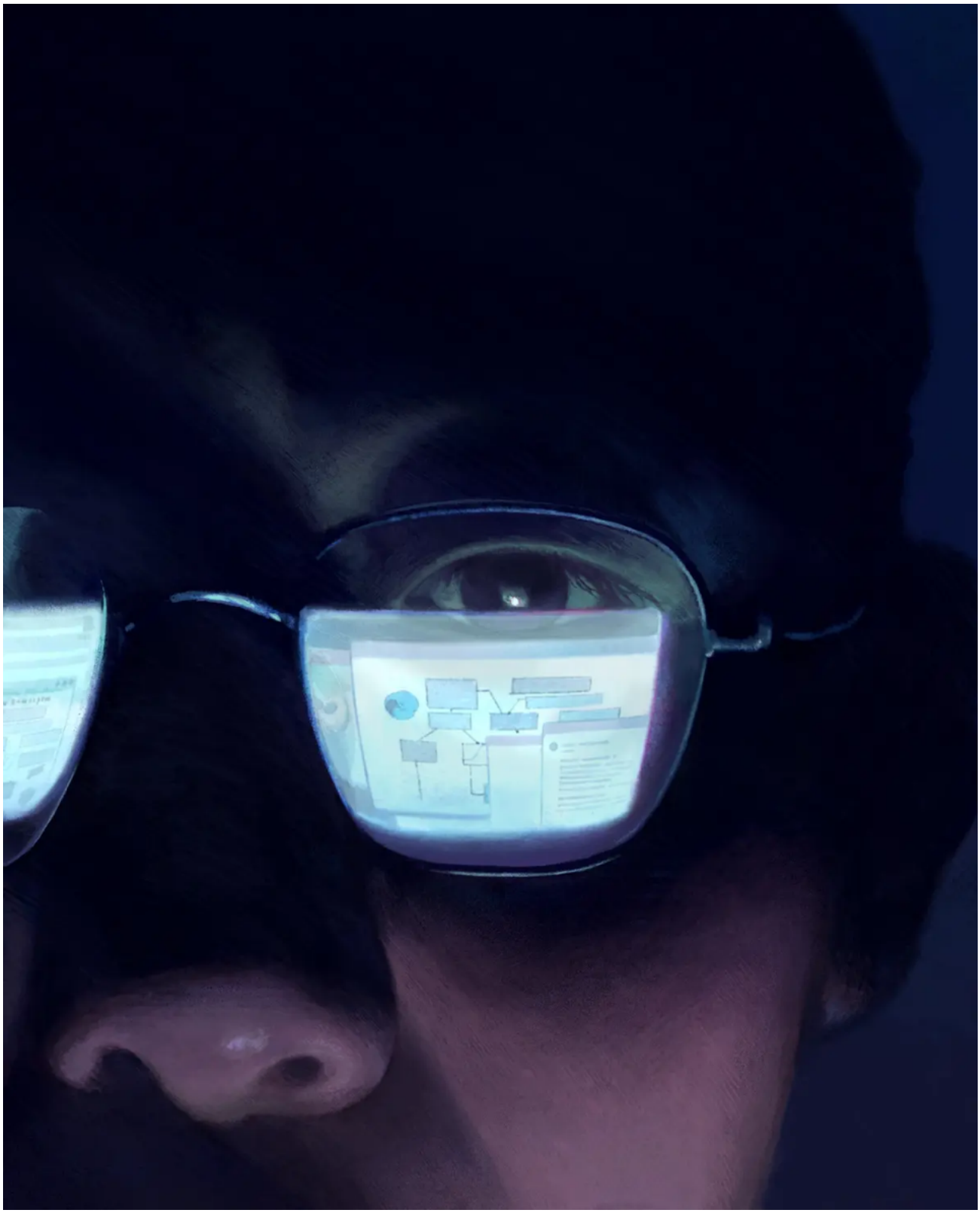
The Daring Ruse That Exposed China's Campaign to Steal American Secrets

How the downfall of one intelligence agent revealed the astonishing depth of Chinese industrial espionage.

Published March 7, 2023Updated March 8, 2023, 11:19 a.m. ET



Illustrations by Hokyoung Kim

Illustrations by Hokyoung Kim

Listen to This Article

Audio Recording by Audm

To hear more audio stories from publications like The New York Times, download Audm for iPhone or Android.

In March 2017, an engineer at G.E. Aviation in Cincinnati whom I will refer to using part of his Chinese given name — received a request on LinkedIn. Hua is in his 40s, tall and athletic, with a boyish face that makes him look a decade younger. He moved to the United States from China in 2003 for graduate studies in structural engineering. After earning his Ph.D. in 2007, he went to work for G.E., first at the company's research facility in Niskayuna, N.Y., for a few years, then at G.E. Aviation.

The LinkedIn request came from Chen Feng, a school official at the Nanjing University of Aeronautics and Astronautics (N.U.A.A.), in eastern China. Like most people who use LinkedIn, Hua was accustomed to connecting with professionals on the site whom he didn't know personally, so the request did not strike him as unusual. "I didn't even think much about it before accepting," Hua told me. Days later, Chen sent him an email inviting him to N.U.A.A. to give a research presentation.

