*Photographer: Ina Jang for Bloomberg Businessweek*

Businessweek | The Big Take

# A Chinese Spy Wanted GE's Secrets, But the US Got China's Instead

How the arrest of a burned-out intelligence officer exposed an economic-espionage machine.

By Jordan Robertson and Drake Bennett

September 15, 2022 at 5:01 AM GMT+1

In January 2014, Arthur Gau, an aerospace engineer who was nearing retirement age, received an unexpected email from a long-lost acquaintance in China. Years before, Gau had made a series of trips from his home in Phoenix to speak at the Nanjing University of Aeronautics and Astronautics, or NUAA, one of China's most prestigious research institutions. The original invitation had come from the head of a lab there studying helicopter design. Increasingly, however, Gau had heard from someone else, a man who worked at the university in a vague administrative capacity. Little Zha, as the man called himself, was the one who made sure Gau never had to pay his own airfare when he came to give talks. When Gau brought his mother on a 2003 visit, Zha arranged and paid for them

to take a Yangtze cruise to see the river's dramatically sculpted middle reaches before they were flooded by the Three Gorges Dam.

The relationship had ended awkwardly, though, when Zha offered Gau money to come back to China with information about specific aviation projects from his employer, the industrial and defense giant Honeywell International Inc. Gau ignored the request, and the invitations stopped.

Now, in 2014, Little Zha was reaching out again. The two started corresponding. In early 2016, Gau, whose interests extended far beyond avionics, said he'd planned a trip to China to visit some friends in the musical theater world. Zha was there that spring to meet him at the airport in Beijing. Waiting with him was a colleague Zha was eager for Gau to meet.

Xu Yanjun was on the tall side, at 5 feet 10 inches, with closely cropped hair, glasses, and a tendency toward bluntness. The three had dinner and met up again before Gau flew back to the US. Over pastries in Gau's hotel room, they discussed Taiwanese politics—Gau grew up there—as well as the engineer's evolving responsibilities at Honeywell. Late in the evening, Xu handed Gau $3,000 in cash. Gau would later testify that he tried to hand it back, but Xu was insistent. "And then, you know, back and forth, but I took it eventually."

The next year, Gau came back to China to give another lecture—this time a private one in a hotel room to several engineers and officials, including Xu. In preparation, Gau had emailed over PowerPoint slides containing technical information, including algorithms and other sensitive design data for the aircraft auxiliary power units Honeywell makes. "Because of the payment, I felt obligated," he would later tell a judge.

Arthur Gau (right) at West Lake in China. *Source: U.S. Department of Justice*

Xu paid him $6,200 more, and two of his associates accompanied the visiting engineer on a two-day sightseeing trip to West Lake, famed for its picturesque gardens, islands, and temples. Gau was planning his next visit when, in the fall of 2018, agents from the FBI appeared at his home in Arizona to execute a search warrant. There would not be another trip. Xu, the agents explained, was not in Nanjing anymore. He wasn't even in China. He was in Ohio, in a county jail awaiting trial.

The issue of Chinese industrial espionage is a fraught one. In November 2018, Jeff Sessions, then the Trump administration's attorney general, announced a program called the China Initiative, intended to combat "the deliberate, systematic, and calculated threats" from Chinese government-directed intellectual-property theft. The program, however, ended up targeting largely academics—not for stealing secrets, but for failing to report affiliations with Chinese research institutions. In some instances, even those charges proved meritless. In February, amid concerns over ethnic profiling and the criminalization of scientific collaboration, the Biden administration shut down the China Initiative, though it vowed to continue pursuing cases involving the country.

Nonetheless, the remit of Chinese intelligence services does cover industrial secrets as well as military and government ones, and their leadership takes that responsibility seriously. It's what rising economic powers have always done: In the late 18th century, the newly independent US offered bounties for textile workers to smuggle loom designs from the great British cotton mills. Those mills had been built in part to specifications once pilfered from Italian silk spinners. And that industry, in turn, wouldn't have existed without silkworm eggs spirited out centuries before from China.

