Behind the doors of a Chinese hacking company, a sordid culture fueled by influence, alcohol and sex

March 8 2024, by DAKE KANG and ZEN SOO

The interior of the I-Soon office, also known as Anxun in Mandarin, is seen after office hours in Chengdu in southwestern China's Sichuan Province on Feb. 20, 2024. Credit: AP Photo/Dake Kang, File

The hotel was spacious. It was upscale. It had a karaoke bar. The perfect venue, the CEO of the Chinese hacking company thought, to hold a Lunar New Year banquet currying favor with government officials. There was just one drawback, his top deputy said.

"Who goes there?" the deputy wrote. "The girls are so ugly."

So goes the sordid wheeling and dealing that takes place behind the scenes in China's hacking industry, as revealed in a highly unusual leak last month of internal documents from a private contractor linked to China's government and police. China's hacking industry, the documents reveal, suffers from shady business practices, disgruntlement over pay and work quality, and poor security protocols.

Private hacking contractors are companies that steal data from other countries to sell to the Chinese authorities. Over the past two decades, Chinese state security's demand for overseas intelligence has soared, giving rise to a vast network of these private hackers-for-hire companies that have infiltrated hundreds of systems outside China.

Though the existence of these hacking contractors is an open secret in China, little was known about how they operate. But the leaked documents from a firm called I-Soon have pulled back the curtain, revealing a seedy, sprawling industry where corners are cut and rules are murky and poorly enforced in the quest to make money.

Leaked chat records show I-Soon executives wooing officials over lavish dinners and late night binge drinking. They collude with competitors to rig bidding for government contracts. They pay thousands of dollars in "introduction fees" to contacts who bring them lucrative projects. I-Soon has not commented on the documents.

Mei Danowski, a cybersecurity analyst who wrote about I-Soon on her

blog, Natto Thoughts, said the documents show that China's hackers for hire work much like any other industry in China.

"It is profit-driven," Danowski said. "It is subject to China's business culture—who you know, who you dine and wine with, and who you are friends with."

Hacking that's styled as patriotic

China's hacking industry rose from the country's early hacker culture, first appearing in the 1990s as citizens bought computers and went online.

I-Soon's founder and CEO, Wu Haibo, was among them. Wu was a member of China's first hacktivist group, Green Army—a group known informally as the "Whampoa Academy" after a famed Chinese military school.

Wu and some other hackers distinguished themselves by declaring themselves "red hackers"—patriots who offered their services to the Chinese Communist Party, in contrast to the freewheeling, anarchist and anti-establishment ethos popular among many coders.

In 2010, Wu founded I-Soon in Shanghai. Interviews he gave to Chinese media depict a man determined to bolster his country's hacking capacity to catch up with rivals. In one 2011 interview, Wu lamented that China still lagged far behind the United States: "There are many technology enthusiasts in China, but there are very few enlightened people."

With the spread of the internet, China's hacking-for-hire industry boomed, emphasizing espionage and intellectual property theft.

High-profile hacks by Chinese state agents, including one at the U.S.

Office of Personnel Management where personal data on 22 million existing or prospective federal employees was stolen, got so serious that then-President Barack Obama personally complained to Chinese leader Xi Jinping. They agreed in 2015 to cut back on espionage.

For a couple of years, the intrusions subsided. But I-Soon and other private hacking outfits soon grew more active than ever, providing Chinese state security forces cover and deniability. I-Soon is "part of an ecosystem of contractors that has links to the Chinese patriotic hacking scene," said John Hultquist, chief analyst of Google's Mandiant cybersecurity unit.

These days, Chinese hackers are a formidable force.

In May 2023, Microsoft disclosed that a Chinese state-sponsored hacking group affiliated with China's People's Liberation Army called "Volt Typhoon" was targeting critical infrastructure such as telecommunications and ports in Guam, Hawaii, and elsewhere and could be laying the groundwork for disruption in the event of conflict.

Today, hackers such as those at I-Soon outnumber FBI cybersecurity staff by "at least 50 to one," FBI director Christopher Wray said January at a conference in Munich.

Documents reveal a seedy state-led industry

Though I-Soon boasted about its hacking prowess in slick marketing PowerPoint presentations, the real business took place at hotpot parties, late night drinking sessions and poaching wars with competitors, leaked records show. A picture emerges of a company enmeshed in a seedy, sprawling industry that relies heavily on connections to get things done.

I-Soon leadership discussed buying gifts and which officials liked red

wine. They swapped tips on who was a lightweight, and who could handle their liquor.

I-Soon executives paid "introduction fees" for lucrative projects, chat records show, including tens of thousands of RMB (thousands of dollars) to a man who landed them a 285,000 RMB ($40,000) contract with police in Hebei province. To sweeten the deal, I-Soon's chief operating officer, Chen Cheng, suggested arranging the man a drinking and karaoke session with women.

"He likes to touch girls," Chen wrote.

It wasn't just officials they courted. Competitors, too, were targets of wooing over late night drinking sessions. Some were partners—subcontractors or collaborators on government projects. Others were hated rivals who constantly poached their staff. Often, they were both.

One, Chinese cybersecurity giant Qi Anxin, was especially loathed, despite being one of I-Soon's key investors and business partners.