Hua had always desired academic recognition. "When I did my Ph.D., I initially wanted to be a professor in China or in the United States," he says. But because his studies were focused more on practical applications than pure research, a career in industry made more sense than one in academia. At G.E. Aviation, he was part of a group that designed containment cases for the rotating fan blades of jet engines. The use of carbon-based composites in fan blades and their casings, instead of metal, means lighter engines and a commercial advantage.

"I felt honored to be invited to give a talk," Hua says. Being recognized back

home was especially fulfilling for Hua, who grew up poor in a small village and was the only child there from his generation to go to college. Beyond the prestige, the invitation also provided a free trip to China to see his friends and family. Hua arranged to arrive in May, so he could attend a nephew's wedding and his college reunion at Harbin Institute of Technology. There was one problem, though: Hua knew that G.E. would deny permission to give the talk if he asked, which he was supposed to do. "Since G.E. is a high-tech company, it is difficult to get approval even to present at conferences in the United States," he says. The company was concerned about giving away proprietary information.

Hua made it clear to Chen that he would be able to discuss only research on composite materials generally, without going into the specifics of what he did at G.E. Aviation. To prepare, Hua told me, he went back over the work he had done for his doctorate and gathered additional information from scientific papers. He also downloaded a few G.E. training files onto his laptop. These contained instructions from G.E. experts on using composites; Hua thought they would help him save time when putting together his presentation, which he planned to do on his flight.

After he landed in China, Hua took a high-speed train from Beijing to Nanjing, where Chen drove him to a hotel on the Nanjing University campus. The next morning, Chen and Hua went to a meeting with a man who was introduced as Qu Hui, deputy director of the Jiangsu Provincial Association for International Science and Technology Development. Qu gave Hua a welcome gift: loose Chinese tea nicely packaged in a gift box. "I accepted it as an honor," Hua says. "I've liked drinking tea since I was a kid."

A few dozen students and faculty members attended Hua's talk. They asked several questions that Hua was happy to answer. "I remember one student asked specifically about the architecture of the material I was talking about

in my presentation," he says. "I said: This is G.E. proprietary information. I am just using this picture as an example, but I cannot share the details of what we are designing or using."

After the presentation, Chen handed Hua an envelope filled with $3,500 in U.S. dollars — reimbursement for his plane ticket and an honorarium for the talk. Then they went to dinner with Qu and a couple of professors. That night, Hua took a train back to Shanghai; the next day, he flew back to the United States. Once home, he realized he had forgotten to delete his presentation from the computer at the university auditorium in Nanjing. He was concerned because the slides included some pictures with G.E.'s logo. "So," Hua told me, "I emailed one of the students and said, Hey, can you delete the presentation?" He thought that would be the end of the matter.

The images of a Chinese spy balloon drifting through American airspace last month before being shot down by a fighter jet off the coast of South Carolina were a conspicuous reminder of the escalating geopolitical antagonisms between the United States and China. Although world powers spying on each other is hardly unusual, the impunity with which the Chinese were apparently conducting surveillance over U.S. military sites alarmed many. The U.S. House of Representatives passed a resolution condemning China's "brazen violation of United States sovereignty" in deploying the balloon, which was fitted with antennas capable of collecting signals intelligence; the Chinese government condemned its downing as an overreaction. The incident — reminiscent of Cold War confrontations — inflamed tensions between two countries already locked in a race for military, technological and economic supremacy.

The spy balloon's flight over U.S. territory was a very public display of China's intelligence gathering, but the Chinese government has for decades been conducting a much less visible and possibly more damaging campaign

to steal American trade secrets and intellectual property. While weapons and military equipment have always been a focus — Chinese agents and civilians have been implicated in the theft or illicit transfer of various military technologies, including those related to radar, fighter jets, submarines and weapons systems — China's espionage expanded in the 1980s and beyond to also target commercial technologies as diverse as pesticides, rice seeds, robotic cars and wind turbines.

Although China publicly denies engaging in economic espionage, Chinese officials will indirectly acknowledge behind closed doors that the theft of intellectual property from overseas is state policy. James Lewis, a former diplomat now at the Center for Strategic and International Studies in Washington, recalls participating in a meeting in 2014 or so at which Chinese and American government representatives, including an officer from the People's Liberation Army, discussed the subject. "An assistant secretary from the U.S. Department of Defense was explaining: Look, spying is OK — we spy, you spy, everybody spies, but it's for political and military purposes," Lewis recounted for me. "It's for national security. What we object to is your economic espionage. And a senior P.L.A. colonel said: Well, wait. We don't draw the line between national security and economic espionage the way you do. Anything that builds our economy is good for our national security." The U.S. government's response increasingly appears to be a mirror image of the Chinese perspective: In the view of U.S. officials, the threat posed to America's economic interests by Chinese espionage is a threat to American national security.