The modern Chinese industrial espionage apparatus—in its organization, scope, and ambition—far eclipses those predecessors. "We consistently see that it's the Chinese government that poses the biggest long-term threat to our economic and national security," FBI Director Christopher Wray said in a speech in July. Since the 1990s, prosecutors have charged almost 700 people with espionage, IP theft, illegally exporting military technology, and other crimes linked to China. Two-thirds of the cases have led to convictions, according to a database kept by Nick Eftimiades, a former official at the US Department of Defense and a senior fellow at the Atlantic Council; most of the rest are pending or involve fugitives. All are part of an intelligence-gathering apparatus that relies not only on trained spies and officers of China's Ministry of State Security but also on ordinary engineers and scientists. This machinery remains largely opaque to outsiders. Limited to going after the people feeding information to handlers in China, US authorities have been like narcotics investigators pursuing low-level buy-and-busts while the larger criminal infrastructure hums along unscathed.

At least, that was the case until Xu Yanjun's trial last fall. His arrest marked the first time an MSS officer was lured out of China and extradited to the US. And it was more than a symbolic victory, yielding an extraordinary trove of digital correspondence, official Chinese intelligence documents, even a personal journal. When Xu was apprehended, he had with him an iPhone whose contents he'd faithfully backed up to the cloud, a lapse that allowed FBI investigators to recover all the data from Apple Inc. Asked about the case, China's Ministry of Foreign Affairs responded, "The accusations by the US are completely fabricated. We demand the US handle the case in a fair manner and ensure the legitimate rights of Chinese citizens."

Over two and a half weeks from late last October into November, federal prosecutors in a courtroom in Cincinnati drew on the wealth of digital material the 41-year-old Xu had stockpiled to lay out a portrait of him—his training, methods, and ambitions, his vices and private doubts and grievances. Translated from the original Mandarin, it's an unprecedentedly intimate portrait of how China's economic espionage machine works, and what life is like for its cogs.

*Photographer: Ina Jang for Bloomberg Businessweek*

One of the pieces of evidence presented at Xu's trial is a four-page document from October 2015 whose dry title reads "Cadre Approval/Removal Appointment Application Form." In the top right corner of the first page is a photo of a fresh-faced Xu in uniform, his mouth set but his eyes carrying the hint of a smile. Below, in a box marked "Current Post," it reads, "Deputy Division Director at Sixth Bureau of Jiangsu Province Ministry of State Security."

The document is similar in some respects to Standard Form 86, a questionnaire American intelligence employees are required to complete. But the paperwork of an autocratic one-party state has an added richness, functioning as not only a professional and personal biography but also a political one. Bradley Hull, the FBI special agent who led the investigation of Xu, was asked at one point in his testimony if he'd ever seen such a form. "No," he replied. "No one has."

Xu was born in 1980 in a small town in Jiangsu, a province on the Yellow Sea just north of Shanghai. His father was a manager at an agricultural company, and his mother worked at the county finance bureau. Before Communist rule, Jiangsu had for centuries been a wealthy trading hub. Nanjing, its capital city, had served multiple dynasties as an imperial seat. Deng Xiaoping's economic reforms, whose emergence coincided with Xu's birth, made the province once again a gateway to the wider world. Multinational technology companies such as Hitachi, Philips, and Samsung built manufacturing facilities there, bringing with them jobs and money—and proprietary information. It was natural for the Jiangsu branch of the MSS to develop an industrial focus.

Xu left home for college, studying electrical engineering in Nanjing. He joined the Communist Party and in February 2002 was appointed secretary of a village youth league committee in Yancheng, a city near his hometown. It was his first step up in the vast civil service cadre bureaucracy through which the party runs the country. The MSS promised a different kind of power, though. The next year he was hired there, returning to Nanjing and finding a mentor in Zha Rong—Little Zha, who'd been so helpful as an unofficial travel agent for Arthur Gau. The two MSS officers developed a specialization in aircraft technology work. Xu married a fellow party member and had one child, a son.

