POLITICO

THE FRIDAY COVER

How Silicon Valley Became a Den of Spies

July 27, 2018

Politico illustration/iStock/Wikipeida | Politico Illustration / iStock / Wikipedia

SAN FRANCISCO—In the fall of 1989, during the Cold War's wan and washed-out final months, the Berlin Wall was crumbling—and so was San Francisco. The powerful Loma Prieta earthquake, the most destructive to hit the region in more than 80 years, felled entire apartment buildings. Freeway overpasses shuddered and collapsed, swallowing cars like a sandpit. Sixty-three people were killed and thousands injured. And local Soviet spies, just like many other denizens of the Bay Area, applied for their share of the nearly $3.5 billion in relief funds allocated by President George H.W. Bush.

FBI counterintelligence saw an opening, recalled Rick Smith, who worked on the Bureau's San Francisco-based Soviet squad from 1972 to 1992. When they discovered that a known

Soviet spy, operating under diplomatic cover, had filed a claim, Smith and several other bureau officials posed as federal employees disbursing relief funds to meet with the spy. The goal was to compromise him with repeated payments, then to turn him. “We can offer your full claim,” Smith told the man. “Come meet us again.” He agreed.

But the second time, the suspected intel officer wasn’t alone. FBI surveillance teams reported that he was being accompanied by a Russian diplomat known to the FBI as the head of Soviet counterintelligence in San Francisco. The operation, Smith knew, was over—the presence of the Soviet spy boss meant that the FBI’s target had reported the meeting to his superiors—but they had to go through with the meeting anyway. The two Soviet intelligence operatives walked into the office room. The undercover FBI agents, who knew the whole affair had turned farcical, greeted the Soviet counterintelligence chief.

“What,” he replied, “You didn’t expect me to come?”

We tend to think of espionage in the United States as an East Coast phenomenon: shadowy foreign spies working out of embassies in Washington, or at missions to the United Nations in New York; dead drops in suburban Virginia woodlands, and surreptitious meetings on park benches in Manhattan’s gray dusk.

But foreign spies have been showing up uninvited to San Francisco and Silicon Valley for a very long time. According to former U.S. intelligence officials, that’s true today more than ever. In fact, they warn—especially because of increasing Russian and Chinese aggressiveness, and the local concentration of world-leading science and technology firms—there’s a full-on epidemic of espionage on the West Coast right now. And even more worrisome, many of its targets are unprepared to deal with the growing threat.

Unlike on the East Coast, foreign intel operations here aren’t as focused on the hunt for diplomatic secrets, political intelligence or war plans. The open, experimental, cosmopolitan work and business culture of Silicon Valley in particular has encouraged a newer, “softer,” “nontraditional” type of espionage, said former intelligence officials—efforts that mostly target trade secrets and technology. “It’s a very subtle form of intelligence collection that is more business connected and oriented,” one told me. But this economic espionage is also ubiquitous. Spies “are very much part of the everyday environment” here, said this person. Another former intelligence official told me that, at one point recently, a full 20 percent of all the FBI’s active counterintelligence-related intellectual property cases had originated in the Bay Area. (The FBI declined to comment for this story.)

Political espionage happens here, too. China, for example, is certainly out to steal U.S. technology secrets, noted former intelligence officials, but it also is heavily invested in traditional political intelligence gathering, influence and perception-management operations in California. Former intelligence officials told me that Chinese intelligence once recruited a staff member at a California office of U.S. Senator Dianne Feinstein, and the source reported back to China about local politics. (A spokesperson for Feinstein said the office doesn't comment on personnel matters or investigations, but noted that no Feinstein staffer in California has ever had a security clearance.) At the Aspen Security Forum last week, FBI director Chris Wray acknowledged the threat Chinese spying in particular poses, saying, "China from a counterintelligence perspective represents the broadest, most pervasive, most threatening challenge we face as a country."

Making it even more complicated, said multiple former U.S. intel officials, many foreign intel "collectors" in the Bay Area are not spies in the traditional sense of the term. They aren't based out of embassies or consulates, and may be associated with a state-owned business or research institute rather than an intelligence agency. Chinese officials, in particular, often cajole or outright threaten Chinese nationals (or U.S. citizens with family members in China) working or studying locally to provide them with valuable technological information.