Like China's economy, the spying carried out on its behalf is directed by the Chinese state. The Ministry of State Security, or M.S.S., which is responsible for gathering foreign intelligence, is tasked with collecting information in technologies that the Chinese government wants to build up. The current focus, according to U.S. counterintelligence experts, aligns with the "Made in

China 2025" initiative announced in 2015. This industrial plan seeks to make China the world's top manufacturer in 10 areas, including robotics, artificial intelligence, new synthetic materials and aerospace. In the words of one former U.S. national security official, the plan is a "road map for theft."

The Chinese government relies not only on its intelligence services but also on businesses, institutions and individuals to gather proprietary information. A 2019 report from the U.S.-China Economic and Security Review Commission, a congressional committee, lists the myriad ways in which Chinese companies, often backed by their government, help transfer strategic know-how from the United States to China. The maneuvers range from seemingly benign (acquiring American firms with access to key intellectual property) to notoriously coercive (compelling American companies to form joint ventures with Chinese firms and share trade secrets with them in return for access to the Chinese market) to outright theft. Cyberattacks have become an increasingly common tactic because they can't always be linked directly to the Chinese government. Over the past few years, however, federal agents and cybersecurity experts in the U.S. have identified the digital footprints left along the trails of these attacks — malware and I.P. addresses among them — and traced this evidence back to specific groups of hackers with proven ties to the Chinese government.

Perhaps most unsettling is the way China has sought to exploit the huge numbers of people of Chinese origin who have settled in the West. The Ministry of State Security, along with other Chinese government-backed organizations, spends considerable effort recruiting spies from this diaspora. Chinese students and faculty members at American universities are a major target, as are employees at American corporations. The Chinese leadership "made the declaration early on that all Chinese belong to China, no matter what country they were born or living" in, James Gaylord, a retired counterintelligence agent with the F.B.I., told me. "They started making

appeals to Chinese Americans saying there's no conflict between you being American and sharing information with us. We're not a threat. We just want to be able to compete and make the Chinese people proud. You're Chinese, and therefore you must want to see the Chinese nation prosper."

Stripped of its context and underlying intent, that message can carry a powerful resonance for Chinese Americans and expatriates keen to contribute to nation-building back home. Not all can foresee that their willingness to help China could lead them to break American laws. An even more troubling consequence of China's exploitation of people it regards as Chinese is that it can lead to the undue scrutiny of employees in American industry and academia, subjecting them to unfair suspicions of disloyalty toward the United States.

Hua didn't regard his visit to China to share his technical expertise as extraordinary in any way. Many scientists and engineers of Chinese origin in the United States are invited to China to give presentations about their fields. Hua couldn't have known that his trip to Nanjing would prove to be the start of a series of events that would end up giving the U.S. government an unprecedented look inside China's widespread and tireless campaign of economic espionage targeting the United States, culminating in the first-ever conviction of a Chinese intelligence official on American soil.

Illustrations by Hokyoung Kim

Around noon on Nov. 1, 2017, a few hours after he scanned his security badge and entered his office at G.E. Aviation, Hua received a call from the

company's I.T. desk asking him to come meet with G.E.'s security officers. The call heightened a sense of anxiety he had felt since that morning, when he and others in his group were asked to hand over their removable hard disks for what I.T. described as a computer security review. A while later, they were asked to turn in their work laptops. Hua couldn't help wondering if this had anything to do with the secret of his Nanjing trip that he had been keeping from his employer.

Soon enough, his fears were confirmed: The G.E. security officers waiting to interview him in an auditorium wanted to know about his trip to China six months earlier. Where had he visited, and why? Hua told them he had gone back home for a college reunion and spent all his time reconnecting with friends and family.

Then the security officers told Hua that the F.B.I. wanted to talk to him. Two F.B.I. agents, who were already in the building, entered the room. One of them was Bradley Hull, a bright-eyed man with a shaved head and a goatee. He started with the same questions that G.E. security had asked about Hua's China trip.

Hua was shaking with nervousness, one of the agents told me in an interview. He repeated the answers he had given to his employer's security officers. Hull proceeded to ask more questions about the trip, giving Hua several chances to amend his story and signaling that he didn't think Hua was being truthful. Finally, he confronted Hua with evidence showing that Hua had met with people other than just friends and family. He had also paid a visit to the Nanjing University of Aeronautics and Astronautics.

Hua sank into his chair as if knocked back. It was a crime to lie to a federal agent, Hull told him. He advised Hua to relate everything he could remember about the visit to N.U.A.A. Hua, in shock, wasn't immediately forthcoming,

but over the course of the interview, as Hull pressed him with follow-up questions, Hua ended up providing an account of why he visited Nanjing and what he did there. The agent who spoke to me described the interview as incremental truth telling.

Hua finally disclosed that he had given a presentation at N.U.A.A. about designing airplane parts out of composite materials. He said he had been careful to not divulge any information that was proprietary to G.E., even though he had downloaded certain files that belonged to his employer to help prepare his slides. As Hua provided more detail about his visit, Hull became convinced that he had been hosted at Nanjing by Chinese intelligence officials looking to cultivate the engineer as an asset, someone who could steal trade secrets for them.

