REPORT

Botched CIA Communications System Helped Blow Cover of Chinese Agents

The number of informants executed in the debacle is higher than initially thought.

BY ZACH DORFMAN | AUGUST 15, 2018, 5:13 PM

It was considered one of the CIA's worst failures in decades: Over a two-year period starting in late 2010, Chinese authorities systematically dismantled the agency's network of agents across the country, executing dozens of suspected U.S. spies. But since then, a question has loomed over the entire debacle.

How were the Chinese able to roll up the network?

Now, nearly eight years later, it appears that the agency botched the communication system it used to interact with its sources, according to five current and former intelligence officials. The CIA had imported the system from its Middle East operations, where the online environment was considerably less hazardous, and apparently underestimated China's ability to penetrate it.

"The attitude was that we've got this, we're untouchable," said one of the officials who, like the others, declined to be named discussing sensitive information. The former official described the attitude of those in the agency who worked on China at the time as "invincible."

Other factors played a role as well, including China's alleged recruitment of former CIA officer Jerry Chun Shing Lee around the same time. Federal prosecutors indicted Lee earlier this year in connection with the affair.

But the penetration of the communication system seems to account for the speed and accuracy with which Chinese authorities moved against the CIA's China-based assets.

"You could tell the Chinese weren't guessing. The Ministry of State Security [which handles both foreign intelligence and domestic security] were always pulling in the right people," one of the officials said.

"When things started going bad, they went bad fast."

The former officials also said the real number of CIA assets and those in their orbit executed by China during the two-year period was around 30, though some sources spoke of higher figures. The *New York Times*, which first reported the story last year, put the number at "more than a dozen." All the CIA assets detained by Chinese intelligence around this time were eventually killed, the former officials said.

The CIA, FBI, and National Security Agency declined to comment for this story. The Chinese Embassy in Washington did not respond to requests for comment.

At first, U.S. intelligence officials were "shellshocked," said one former official. Eventually, rescue operations were mounted, and several sources managed to make their way out of China.

One of the former officials said the last CIA case officer to have meetings with sources in China distributed large sums of cash to the agents who remained behind, hoping the money would help them flee.

When the intelligence breach became known, the CIA formed a special task force along with the FBI to figure out what went wrong. During the investigation, the task force identified three potential causes of the failure, the former officials said: A possible agent had provided Chinese authorities with information about the CIA asset network, some of the CIA's spy work had been sloppy and might have been detected by Chinese authorities, and the communications system had been compromised. The investigators concluded that a "confluence and combination of events" had wiped out the spy network, according to one of the former officials.

Eventually, U.S. counterintelligence officials identified Lee, the former CIA officer who had worked extensively in Beijing, as China's likely informant. Court documents suggest Lee was in contact with his handlers at the Ministry of State Security through at least 2011.

Chinese authorities paid Lee hundreds of thousands of dollars for his efforts, according to the documents. He was indicted in May of this year on a charge of conspiracy to commit espionage.

But Lee's alleged betrayal alone could not explain all the damage that occurred in China during 2011 and 2012, the former officials said. Information about sources is so highly compartmentalized that Lee would not have known their identities. That fact and

others reinforced the theory that China had managed to eavesdrop on the communications between agents and their CIA handlers.

When CIA officers begin working with a new source, they often use an interim covert communications system—in case the person turns out to be a double agent.

The communications system used in China during this period was internet-based and accessible from laptop or desktop computers, two of the former officials said.

This interim, or "throwaway," system, an encrypted digital program, allows for remote communication between an intelligence officer and a source, but it is also separated from the main communications system used with vetted sources, reducing the risk if an asset goes bad.

Although they used some of the same coding, the interim system and the main covert communication platform used in China at this time were supposed to be clearly separated. In theory, if the interim system were discovered or turned over to Chinese intelligence, people using the main system would still be protected—and there would be no way to trace the communication back to the CIA. But the CIA's interim system contained a technical error: It connected back architecturally to the CIA's main covert communications platform. When the compromise was suspected, the FBI and NSA both ran "penetration tests" to determine the security of the interim system. They found that cyber experts with access to the interim system could also access the broader covert communications system the agency was using to interact with its vetted sources, according to the former officials.

In the words of one of the former officials, the CIA had "fucked up the firewall" between the two systems.

U.S. intelligence officers were also able to identify digital links between the covert communications system and the U.S. government itself, according to one former official —links the Chinese agencies almost certainly found as well. These digital links would have made it relatively easy for China to deduce that the covert communications system was being used by the CIA. In fact, some of these links pointed back to parts of the CIA's own website, according to the former official.

The covert communications system used in China was first employed by U.S. security forces in war zones in the Middle East, where the security challenges and tactical objectives are different, the sources said. "It migrated to countries with sophisticated counterintelligence operations, like China," one of the officials said.

The system was not designed to withstand the scrutiny of a place like China, where the CIA faced a highly sophisticated intelligence service and a completely different online environment.

As part of China's Great Firewall, internet traffic there is watched closely, and unusual patterns are flagged. Even in 2010, online anonymity of any kind was proving increasingly difficult.

Once Chinese intelligence obtained access to the interim communications system,- penetrating the main system would have been relatively straightforward, according to the former intelligence officials. The window between the two systems may have only been open for a few months before the gap was closed, but the Chinese broke in during this period of vulnerability.

Precisely how the system was breached remains unclear. The Ministry of State Security might have run a double agent who was given the communication platform by his CIA handler. Another possibility is that Chinese authorities identified a U.S. agent—perhaps through information provided by Lee—and seized that person's computer. Alternatively, authorities might have identified the system through a pattern analysis of suspicious online activities.

China was so determined to crack the system that it had set up a special task force composed of members of the Ministry of State Security and the Chinese military's signals directorate (roughly equivalent to the NSA), one former official said.

Once one person was identified as a CIA asset, Chinese intelligence could then track the agent's meetings with handlers and unravel the entire network. (Some CIA assets whose identities became known to the Ministry of State Security were not active users of the communications system, the sources said.)

One of the former officials said the agency had "strong indications" that China shared its findings with Russia, where some CIA assets were using a similar covert communications system. Around the time the CIA's source network in China was being eviscerated, multiple sources in Russia suddenly severed their relationship with their CIA handlers, according to an NBC News report that aired in January—and confirmed by this former official.

The failure of the communications system has reignited a debate within the intelligence community about the merits of older, lower-tech methods for covert interactions with sources, according to the former officials.

There is an inherent paradox to covert communications systems, one of the former officials said: The easier a system is to use, the less secure it is.

The former officials said CIA officers operating in China since the debacle had reverted to older methods of communication, including interacting surreptitiously in person with sources. Such methods can be time-consuming and carry their own risks.

The disaster in China has led some officials to conclude that internet-based systems, even ones that employ sophisticated encryption, can never be counted on to shield assets.

"Will a system always stay encrypted, given the advances in technology? You're supposed to protect people forever," one of the former officials said.

Zach Dorfman is a senior fellow at the Carnegie Council for Ethics in International Affairs and an investigative journalist. Follow him on Twitter: @zachsdorfman.

TAGS: CHINA, CIA, ESPIONAGE, REPORT, UNITED STATES

VIEW COMMENTS