"You get into situations where you have really good, really bright, conscientious people, twisted by their home government," said a chief security officer at a major cloud storage company that maintains sensitive government contracts. U.S.-based Chinese employees of this company have had Chinese government officials attempt to "leverage" these individuals' family members in China, this person told me. The company now requires employees working on certain projects to be U.S. citizens.

> "As Silicon Valley continues to take over the world, the local spy war will only get hotter–and the consequences will resonate far beyond Northern California.

And yet, it's not clear that the Bay Area—historically famous for its liberalism, and now infamous for its madcap capitalism—is prepared to handle this escalation and these new tactics. Tech firms, especially start-ups, lack incentives to report potential espionage to U.S. officials; and businesses and universities are often ignorant about the espionage threat, or

so attuned to local political sensitivities they may fear being accused of stereotyping if they attempt to institute more stringent defensive security and screening measures.

As Silicon Valley continues to take over the world, the local spy war will only get hotter—and the consequences will resonate far beyond Northern California. This story is based on extensive conversations with more than half a dozen former intelligence community officials with direct knowledge of, or experience with, U.S. counterintelligence activities in the Bay Area. All requested anonymity to discuss sensitive matters more openly. A few other individuals, all of whom worked counterintelligence in the Bay Area from the early 1970s through the mid-2000s, agreed to be interviewed on the record.

As one former senior intelligence official put it: "San Francisco is a trailblazer—you see the changes there in foreign counterintelligence first. Trends emerge there." If we want to understand a world where Russia and China are ramping up their spy games against the United States, then we need to pay attention to what's happening in San Francisco.

***

Russian intelligence has had an intensive interest in San Francisco stretching back to the beginning of the Cold War. In those days, the Russians were primarily gathering information on local military installations, said former officials, including the Presidio, the strategically located former military base set on a wind-swept northern tip of the San Francisco peninsula, overlooking the Golden Gate Bridge.

Since then, Russian operations have become bolder, with one notable exception: the immediate post-Cold War period. "The only time there was a collective sigh regarding Russia, like maybe things have changed, was under Gorbachev," said LaRae Quy, who worked on Russian and Chinese counterintelligence in the Bay Area from 1985 to 2002. "We even put in a big 'Going Out Of Business' sign in the Palo Alto squad room."

But this optimism quickly faded when Putin was elected in 2000, recalled Quy, who retired in 2006. "Russia has been steadily escalating since then."

As the Bay Area transformed itself into a tech hub, Russia adapted its efforts accordingly, with Russian spies increasingly focused on obtaining information on valuable, sensitive or potentially dual-use technologies—those with both civilian and military applications—being developed or financed by companies or venture-capital firms based in the region. Russia's espionage activities have traditionally been centered on its San Francisco Consulate, which was forcibly closed by the Trump administration in early September 2017.

But even with the consulate shuttered, there are alternative vehicles for Russian intelligence-gathering in Silicon Valley. One potential mechanism, said three former intelligence officials, is Rusnano USA, the sole U.S. subsidiary of Rusnano, a Russian government-owned venture capital firm primarily focused on nanotechnology. Rusnano USA, which was founded in 2011, is located in Menlo Park, near Stanford University. "Some of the [potential intelligence-gathering] activities Rusnano USA was involved in were not only related to the acquisition of technology, but also inserting people into venture capital groups, in developing those relationships in Silicon Valley that allowed them to get their tentacles into everything," one former intelligence official told me. "And Rusnano USA was kind of the mechanism for that."

Rusnano's interests, said this former official, have extended to technology with both civilian and potential military applications. U.S. intelligence officials were very concerned about contacts between Rusnano USA employees and suspected Russian intelligence officers based at Russia's San Francisco Consulate and elsewhere, this person said. "The Russians treated [Rusnano USA] as an intelligence platform, from which they launched operations," said another former U.S. intelligence official. (Rusnano USA and the Russian Embassy in Washington, did not respond to requests for comment.)

Russia also employs older, tried-and-true methods locally. Intel officials have suspected that Russian spies were enlisting local high-end Russian and Eastern European prostitutes, in a classic Russian "honeypot" maneuver, to gather information from (and on) Bay Area tech and venture-capital executives. Sex workers targeting executives at high-end bars and nightclubs such as the Rosewood Sand Hill, an ultra-luxury hotel located near many of Silicon Valley's top financial firms—infamous for its raucous, hook-up oriented Thursday nights—the Redwood Room, a tony bar located in the Clift Hotel in downtown San Francisco, and other spots have been identified as potentially reporting back to Russian intel officers, said another former official. "If I were a Russian intelligence officer, and I knew that these high-end girls were dragging CEOs of major companies back to their rooms, I'd be paying them for info too," said this person. "It's that whole idea of concentric rings: You don't need to be on the inside, you just need somebody on the inside that you have access to."