Around 4:30 p.m., at which point the interview had been going for a few hours, Hull suggested taking a break to eat some pizza that he had ordered for everyone. He also made Hua an offer: The F.B.I. wouldn't recommend that charges be brought against him if he agreed to cooperate and take part in a counterintelligence operation against the Chinese. Hua had already been informed that the F.B.I. had been carrying out a search at his home that afternoon, while he was being interviewed; his car had also been towed away to be searched. And here at work, the agents had already caught him lying, which he realized was enough to land him in trouble. Even though he hadn't shared any trade secrets at his Nanjing presentation, some of the documents downloaded to his laptop before he went to China were marked export-controlled — a government-mandated designation — for which he could face criminal charges. He knew what he had to do to save himself and his family.

"No one begrudges a nation that generates the most innovative ideas and from them develops the best technology," John Demers, former assistant

attorney general for national security, said in a 2018 hearing before the U.S. Senate Judiciary Committee. "But we cannot tolerate a nation that steals our firepower and the fruits of our brainpower."

The accusation that China has been relentlessly stealing intellectual property from American companies and institutions — although China is now a manufacturing giant, for technology it still relies heavily on the United States and Europe — is neither new nor unfounded. In 2008, a Chinese-born engineer named Chi Mak who worked for a defense contractor in California was sentenced to more than 24 years in prison for having stolen and passed on to China information about several sensitive technologies, including systems for the U.S. Navy. The Chi Mak investigation led to the uncovering of another Chinese spy, Dongfan Chung, an engineer at Boeing who gave his handlers in China thousands of documents containing designs and other technical specifications relating to American fighter jets, the U.S. space shuttle and the Delta IV rocket. In the past decade, individuals working for Chinese entities have been caught taking or trying to take trade secrets across many industries. One notable case involved six Chinese nationals in the United States attempting to steal proprietary corn seeds from fields in Iowa and Illinois. A California engineer named Walter Liew was caught stealing secrets relevant to the production of titanium dioxide, which is used as a whitener in paint and toothpaste. Individuals of Chinese origin have been indicted in recent years for the theft of proprietary information relating to locomotives, semiconductors, solar panels and other high-tech products.

In recent years, China has been recruiting those it considers expat nationals through hundreds of formal "talent" programs, which identify experts in American schools and industries to help fill specific gaps in knowledge back home. "It's a vehicle to get them to travel back to China to attend conferences, to provide lectures, which allows the opportunity to develop a relationship with them and later take advantage of that relationship to get

intellectual property," Gunnar Newquist, a former counterintelligence agent for the Naval Criminal Investigative Service, told me.

The guests are often hosted in luxury hotels, driven around in limousines, taken on sightseeing tours. After receiving this lavish treatment, Gaylord says, some feel obligated to provide information that they might not have initially planned to share. While at the F.B.I., Gaylord interviewed many scientists and engineers of Chinese origin who had been courted in this fashion. Some of them described how they had been pressured. "They would say: 'Everything in my presentation was approved by my company. After I finished it and stepped down, a gaggle of students surrounded me to ask more questions. And they kept pushing me for more and more sensitive information,'" Gaylord says. "And a lot of them say: 'You know, after a while, you start to break down. You can't keep saying, "I can't talk about this." You then start answering around the edges, giving away more and more.'"

The Chinese government also offers financial incentives to help Chinese expats start their own businesses in China using trade secrets stolen from their American employers. Gaylord told me about Wenfeng Lu, an engineer who worked at Edwards Lifesciences in Irvine, Calif. Lu's employer reported him to the F.B.I. after discovering that he had been downloading proprietary information about the company's heart catheters. Gaylord and his colleagues opened an investigation and discovered, among other red flags, that Lu was often collecting this material right before trips to China. Agents arrested him as he was preparing to leave the country for another visit. On the laptop and thumb drives that he was carrying, investigators found information he had taken from his employer. Searching his house, agents found more documents he had collected from two other U.S. medical device companies where he had worked. "Then, in his laptop, we found agreements between him and municipal government officials in China offering him research offices in an industrial park in Nanjing that would be rent-free for the first

three years," Gaylord says. "In other words, he steals the R. & D. cost our companies incur, and he goes there and develops it for a lot cheaper. And has the whole China market without any revenues going to the American companies." Lu pleaded guilty to charges of unauthorized possession of trade secrets and in 2019 was sentenced to 27 months in prison.

The F.B.I. is loath to give away sources and methods, so the agency would not disclose to me how agents learned of Hua's visit to Nanjing. But from the start it suspected that Hua's hosts wanted more than an innocent academic exchange. As the investigators learned more about the trip, they could see that it had all the hallmarks of an intelligence operation — the initial contact through LinkedIn, the introduction to people who had weaker ties to N.U.A.A. The F.B.I. suspected that the Jiangsu science and technology association was a front for the Chinese government and that Qu Hui, the man who gave Hua the tea, was an intelligence officer.

