those in Iraq and China. He received a Livingston Award for his Iraq War coverage and was on a team of Pulitzer Prize finalists. He has been a Nieman Fellow at Harvard and a Ferris Professor of Journalism at Princeton. @ewong