***

Russia's interference in the 2016 presidential election has given Putin's regime an outsized role in the national conversation on espionage. But talk to former intel officials, and many will say that China poses an equal, if not greater, long-term threat. "The Chinese just have *vast* resources," said Kathleen Puckett, who worked counterintelligence in the

Bay Area from 1979 to 2007. “They have all the time in the world, and all the patience in the world. Which is what you need more than anything.” (China's Embassy in Washington, did not respond to requests for comment.)

Because of California’s economic and political importance, as well as its large, well-established, and influential émigré and Chinese-American communities, the People’s Republic places great weight on its intelligence activities here, said multiple former intelligence officials. Indeed, two told me that California is the only U.S. state to which the Ministry of State Security—China’s main foreign intelligence agency—has had a dedicated unit, focused on political intelligence and influence operations. (China has had a similar unit for Washington.)

And if California is elevated among Chinese interests, San Francisco is like “nirvana” to the MSS, said one former official, because of the potential to target community leaders and local politicians who may later become mayors, governors or congressmen. Their efforts are becoming increasingly sophisticated.

Sometimes these recruitment efforts have been successful. According to four former intelligence officials, in the 2000s, a staffer in Senator Dianne Feinstein’s San Francisco field office was reporting back to the MSS. While this person, who was a liaison to the local Chinese community, was fired, charges were never filed against him. (One former official reasoned this was because the staffer was providing political intelligence and not classified information—making prosecution far more difficult.) The suspected informant was “run” by officials based at China’s San Francisco Consulate, said another former intelligence official. The spy’s handler “probably got an award back in China” for his work, noted this former official, dryly.

Or take the case of Rose Pak. Pak, who died in September 2016, was for decades one of San Francisco’s preeminent political power brokers. Though she never held elective office, she was famous for making and unmaking mayors, city councilmen (or “supervisors,” as they’re known in San Francisco), and pushing city contracts to her allies and constituents in Chinatown.

According to four former intelligence officials, there were widespread concerns that Pak had been co-opted by Chinese intelligence, and was wielding influence over San Francisco politics in ways purposefully beneficial to the Chinese government. Another worry, U.S. officials said, was Pak’s role in organizing numerous junkets to China, sometimes led by Pak in person and attended (often multiple times) by many prominent Bay Area politicians, including former San Francisco Mayor Ed Lee, who died while in office in 2017. Political

junkets are used by Chinese intelligence for surveillance ("every single hotel room is bugged," one former official told me) and collection purposes, as well as for spotting and assessing potential recruits, said former intel officials. (There is no indication that Pak herself participated in, or had knowledge of, specific intelligence-gathering efforts.) Concerns about Pak's links to the Chinese Communist Party occasionally percolated into local political debate, but the intelligence community's identification of Pak as a likely agent of influence for Beijing is being reported here for the first time.

Occasionally, Chinese intelligence activities in San Francisco burst into plain view. Consider the story—and it is an incredible one, also told here for the first time—of the 2008 Olympic Torch Run. San Francisco was the only U.S. city to host the Olympic torch as it made its way, tortuously, to Beijing. And Chinese officials were very concerned about disruptions to the run by protesters, as well as in managing the image China projected to the rest of the world in the run-up to the games.

So they decided to leave nothing to chance. According to three former intelligence officials, Chinese MSS and Ministry of Public Security (MPS) officers flew in to San Francisco from abroad for the occasion, joining suspected MSS officers based in the Bay Area. (At the time, the diplomat responsible for Overseas Chinese Affairs at China's San Francisco Consulate was a suspected MSS officer, said two of these former officials.) U.S. officials watched as Chinese intelligence officers filmed Tibetan monks on their march across the Golden Gate Bridge, and known Chinese spies surveilled a pro-Tibet rally downtown featuring Desmond Tutu and Richard Gere. Chinese spies also recorded participants in a Falun Gong rally in Union Square, and shot footage of protestors at the torch run itself.

Most brazenly, said former intelligence agents, Chinese officials bussed in 6,000-8,000 J-Visa holding students—threatening them with the loss of Chinese government funding—from across California to disrupt Falun Gong, Tibetan, Uighur and pro-democracy protesters. (They even provided these students with a box lunch.) "I'm not sure they would have pulled out these stops in any other city, but San Francisco is special" to China, said a former senior U.S. official.