The agents wanted to learn more about Qu, who seemed to be the key figure behind the Chinese attempt to recruit Hua, and they saw an opportunity to go further than just an investigation into Hua. The agent who spoke to me likened their counterintelligence operation to swimming upstream. And so, in exchange for an assurance that he wouldn't face charges, Hua became an asset for the F.B.I., willing to communicate with his Chinese contacts at the F.B.I.'s behest.

Deception often lies at the heart of espionage and counterespionage; success for both spies and spy hunters can hinge on finding a foolproof way to deceive their targets. Describing Hua's communications with his hosts in

China, the agent emphasized that the investigators didn't type anything themselves. Hua wrote the messages himself, to give them the veneer of authenticity that the F.B.I. wanted. A team of agency linguists assisted Hull, who doesn't know Mandarin, with figuring out what Hua might say and how to say it. Ultimately, though, they needed to rely on Hua's own judgment about exactly how to phrase things.

> ***The ubiquitous use of iPhones around the world — a result of American technological prowess — was helping to fight back against a rival nation's efforts to steal technology.***

After his return from China, Hua stayed in touch with his hosts in Nanjing. "I will definitely contact you again if I have a chance to visit China in the future," he wrote to Qu, keeping the door open for another academic exchange at the university. Now, at Hull's direction, he sent Qu a message over WeChat on Dec. 20, a month and a half after the F.B.I. first interviewed him. He told Qu he would be willing to return for another visit in February, a week before the Chinese New Year. In earlier conversations with Qu, he talked about his responsibilities as the oldest son in the family, and so it made sense for him to want to visit home during the Chinese New Year.

Qu consented to the offer. "I will touch base with the scientific research department here to see what technology is desired and I will let you know what to prepare," he texted Hua on Jan. 9, 2018.

By now federal agents had obtained search warrants for two email addresses that Qu had used for his correspondence with Hua: jastxyj@gmail.com and jastquhui@gmail.com. In what would prove to be a lucky break, the investigators found that each email address was the Apple ID used for an iPhone, linked to an iCloud account where data from the phones was periodically backed up. The agents were later able to obtain search warrants for the two iCloud accounts. The one linked to jastquhui@gmail.com opened a treasure trove.

This included confirmation of what they had suspected all along: that Qu worked for Chinese intelligence. His real name was Xu Yanjun. He had worked at the Ministry of State Security since 2003, earning six promotions to become a deputy division director of the Sixth Bureau in the Jiangsu Province M.S.S. Like so many of us, he had taken pictures of important documents using his iPhone — his national ID card, pay stubs, his health insurance card, an application for vacation — which is how they ended up in his iCloud account. There, investigators also found an audio recording of a 2016 conversation with a professor at N.U.A.A. in which Xu had talked about his job in intelligence and the risks associated with traveling. "The leadership asks you to get the materials of the U.S. F-22 fighter aircraft," he told the professor. "You can't get it by sitting at home." The discovery of evidence of Xu's identity in an iCloud account makes for a kind of delicious reversal. The ubiquitous use of iPhones around the world — a result of America's technological prowess — was helping to fight back against a rival nation's efforts to steal technology.

The revelation that the target of their investigation was a senior-level M.S.S. officer raised the stakes for the F.B.I. The agent characterizes the unmasking of Xu as a significant milestone in the effort to combat economic espionage by the Chinese, for reasons that go beyond this one case. When F.B.I. agents go out to talk to companies and universities about the threat, he says,

skeptical listeners ask for the evidence that proves the theft of trade secrets is part of a campaign directed by China's government. In Xu Yanjun, the F.B.I. now had the example it needed. Here was an intelligence officer working as a puppet-master, in one agent's characterization of the events, cultivating people at American companies in order to steal trade secrets. The F.B.I. was determined to build a case against him and even arrest him if it could.

Illustrations by Hokyoung Kim

Hua was put on leave without pay by G.E. Aviation right after the F.B.I. interviewed him in November 2017. As he struggled to find paid work in the weeks that followed, his efforts on behalf of the F.B.I. kept him engaged. Under the agency's direction, he kept up his exchanges with Xu over WeChat and email, expressing eagerness to share information from G.E. "Just recently I've heard the speculation about laying off in my department. I, of course, don't want to be affected, but the possibility is there," he wrote in a message on Jan. 23. "That's why I'm trying my best to collect as much information as possible." Xu asked if Hua could send material relating to the specifications and design process for building an encasement for fan blades. Hua obliged with a document titled "G.E.9X Fan Containment Case Design Consensus Review." It had the appearance of being useful but didn't contain anything of real value — G.E. Aviation, which was cooperating with the F.B.I., had altered the document. This bait worked: Xu, emboldened, sent a list of "domestic requirements" that he wanted Hua to collect information for, such as the type of software used in designing composite structures.

On Feb. 5, about a week before Hua arranged with Xu to visit Nanjing again, Xu asked him to copy the table of contents of his G.E. laptop's directory into a file that he could bring with him. He provided instructions on how to create the file in Notepad. The document would give a high-level picture of the work Hua's group at G.E. was doing — and more important, it would indicate

what information Hua had access to.