By late 2013, Xu had ascended to the rank of section chief, and the portrait of him begins to fill out with other information, some of it extracted from his phone and cloud backup, some of it gathered in other counterespionage investigations by the US and its allies. At the time, Xu was targeting Frederic Hascoet, a project manager for Safran Aircraft Engines of France. In partnership with GE Aviation, Safran was developing an engine called the LEAP for narrowbody jetliners such as the Airbus A320, the Boeing 737, and China's Comac C919. The engine's low-pressure turbine was assembled from steel segments at a plant in Jiangsu's sprawling Suzhou Industrial Park, where more than 150 of the Fortune 500 have operations. Hascoet regularly traveled there to oversee this process, working closely with a local Safran manufacturing engineer named Tian Xi.

Tian, however, was also working with Xu and the MSS. That November, Tian and Xu were deep in discussions over hacking Hascoet's computer. Xu texted on Nov. 19 asking when "the Frenchman" would arrive. Then, on Nov. 27: "I'll bring the horse to you tonight. Can you take the Frenchman out for dinner tonight? I'll pretend I bump into you at the restaurant to say hello." The "horse" was malware known as a Trojan, which allows a computer to be accessed covertly and remotely by a hacker. The handoff at the restaurant doesn't seem to have happened, but Xu was eventually able to get Tian a USB drive with the Trojan on it. On Jan. 25, 2014, after a series of increasingly impatient messages from Xu, Tian texted back, "The horse is planted this morning." Xu confirmed that his malware had evaded Safran's firewalls and was communicating with MSS controlled servers, handed the operation over to colleagues, and headed out on vacation.

For Western intelligence agencies, this may have been among the earliest evidence of Xu's handiwork. When Hascoet returned to France in February, his computer couldn't connect to the Safran website, and the IT department found the malware. At the same time, US officials alerted their French counterparts that they'd picked up the digital beacon the malware was sending out to its remote operators. The General Directorate for Internal Security, France's domestic intelligence and security arm, started an investigation. So did Safran. One employee helping to carry out the company's inquest was Gu Gen, a senior IT infrastructure manager and information security officer at Safran's Suzhou offices.

Unfortunately for the investigation, Gu was another one of Xu's assets. It wasn't from him, however, that Xu learned his malware had been discovered. On Feb. 25, a week and a half after Hascoet's computer stopped beaconing back to China, the US cybersecurity company Crowdstrike Holdings Inc. published a blog post revealing the hack.