Counterintelligence officers possessed advance knowledge about some aspects of this operation and observed Chinese intelligence officers, who often wore earpieces connected to a radio, managing the movements of counterprotesters, directing blocs of pro-PRC students to intimidate, disrupt and overwhelm anti-Beijing protesters across the parade route. Chinese intelligence officers would "communicate with each other, and say, 'We've got three Tibetan monks about to do a reading on Pier 39—I need you to move bloc A and

bloc B to that location so we can drown them out,'" recalled another former official. "So they'd move these groups around to prevent any protests along the Embarcadero."

"We got pissed off," said the same former intelligence official, because the Chinese "were interfering with the free expression of opinion" at the torch relay—their operation was, in essence, an effort by a hostile foreign intelligence service to forcibly suppress First Amendment activities in a major American city.

Disagreements between the FBI and the State Department, which counseled a more restrained approach, prevented U.S. intelligence personnel from interfering directly in Chinese activities during the torch run itself, said this former intel official. (The State Department said it does not comment on intelligence matters.) The same source noted that U.S. intelligence officials did, however, pass information about the torch run to their Australian counterparts—the torch was later scheduled to pass through Canberra—which denied visas to some of the Chinese intelligence officers responsible for the melee in San Francisco.

Chinese intelligence has long focused on surveilling, and attempting to control, Chinese nationals studying abroad. One well-documented mechanism for this effort has been the use of Chinese Students and Scholars Associations groups on university campuses. The connectivity between individual campus CSSAs and local Chinese diplomatic facilities varies. Some groups are unreceptive to the intercession or influence of Chinese government officials, but many consider themselves to be under the direct "guidance" of their local consulate or embassy, receiving funds from these institutions. "Intelligence officers in diplomatic facilities are the primary point of contact for students in CSSAs," said one former official.

But some of these links between these student groups and Chinese officials are covert, and even coercive. In one case in the mid-2000s in the Midwest, a student affiliated with a CSSA reported another Chinese student's contact with the FBI to an MSS officer operating under diplomatic cover in Chicago, said a former intelligence official. The student was quickly flown out of the country. And, roughly half a decade ago in the Bay Area, counterintelligence officials believed that a graduate student affiliated with the Berkeley CSSA was working for the MSS, and reporting on the activities of other Chinese students on campus, said another former official.

***

When it comes to economic espionage in particular, Chinese intelligence employs a more decentralized strategy than Russia does, former intelligence officials told me. China draws from a much larger population pool to achieve its objectives—using opportunistic businessmen, ardent nationalists, students, travelers and others alike. One former intelligence official likened China's approach to an "Oklahoma land rush"—an attempt to grab as much targeted proprietary technology or IP as possible, as quickly as possible, through as many channels as possible.

Chinese intelligence also undertakes very intentional efforts to recruit insiders placed within organizations whose technologies they are interested in, said the same former intelligence official. "They are very good at softly recruiting people, and taking advantage of vulnerabilities"—including via threats—"and they are very patient in putting different parts of it together. We've seen them repeatedly save money and time that the U.S. spends on research and development."

The July 2018 arrest of Silicon Valley-based Apple employee Xiaolang Zhang, who allegedly stole proprietary information about Apple's self-driving car program to benefit his new employer, a China-based competitor, appears to fit this pattern. (Zhang was charged with theft of trade secrets and has not been accused of any espionage-related crimes. He maintains his innocence.)

> "China "[puts] all their efforts into espionage, and get everything for free," said Kathleen Puckett, a former longtime counterintelligence officer in the Bay Area.

The case of Walter Liew, a Bay Area local who was found guilty in 2014 of selling a highly valuable proprietary pigmentation formula owned by DuPont to a state-owned Chinese conglomerate, is a clearer example.

Liew was found guilty of violating the Economic Espionage Act, a landmark 1996 federal law that strengthened penalties for trade theft benefiting a foreign government. San Francisco has played an outsized role in cases involving this law. In fact, the first conviction under the act occurred in San Francisco, in 2006; as did the first sentencing under the law, in 2008; as did the first jury conviction—of Liew himself—in 2014. All three cases involved China.

The Chinese have pursued this strategy “brilliantly” for years, said Puckett. “They put all their efforts into espionage, and get everything for free.”