The F.B.I. never intended for Hua to travel to China. On Feb. 7, he sent Xu a message saying he couldn't make the trip because his boss had asked him to go to France in March for work. There was a lot to do in preparation for that trip, he explained, so he wasn't being allowed to take any time off. "Because the ticket already booked is not refundable," he wrote, "even my parents are very disappointed."

He asked if he could still be reimbursed for the airfare. Xu, presumably disappointed that the meeting wasn't going to happen, was noncommittal. He messaged in response: "Can we resolve all these issues the next time you come back?"

Xu's interest was rekindled a week later, however, when Hua emailed him a copy of his laptop directory, stripped of any information that G.E. regarded as sensitive. Xu proposed that they get together somewhere in Europe after Hua traveled to France in March. Until this point, they had been communicating by email and WeChat, but on Feb. 27, apparently eager to finalize his suggested meeting, Xu attempted to make a video call to Hua when it was nearly 10 p.m. in Cincinnati. Hua was at home, but with no F.B.I. agents by his side to instruct him on what to do, he couldn't risk answering. About an hour later, at Hull's direction, he messaged Xu: "Sorry missed your call. I was trying to put the child to sleep." He added that he would be visiting France from March 25 to April 6.

When Xu and Hua spoke the next day to arrange a meeting place, Hua suggested Belgium or Germany or the Netherlands — that way, he said, he could get away from his G.E. colleagues.

The real reason was different. The F.B.I. wanted the meeting to happen in a country that would be amenable to arresting Xu. The French government

was unlikely to agree.

Xu asked if Hua could bring along the contents of the directory he had sent. "I think that is pretty good stuff," Xu said.

Hua said he planned to bring his laptop to their meeting.

"The thing is, can you export the stuff out?" Xu asked.

Hua confirmed that he could and assured him again that he would have the files with him.

"All right," Xu said. "Let's try our best to meet in Europe."

In the last week of March 2018, Hua flew to Brussels, accompanied by Hull and other agents. For months he had been playing an active role in their investigation; now he was about to participate in a field operation. His wife was worried. "I tried to explain to her that everything would be fine," he told me.

Xu had flown to Amsterdam. He wanted Hua to meet him there, but the F.B.I. wanted Xu to go to Belgium. Behind the scenes, U.S. authorities had been working to secure cooperation from a European country, which they ultimately got from the Belgian government. Hull had Hua explain to Xu that he couldn't come to Amsterdam on March 31 as planned because his boss had asked him to visit a plant in Belgium. He could meet on April 1 instead, and it would have to be in Brussels.

The change of plans flustered Xu. It would be difficult for him to change his itinerary, he messaged back; he suggested they stick to meeting in Amsterdam. In a voice call to Hua over WeChat, he explained that traveling to a new country for the meeting without prior approval from his superiors in China would be considered serious misconduct. He then proposed they

meet in Rotterdam — Hua could make it to the Dutch city and return to Brussels the same day.

The F.B.I. had to come up with a reason for Hua to reject Xu's proposal. "Sunday is Easter, which my boss takes seriously," Hua messaged Xu over WeChat. "He has reserved an Easter lunch for the traveling team and asked us better to attend." There was no way he could leave Brussels.

Xu finally gave in, and Hua sent him a photo of a coffee shop in the Galleries of Saint Hubert, a historic landmark in central Brussels whose grand, high-pillared architecture and arched glass-paned roof are a draw for tourists.

The meeting was set for 3 in the afternoon. But Xu went to check out the coffee shop a few hours earlier, accompanied by a colleague from the M.S.S. The two men walked through the galleries. As they approached the coffee shop, Belgian federal police officers placed them under arrest. In addition to two smartphones and about 7,000 euros, Xu and his colleague had $7,000 in hundred-dollar bills — cash that they presumably planned to give to Hua that afternoon. Six months later, Xu was extradited to the United States to face charges of economic espionage.

Illustrations by Hokyoung Kim

I saw Xu at a pre-sentencing hearing on Aug. 23 last year, in federal court in Cincinnati, dressed in an orange-and-white prison jumpsuit. Despite being somewhat tall, Xu looks compact, with a squarish face that didn't betray much emotion as the day's proceedings got underway, except for one moment early on when he was struggling with shackled hands to review some papers his lawyers were showing him. At the judge's direction, a federal marshal unshackled him. Freed, even if only in a limited sense, Xu gave a nod of gratitude.

It was striking, based on a court filing submitted by Xu's lawyers, to note the parallels in the early lives of Xu and Hua in China. Like Hua, Xu was born into a family of modest means. Like Hua, he devoted himself to the pursuit of good grades, studying late into the night and on weekends — excelling in academics was one way to build a better life. Like Hua, Xu became the first person in his family to go to college, where he earned undergraduate and graduate engineering degrees. That's where the similarities between the paths of their two lives end. In 2003, the year Hua left for the United States, Xu started working for the Ministry of State Security.