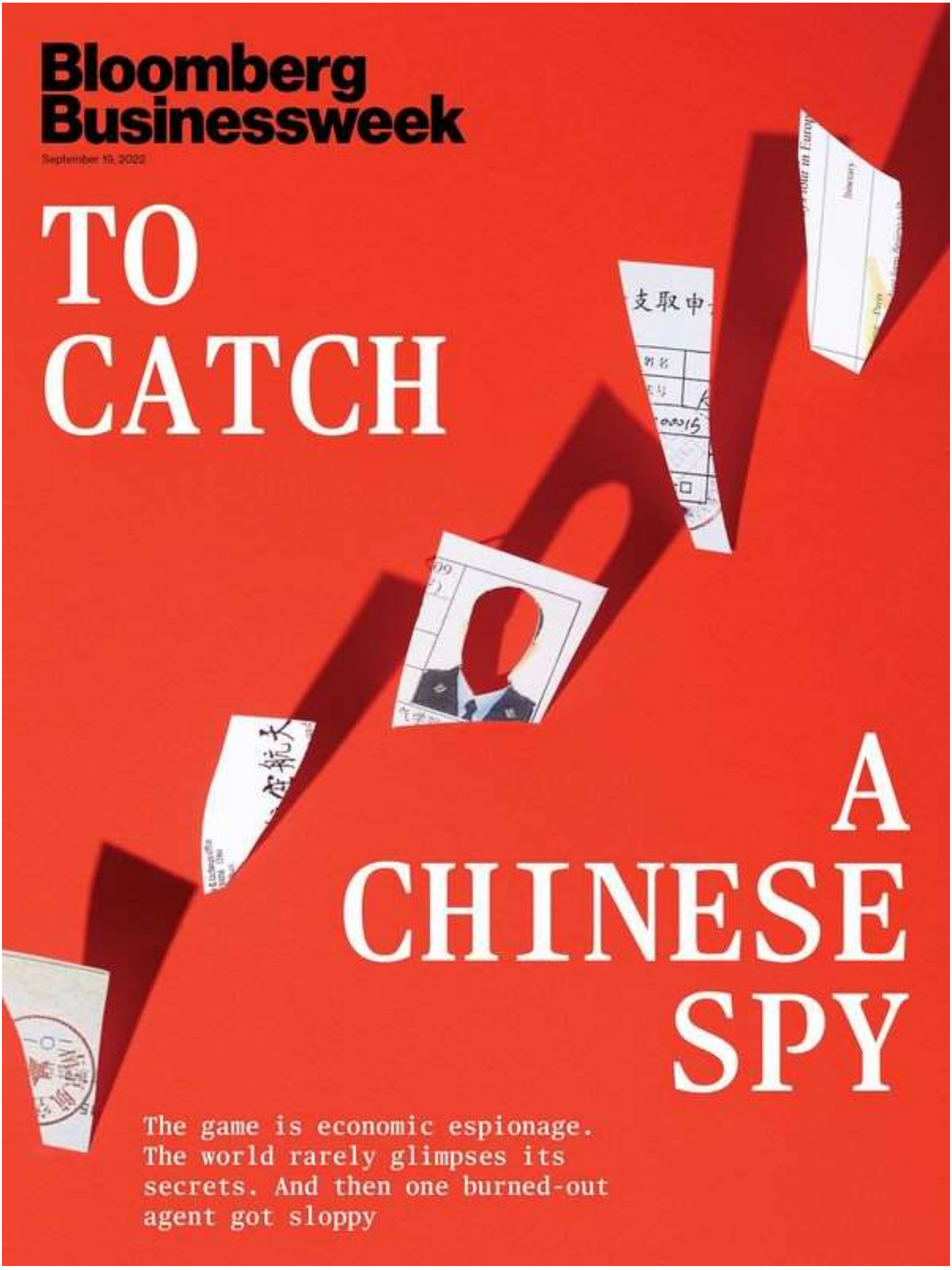
Xu's dismay at the failure of the operation was quickly eclipsed by his outrage at the reaction of his superiors. His division chief angrily called Xu on the carpet and ordered him to have his two sources at Safran contact each other to find out what the company knew. Xu was horrified: Doing that would attract suspicion. "Isn't it like putting a noose on his own neck?" he wrote to a colleague. "It feels bitterly disappointing to have leaders like that." To Xu's relief, Gu reported a few weeks later that the company's investigation was going nowhere. The sense of betrayal, though, lingered.

Meanwhile, Xu and Little Zha continued to collaborate. In April 2014 an engineer who had information about the Lockheed Martin F-35 and Northrop Grumman E-2, two American military planes, visited Nanjing from Great Britain. Xu, posing as an official with an anodyne-sounding nonprofit, had invited him to participate in an academic exchange. That night, while Zha was hosting a dinner in the visitor's honor in a hotel banquet hall, Xu was upstairs breaking into the visitor's room. The plan was to copy the contents of the laptop and portable hard drives there, with help from MSS cyber specialists. It was taking longer than planned.

"Copying the entire thing needs three hours," Xu texted from the room.

"It's too slow," Zha replied from the dinner. "Speed it up."

An hour and a half later, Xu had copied what they needed. "Restoring the scene and the documents will take roughly 20 minutes." And finally: "Restored, and we have left the scene." The banquet could finally end.