"Qi Anxin's HR is a green tea bitch who seduces our young men everywhere and has no morals," COO Chen wrote to Wu, the CEO, using a Chinese internet slur that refers to innocent-looking but ambitious young women.

I-Soon also has a complicated relationship with Chengdu 404, a competitor charged by the U.S. Department of Justice for hacking over 100 targets worldwide. They worked with 404 and drank with their executives but lagged on payments to the company and were eventually sued over a software development contract, Chinese court records show.

The source of the I-Soon documents is unclear, and executives and

Chinese police are investigating. And though Beijing has repeatedly denied involvement in offensive hacking, the leak illustrates I-Soon and other hacking companies' deep ties with the Chinese state.

For example, chat records show China's Ministry of Public Security gave companies access to proofs of concept of so-called "zero days", the industry term for a previously unknown software security hole. Zero days are prized because they can be exploited until detected. I-Soon company executives debated how to obtain them. They are regularly discovered at an annual Chinese state-sponsored hacking competition.

In other records, executives discussed sponsoring hacking competitions at Chinese universities to scout for new talent.

Many of I-Soon's clients were police in cities across China, a leaked contract list showed. I-Soon scouted for databases they thought would sell well with officers, such as Vietnamese traffic data to the southeast province of Yunnan, or data on exiled Tibetans to the Tibetan regional government.

At times, I-Soon hacked on demand. One chat shows two parties discussing a potential "long-term client" interested in data from several government offices related to an unspecified "prime minister."

A Chinese state body, the Chinese Academy of Sciences, also owns a small stake in I-Soon through a Tibetan investment fund, Chinese corporate records show.

I-Soon proclaimed their patriotism to win new business. Top executives discussed participating in China's poverty alleviation scheme—one of Chinese leader Xi Jinping's signature initiatives—to make connections. I-Soon CEO Wu suggested his COO become a member of Chengdu's People's Political Consultative Conference, a government advisory body

comprised of scientists, entrepreneurs, and other prominent members of society. And in interviews with state media, Wu quoted Mencius, a Chinese philosopher, casting himself as a scholar concerned with China's national interest.

But despite Wu's professed patriotism, leaked chat records tell a more complicated story. They depict a competitive man motivated to get rich.

"You can't be Lei Feng," Wu wrote in private messages, referring to a long-dead Communist worker held up in propaganda for generations as a paragon of selflessness. "If you don't make money, being famous is useless."

Lax security, poor pay among hacking workers

China's booming hackers-for-hire industry has been hit by the country's recent economic downturn, leading to thin profits, low pay and an exodus of talent, the leaked documents show.

I-Soon lost money and struggled with cash flow issues, falling behind on payments to subcontractors. In the past few years, the pandemic hit China's economy, causing police to pull back on spending that hurt I-Soon's bottom line. "The government has no money," I-Soon's COO wrote in 2020.

Staff are often poorly paid. In a salary document dated 2022, most staff on I-Soon's safety evaluation and software development teams were paid just 5,600 yuan ($915) to 9,000 yuan ($1,267) a month, with only a handful receiving more than that. In the documents, I-Soon officials acknowledged the low pay and worried about the company's reputation.

Low salaries and pay disparities caused employees to complain, chat records show. Leaked employee lists show most I-Soon staff held a

degree from a vocational training school, not an undergraduate degree, suggesting lower levels of education and training. Sales staff reported that clients were dissatisfied with the quality of I-Soon data, making it difficult to collect payments.

I-Soon is a fraction of China's hacking ecosystem. The country boasts world-class hackers, many employed by the Chinese military and other state institutions. But the company's troubles reflect broader issues in China's private hacking industry. The country's cratering economy, Beijing's tightening controls and the growing role of the state has led to an exodus of top hacking talent, four cybersecurity analysts and Chinese industry insiders told The Associated Press.

"China is no longer the country we used to know. A lot of highly skilled people have been leaving," said one industry insider, declining to be named to speak on a sensitive topic. Under Xi, the person added, the growing role of the state in China's technology industry has emphasized ideology over competence, impeded pay and made access to officials pivotal.

A major issue, people say, is that most Chinese officials lack the technical literacy to verify contractor claims. So hacking companies prioritize currying favor over delivering excellence.

In recent years, Beijing has heavily promoted China's tech industry and the use of technology in government, part of a broader strategy to facilitate the country's rise. But much of China's data and cybersecurity work has been contracted out to smaller subcontractors with novice programmers, leading to poor digital practices and large leaks of data.

Despite the clandestine nature of I-Soon's work, the company has surprisingly lax security protocols. I-Soon's offices in Chengdu, for example, have minimal security and are open to the public, despite

posters on the walls of its offices reminding employees that "to keep the country and the party's secrets is every citizen's required duty." The leaked files show that top I-Soon executives communicated frequently on WeChat, which lacks end-to-end encryption.

The documents do show that staff are screened for political reliability. One metric, for example, shows that I-Soon checks whether staff have any relatives overseas, while another shows that employees are classified according to whether they are members of China's ruling Communist Party.

Still, Danowski, the cybersecurity analyst, says many standards in China are often "just for show." But at the end of the day, she added, it may not matter.

"It's a little sloppy. The tools are not that impressive. But the Ministry of Public Security sees that you get the job done," she said of I-Soon. "They will hire whoever can get the job done."