During a two-week trial in Cincinnati that began in October 2021 — more than three years after Xu's extradition to the United States — federal prosecutors laid out their case. Xu was represented by a team that included five attorneys from Taft, Stettinius and Hollister, a leading Midwest law firm, which suggests that the hundreds of thousands of dollars required in legal fees was paid by the Chinese government. (The firm declined to comment for this article.) The defense argued that Xu had been tricked; the intent behind his correspondence with Hua was not to steal trade secrets but simply to facilitate an academic exchange between Hua and Chinese scientists. Ralph Kohnen, one of the defense attorneys, said in his closing argument, "What's happened here is Mr. Xu, my client, has become a pawn, a pawn in the tense place between U.S. industries trying to exploit China and trying to get along with China."

The prosecution contended that Xu had been systematically going after intellectual property at aerospace companies in the United States and Europe through cyberespionage and the use of human sources. It's not often that prosecutors find a one-stop shop for much of their evidence, but that's what Xu's iCloud account was — a repository of the spy's personal and professional life. That's because often Xu used his iPhone calendar as a diary, documenting not just the day's events but also his thoughts and

feelings. Several entries from 2017, for instance, indicate rising tensions with his boss, a man named Zha Rong. "Zha rejected a meal receipt today," he wrote on March 27. Then, on April 28: "Relationship with Zha has dropped to freezing point." Other entries from that period — when he started corresponding with Hua — reflect an unhappiness in Xu's personal life. Such as one from Aug. 17, in which he lamented the breakup of what appears to have been an extramarital romance. She "saw me in the rain yesterday morning, didn't stop and she walked away with her umbrella." Things weren't going well financially, either, as evidenced by a snippet from an entry on May 19: "I lost so much in the stock market. I got myself into this financial hole."

> ***'If you ask me, are there days when I have trouble falling asleep? Yes, there are. I regret what I did.'***

Also backed up to the cloud were messages that Xu had exchanged with several other U.S. aerospace-industry employees, which prosecutors laid out at trial. One of them was Arthur Gau from a Honeywell division in Phoenix, who testified at trial that Rong and Xu paid him $5,000 and covered his airfare to China for a 2017 visit to Nanjing to make a technical presentation. (In May 2021, Gau pleaded guilty in Arizona to a charge of exporting controlled information without a license. Bloomberg Businessweek covered Xu's case extensively in an article published last September.) Another was an engineer at the aviation company Fokker, who accepted Xu's invitation to visit China to share information with a Chinese research institute after Xu arranged to help the engineer's parents, who had lost their home in China when their building was set to be demolished as part of a development project. An I.T. specialist from Boeing, who testified at the trial under the alias

Sun Li, described how Xu attempted to cultivate a relationship with him, first reaching out through an email in which he mentioned having contacted the witness's dad, an academic in China. The witness subsequently met with Xu, who repeatedly offered to reimburse his round-trip tickets to China in exchange for sharing his knowledge of and experience in I.T. The witness finally stopped communicating with Xu after realizing that Xu was not actually interested in his expertise, which was project management, but in "something else that I could not provide."

"What they call exchanges are not just a nice invitation," Timothy Mangan, who led the prosecution, told me, encapsulating a point he made to the jury. "It's part of a recruiting cycle. Some pan out, some don't, but this is them throwing the fishing lines out, trying to vet people."

At Xu's trial, Mangan buttressed the argument about the so-called exchanges being anything but benign by citing an audio recording of a four-hour meeting between Xu and several Chinese engineers. Why Xu should have recorded this conversation is inexplicable — and surprisingly imprudent in hindsight, given that it ended up in an iCloud account — but in it he explains the approach to soliciting information from Chinese expatriates. "As experts abroad, it would be very difficult for them to directly take large batches of materials due to the fact that their companies' security is very tight," Xu tells the engineers, emphasizing the need to consider the risks involved for sources being targeted. At another point in the conversation, he talks about how to spot potential recruits while targeting specific technologies. "For example, if I am an aircraft person, then I would search into Boeing or Lockheed, right? Find it at Lockheed Martin," Xu said. "After I found the person, I would find out if this person is doing something? Like in charge of overall design or avionics."

The messages in Xu's iCloud account enabled investigators to make another

damning discovery. Xu had helped coordinate a cyberespionage campaign that targeted several aviation technology companies. Those attacks — described in a report by CrowdStrike, a cybersecurity firm — started in 2010, shortly after the state-owned Commercial Aircraft Corporation of China (COMAC) announced that it had chosen a joint venture between G.E. Aviation and Safran to supply a custom-made engine for China's first domestically manufactured commercial airliner, the C919. The plan behind the campaign, which was directed against Honeywell, Capstone Turbine and Safran, among others, became clear only later when security researchers connected the dots. "When I started putting all these victims together — I was like, OK, these are all component manufacturers for different pieces of the C919," Adam Kozy, a cybersecurity expert who runs the security firm SinaCyber and was the lead author of the CrowdStrike report, told me. Although COMAC was prepared to procure components needed to build the aircraft from these companies, the Chinese government was evidently also working to steal intellectual property from those suppliers in order to make domestic manufacturing possible in China, according to the report.

