Female spies are waging sex warfare to steal Silicon Valley secrets

China and Russia are sending attractive women to seduce tech workers — even marrying and having children with their targets. 'It's the Wild West out there,' says insider

Chinese and Russian operatives are using "sex warfare" to seduce and spy on Silicon Valley professionals, industry insiders have told The Times.

James Mulvenon, the chief intelligence officer of Pamir Consulting, which provides risk assessments for American companies investing in China, said he was one of the many men recently targeted by foreign seductresses hoping to gain access to US tech secrets. "I'm getting an enormous number of very sophisticated LinkedIn requests from the same type of attractive young Chinese woman," said Mulvenon. "It really seems to have ramped up recently."

Mulvenon also described how, at a business conference on Chinese investment risks hosted last week in Virginia, two attractive Chinese women showed up and attempted to gain entry. "We didn't let them in," he said. "But they had all the information [about the event] and everything else."

He added: "It is a phenomenon. And I will tell you: it is weird."

Mulvenon, who has investigated espionage in the US for 30 years, said the honeytrap tactic was "a real vulnerability" for the US "because we, by statute and by culture, do not do that. So they have an asymmetric advantage when it comes to sex warfare".

Sex warfare is just one way American tech workers are being played, according to five counterintelligence experts who spoke to The Times. China is also hosting competitions for startups on US soil to steal sensitive business plans, and even trying to sabotage American tech companies, sources said. In February, the House committee on homeland security warned that the Chinese Communist Party (CCP) has conducted more than 60 cases of espionage in the US over the past four years — though a former counterintelligence source fears this "only scratches the surface".

Both Russia and the CCP are using ordinary citizens — investors, crypto analysts, businessmen and academics — to target their American counterparts, rather than trained agents, making the espionage harder to spot. "We're not chasing a KGB agent in a smoky guesthouse in Germany anymore," said one senior US counterintelligence

official. “Our adversaries — particularly the Chinese — are using a whole-of-society approach to exploit all aspects of our technology and Western talent.”

• **The inside story of China spy case collapse: ‘It came from the very top’**

One former counterintelligence official, who now helps Silicon Valley founders divest their foreign investments, said he recently investigated the case of one “beautiful” Russian woman who worked at an aerospace company and married an American colleague. He discovered that she had gone to a modelling academy in her twenties but later attended a “Russian soft-power school” before disappearing for a decade and re-emerging in the US as a cryptocurrency expert.

“But she doesn’t stay in crypto,” the ex-official said. “She is trying to get to the heights of the military-space innovation community. The husband’s totally oblivious.”

“Showing up, marrying a target, having kids with a target — and conducting a lifelong collection operation, it’s very uncomfortable to think about but it’s so prevalent,” he continued. “If I wanted to be out of the shadows, I’d write a book on it.”

The theft of trade secrets is estimated to cost the American taxpayer up to $600 billion a year, with China identified as the principal source of this loss, according to the Commission on the Theft of American Intellectual Property.

In 2023 Klaus Pflugbeil, a resident of Ningbo, China, tried to sell intellectual property he had stolen from Tesla to undercover agents at a Las Vegas trade conference for $15 million. He was sentenced to 24 months in prison last December; his alleged accomplice, Yilong Shao, who also lived in Ningbo, remains on the run. (Shao has not publicly commented on the case.)

The men, both former employees of a Canadian manufacturing company that was acquired by Tesla in 2019, were said to have used the stolen trade secrets to build a rival business in China. Pflugbeil told Shao that he had “a lot of original documents” related to Tesla’s battery technology and sought out more “original drawings” of the trade secrets, prosecutors said.

The assistant attorney-general for national security, Matthew Olsen, said in a statement in December: “In stealing trade secrets from an American electric-vehicle manufacturer to use in his own China-based company, Pflugbeil’s actions stood to benefit the PRC [People’s Republic of China] in a critical industry with national security implications.”

Meanwhile the US government has warned startups against entering international “pitch competitions” where founders pitch their business ideas to Chinese investors. Winners

can receive cash awards, subsidies and investment — on the condition that they bring their IP to China and set up an operation in the country.

Some of the competitions ask startups to share their business strategies, intellectual property and even personal data and photos before participating, US officials said in a warning issued last month.

“Part of it is a counterintelligence risk. They’re looking at how they can exploit you later,” the senior US counterintelligence official said. “And part of it is they may simply take your idea, exploit it and patent it, stealing your financial future.”

Academics and younger innovators eager to develop their ideas and establish a lucrative business are especially susceptible to exploitation, the official added. One contest that has officials concerned is the ninth annual China (Shenzhen) Innovation and Entrepreneurship International Competition, held this month in several cities across the world including Boston, London and Tokyo. Winners are expected to form a business in China in order to receive cash awards and investment.

The China (Shenzhen) Innovation and Entrepreneurship International Competition has concerned national security officials

ITCSZ

One chief executive of a Silicon Valley biotech firm who attended last year’s competition in November said he had been made to wear a microphone throughout the event and was followed around by officials.

“They would record everything I would say, do and then ask questions like a reporter would: ‘What do we do? How do we do it?’” he said. He added that there were “government representatives in the back observing the competition”.

His company won one of the prizes on offer, taking home $50,000. He said there were no conditions attached to this money, but he was surprised that organisers wired the funds to his personal account rather than his company’s. “That was weird,” he added.

He now thinks that participating in the contest put a target on his back with US officials. Earlier this year the US government paused federal funding to his company, forcing him to dissolve the operation. He suspects it happened “because we disclosed to them that we do have some Asian investors”, he said.

This is a deliberate tactic, Mulvenon warned. He said it was common for China-backed venture capitalists to target US startups initially funded by the Department of Defence (DoD) and then later make investments in those firms. “The percentage of foreign ownership crosses a threshold so the DoD can’t make any more investments in those companies, denying the government access to innovative startups and IP,” said Mulvenon, who is investigating this phenomenon. “It’s the latest iteration of the Chinese gameplay. I call it ‘drafting’.”

Xi Jinping’s ruling CCP is said to be targeting startups which have received US investment

LI GANG/XINHUA/ALAMY

In May the Senate committee on small business and entrepreneurship found that six of the 25 largest recipients of federal funding via the Small Business Innovation Research programme had “clear links” to China — but still received nearly $180 million from the Pentagon in 2023 and 2024.

Jeff Stoff, a security academic and former China and national security analyst for the US government, said that a lot of what China was doing was not illegal. Rather, they were taking advantage of America’s corporate vulnerabilities using regulatory blind spots.

“The Chinese understand our system and they know how to work within it with virtual impunity — most of the time,” said Stoff.

For now, all America’s counterintelligence community can do is play catch-up. That means spending more on combating corporate espionage, heightening scrutiny of “cross-border” funds and raising awareness of the Russian and Chinese threat in Silicon Valley.

“It’s the Wild West out there,” said Stoff. “China is targeting our startups, our academic institutions, our innovators, our DoD-funded research projects. But there’s not enough oversight and action. It’s all intertwined as part of China’s economic warfare strategy, and we’ve not even entered the battlefield.”