Featured in *Bloomberg Businessweek*, Sept. 19, 2022. Subscribe now. *Photographer: Ina Jang for Bloomberg Businessweek*

Opportunities to play cat burglar seem to have been rare, however, especially compared with a section chief's more mundane duties. One of Xu's most time-consuming tasks was helping run the local MSS recruiting efforts, sending emails to university officials who helped him disguise intelligence service job postings as coming from a local industry group. In one, Xu outlined the application requirements: "under the age of 25, Party member, male," with an elite university degree. Résumés were to be sent to the email address jastxyj@gmail.com. (JAST is the Jiangsu Association for Science and Technology, one of Xu's cover organizations, and XYJ are his romanized initials.) He also corresponded extensively with specialists and managers at the Aviation Industry Corp. of China and other state-owned aerospace companies, discussing exactly what information would be helpful to them. In the evenings there were alcohol-soaked work dinners, card games, and late-night visits with co-workers to massage parlors.

At the end of 2014, Xu's future at the MSS looked bright. Despite the Safran incident, his cadre approval form shows that his annual evaluation improved from "competent" to "outstanding." In the spring of 2015 his division chief told him he was in line for the new deputy division director position, and on May 22, Xu's iCalendar records show, the party committee approved him for the post. Zha, too, was promoted, remaining Xu's supervisor.

And yet, as Xu's responsibilities increased, so did his disenchantment with his job. He complained in his diary when he languished in a probationary period before his promotion became official. In February 2016, writing to a friend who worked in a different MSS bureau, he bemoaned his "stupid" decision, years before, to leave his township government job. "I was really tricked." His superiors were autocratic and demanding, he wrote, and stingy with the expense budget. The next day he messaged an acquaintance at an investment company where Xu had once referred a colleague for a job. "I'm not as capable as he is," he wrote, "or I would have gone a long time ago."

Xu's ambition was curdling into something more cynical. Around this time, as part of a selective MSS professional development program, he enrolled in graduate studies in aeronautical engineering. The program was at NUAA, where MSS officers operate freely—the university is one of the Seven Sons of National Defense, an elite group of public universities that develop advanced military technologies for the People's Liberation Army.

Xu seems to have treated his graduate classes like one more academic front operation. In a recording he made in December 2016, he's at a restaurant with a professor from the college of aerospace engineering, sharing fried meat with garlic and braised fish with spicy bean sauce. (Xu, his eye on expenses, suggests they not order too much.) Against his better judgment, the professor has agreed to share information about an upcoming exam; Xu assures him that no one will find out about their "tutoring" sessions. "For a job like mine, we have a lot of friends out there who risk their life to work for us," he boasts. Still, the professor asks, how is Xu going to master a complex subject such as fluid mechanics, even with help? "Ah, fluid mechanics, that will be easier to pass," Xu replies. "I know everyone on that floor!"

Gradually the conversation turns to the MSS officer's work, which seems to intrigue his dinner companion. "We are under great pressure," Xu says, over the din of the restaurant kitchen and the

click of chopsticks. “The leadership asks you to get the materials of the US F-22 fighter aircraft. You can’t get it by sitting at home.”

So you also have to “flip” someone, the professor says, to “travel outside [China] and take the risk.”

“That’s correct,” Xu confirms.

One of Xu’s collaborators at NUAA was Chen Feng, a vice dean with a distinctive pompadour who ran the university’s International Cooperation & Exchange Office. Chen’s duties included issuing speaking invitations to notable foreign technologists, often though not always of Chinese descent. In March 2017 he sent one to an engineer named David Zheng at GE Aviation’s complex outside Cincinnati. “I learned from your online resume that you have accumulated a wealth of engineering experience in well-known companies such as GE Aviation,” it read. The email was a form letter—the only personalization was the name of Zheng’s employer, which Chen had discovered on LinkedIn. But still, Zheng was flattered at the invitation to give his first overseas talk. And he already had a trip to China planned for his college reunion and for a family wedding in his hometown in Anhui province, right next to Jiangsu.

Zheng is a composites expert who worked at GE Aviation on jet engines. The General Electric Co. industrial conglomerate, which once made everything from toasters to television shows, is now in large part a fan and turbine company, and it’s very good at making them. Some are designed to harvest wind energy, and others, locomotive-size, run gas power plants. Still others draw in and compress the air that, when infused with fuel and ignited, propels airplanes.