Xu played a role in these efforts, the prosecution argued at trial. In his iCloud account were several messages that Xu had exchanged with a manufacturing engineer employed with Safran named Tian Xi, indicating that they had been plotting to hack into the company's computer network. The plan was to have Tian — who was working at a Safran plant in Jiangsu — install malware provided by Xu onto the laptop of a Safran employee visiting from France. It took many weeks for the plan to succeed. Tian sent Xu a triumphant text on Jan. 25, 2014, saying, "The horse is planted" — a reference to a Trojan horse, a type of malware. (Tian was indicted on related charges; the case is pending.)

At the end of the trial, Xu was convicted of conspiring and attempting to commit economic espionage and theft of trade secrets. In a sentencing

memorandum filed last November, Xu's lawyers painted a sympathetic portrait of the spy, describing him as a kind man who loved playing soccer with his son and routinely carried groceries up several flights of stairs for elderly neighbors. Xu was simply doing his job, they pointed out, adding that "he was not a rogue operator or criminal mastermind." A lenient sentence would be appropriate, the memo argued, because the U.S. government couldn't hope to deter China's theft of intellectual property by harshly punishing a single intelligence officer. The judge wasn't swayed. On Nov. 16 last year, Xu was sentenced to 20 years in prison. His conviction is now being appealed.

Xu's arrest and prosecution could be likened to the capture of an enemy combatant who is then made a prisoner of war, but for an important distinction that U.S. officials make — that this war, or economic espionage offensive, is being waged unilaterally by China. The Chinese government, which maintains that America's accusations of economic espionage are "slanderous," has described the charges against Xu as "made out of thin air." According to Mangan, the evidence laid out during Xu's trial goes far beyond merely proving his guilt — it uncovers the systematic nature of China's vast economic espionage. The revelation of Xu's activities lifts the veil on how pervasive China's economic espionage is, according to the F.B.I. agent. If just one provincial officer can do what he did, the agent suggests, you can imagine how big the country's overall operations must be.

A sense of that scale comes from a pair of indictments unveiled in federal court in the District of Columbia in 2019 and 2020 naming five computer hackers in China responsible for intrusions into more than 100 businesses, nonprofits and government agencies in the United States and other countries. The hackers belong to the group APT41, which the Department of Justice says is backed by the Chinese government, and it didn't restrict itself to the theft of intellectual property and business information. Investigators

say the hackers also purloined more than a million detailed call records from telecom companies. APT41 appears to have developed a data-modeling way to mine this type of information and map the social networks of specific targets, including a Tibetan monk living in India and pro-democracy activists in Hong Kong. The cases are pending.

One day last September, I traveled to Cincinnati to ask Hua about what he had gone through. He agreed to meet on the condition that I protect his identity. Even though he testified in court under his real name, he wanted to draw as little attention to himself as possible, especially out of a concern for his family. We met at a Chinese restaurant for lunch. Walking over to the table where I was sitting with his attorney, he greeted me with a gentle handshake and asked me to excuse him for speaking softly because of a rib injury he'd suffered while jogging.

Hua told me he had spent the past few years rebuilding his life. During the time he was helping the F.B.I. with its investigation, he was effectively unemployed — G.E. fired Hua after he was on leave for several months — except for a couple of weeks when he worked as a driver for Uber Eats. He finally found a job with an engineering company unrelated to his expertise. Still, he didn't see himself as a victim. "Why did I have to accept the invitation without consulting my employer, my family?" he said. "I bear the consequences of what I did."

He brightened when I asked him about his interest in composites. "It's a fascinating field," he said. "You can design a composite in many ways. You can think out of the box, you have a lot of flexibility in engineering it." When I asked if he'd thought about returning to the field, however, he shook his head. "I don't want to," he said. He seemed worried that going back to designing composite structures would somehow open a fresh portal to the trauma he was trying to leave behind.

A few times during our conversation, I saw his eyes glisten and his lips quiver. But whenever I pressed him to describe how he felt about what he had been through, his face would take on a stoic expression, as if he was trying to keep his emotions in check. "If you ask me, are there days when I have trouble falling asleep? Yes, there are. I regret what I did. But I always tell myself, that's the past, what can I do? I can only look forward, to see what I can do tomorrow."

When Hua told me how he agreed to assist the F.B.I. to save himself and his family, I couldn't help thinking of him and Xu as chess pieces in a geopolitical game that they had little control over — two men of similar background whose lives had collided, with unfortunate results for both. I asked Hua if he felt any anger toward Xu for arranging his visit to Nanjing. "No," Hua replied. "He was just doing what he was asked to do."Weeks later, after Xu's sentencing on Nov. 16, Hua relayed a message to me through his attorney to say that he was saddened to hear that Xu would be spending such a long time in prison. "He's not my enemy," Hua said. "We are all just normal people."

Yudhijit Bhattacharjee is the author of "The Dinner Set Gang" and "The Spy Who Couldn't Spell." He last wrote for the magazine about scam calls and where they come from. **Hokyoung Kim** is an illustrator from South Korea living in New York. She is known for a filmic style with narrative focus and dramatic lighting.