Chinese cyberespionage operations have also targeted a number of Silicon Valley-based technology giants. During a number of attacks, two former intelligence officials told me, Chinese intelligence immediately sought the files of U.S. companies’ legal counsel or other legal documentation, to access Foreign Intelligence Surveillance Act warrants or National Security Letters previously issued to these institutions. In other words, the paramount Chinese interest was finding out the extent of the U.S. officials’ knowledge about China’s own intelligence operatives—and in adjusting their behavior accordingly. “If in fact the person in question was Chinese intelligence,” said this former official, “they could then alter their approach.” This strategy began being observed during a hack of Google, said two former officials, that occurred about a decade ago.

While China and Russia demand the lion’s share of counterintelligence resources in the Bay Area, a number of friendly intelligence services are also active in Silicon Valley, said former intelligence officials. South Korea, according to one, has become “formidable” in the realm of economic espionage, with particular sophistication in cyberespionage. U.S. officials have had to issue “stern warnings” to South Korea to “stop hacking” within the United States, said this person. (The South Korean Embassy in Washington, D.C., did not respond to requests for comment.)

Israel is also active in the Bay Area—but it’s complicated. According to one former intelligence official, Israel has “a culture that facilitates and encourages acquisition of targeted companies”—in other words, it will use information it has gathered locally to cajole or incentivize private Israeli firms to purchase specific start-ups or other Silicon Valley-based tech companies. Throughout the 2000s, said former officials, French intelligence employed a similar strategy.

In an email response, a spokesperson for the Israeli Embassy in Washington, D.C., wrote that “the allegations are totally untrue and downright ridiculous. Israel does not conduct espionage in the United States.” A spokesperson for the French Embassy declined to comment.

There is disagreement, however, within the U.S. intelligence community about the amount of resources that should be devoted to what is, in essence, a “soft” form of spying by U.S. allies. “I get they try to get advantages from economic espionage,” said another former senior intelligence official, “but is French espionage worth that much emotional discharge, given what the Russians are up to?”

***

There's another big challenge to doing counterintelligence work in the Bay Area, say these officials: getting the cooperation of local private-sector actors, especially in tech. Indeed, said former intelligence officials, not only do many cases of economic espionage not reach the prosecution stage here, they often go unreported entirely.

This has been a longstanding source of friction in the Valley. "The biggest problem we had —really, seriously—with a lot of these companies is that they wouldn't prosecute," said Larae Quy, the former Palo Alto-based FBI counterintelligence agent who retired in 2006. "They would have an employee sell technology to, say, the Russians or the Chinese, and rather than let their stockholders or investors know about it, they just let it walk. So, we've caught the guy, or we have information and we'd like to take it to the next level, and they don't want to push it because of the bad press that gets out. It's the most frustrating thing in the world."

Silicon Valley firms continue to downplay, or outright conceal, the extent to which the theft of trade secrets and other acts of economic espionage occur, said multiple former officials. "Coming forward and saying you didn't have controls in place—that totally impacts shareholder or investor value," noted one former intelligence official. "Especially when you're dealing with startups or mid-level companies that are looking for funding, that's a big deal. You're basically announcing to the world, especially if you're potentially going forward with a public trial, that you were not able to protect your information."

The open, start-up culture in the Bay Area has also complicated U.S. counterintelligence efforts, said former officials, because Russian and Chinese operatives have an easier time infiltrating organizations without any security systems or hierarchies in place. These services like penetrating young companies and start-ups, noted one former official, because "it's always better to get in at the ground floor" when seeking to pilfer valuable information or technology.

The exorbitant cost of living in Silicon Valley, however, means that opportunities for tech employees—and potential spies or co-optees—to "get in at the ground floor" are becoming increasingly uncommon. The tech industry, chasing talent and lower overhead, is now spread more widely across the country than ever before. And this diffusion will create new vulnerabilities. Consequently, places like Chapel Hill, North Carolina and Boulder, Colorado—both midsized cities with thriving tech industries—will likely see an uptick in counterintelligence cases. (One former intelligence official noted that the FBI's office in Austin, Texas, has built up its counterintelligence capacities.)

But spies will never leave Silicon Valley. As the region's global clout grows, so will its magnet-like attraction for the world's spooks. As one former U.S. intelligence official put it, spies are pulled toward the Bay Area "like moths to the light." And the region will help define the struggle for global preeminence—especially between the United States and China—for decades to come.