In GE Aviation’s most advanced engines—such as the $45 million GE9X, which powers the latest-generation Boeing 777—the fan blades and casings are made from composites: hardened, resin-infused carbon fibers of extraordinary lightness and strength. (The LEAP engine developed with Safran is similarly built.) Lighter engines mean planes can carry more passengers or more freight and fly farther with less fuel. And, over time, composite blades are less likely than titanium ones to weaken from the torque of being spun at thousands of revolutions per minute—and less likely to break and fly loose as projectiles.

Even within GE Aviation, details about the design and materials of these engines are inaccessible to most employees. So are aspects of the modeling and testing methods the company has developed. Certain high-stakes safety tests required for Federal Aviation Administration approval destroy an entire engine. Others require more macabre sacrifices: proving that the assemblage can survive bird strikes involves launching bird carcasses of regulatorily specified sizes into its spinning maw. Competitors such as Rolls-Royce Ltd. and Pratt & Whitney have been trying for decades to bring engines with composite fan blades and casings to market. Newer Chinese manufacturers are also working on the problem.

Over the weeks that followed the initial overture, Zheng and Chen exchanged emails, in Chinese, about timing and logistics. Then, in early May, the vice dean’s messages grew more technical. “Is

your work mainly in the design of pod and engine hood, or in the area of blades?" he asked on May 9. Colleagues at NUAA, he relayed, had suggested a title for Zheng's presentation: "Application, Design, and Manufacturing Technologies of Composite Materials in Aircraft Engines." The engineer replied a few days later from Cincinnati to say the suggestions were fine. "However, I am required to sign a technical agreement with the company that I work for here," he wrote. "Therefore, a lot of the work that I have conducted at the company could not be shared."

In hindsight there were red flags in the email Zheng received next. It wasn't from Chen's university email address, but from jastxyj@gmail.com—the same address to which Xu routinely invited MSS job applicants to submit their résumés. And though signed by Chen, it seemed to have been written by someone who hadn't read all the earlier correspondence.

Xu had actually written the email. The GE Aviation engineer had been handed off from the university official who'd found him on LinkedIn to the intelligence officer who would now handle him. As handoffs go, it was clumsy: Xu was writing to ask Zheng to respond to an email Zheng had, in fact, just responded to. But the engineer just assumed that Vice Dean Chen was busy, or maybe bad about checking his email. By the time Zheng arrived in Nanjing on June 1, he'd been assured that his talk wouldn't be expected to touch on anything sensitive.

The trip went smoothly. The morning after Zheng's arrival, Chen and Xu joined him for tea in the lobby of his hotel on the NUAA campus, then took him to lunch. Xu introduced himself as "Qu Hui" and produced a business card identifying him as the deputy secretary-general of the Jiangsu Provincial Association for International Science and Technology Development. In the afternoon the group returned to campus, and Zheng gave his presentation to two dozen people he thought were students and faculty. When questions veered into specific and technical territory, as they often did, he declined to answer. Later, at dinner, Xu presented Zheng with two boxes of tea to go with a $3,500 speaking fee and travel reimbursement. A little over a week later, Xu, under his alias, messaged Zheng over WeChat to thank him. Zheng replied that he would love to come back for another exchange, "as long as it does not involve any non-public information from the company."

For Xu this was a promising start, especially considering that little else seemed to be going well for him. His iCalendar diary entries throughout the spring and summer of 2017 are shot through with grievance. On March 27 he was livid after Zha rejected a meal receipt and rebuked one of their colleagues. "The ingratitude [of a] person like him is shameless," Xu wrote. "Will revenge." A month later, Xu described his relationship with Zha as having dropped to the "freezing point." Zha, he believed, was actively undermining him. On May 4, Xu reveled in the spectacle of "the big cat fight" between Zha and another higher-up. "Watching the show!" he wrote. By June 12 he'd decided that only further office dysfunction could save his career. "The more chaotic and disorderly within the division," he wrote, "the better."

Things were no better outside the office. In early April, right when he was beginning to cultivate Zheng at GE Aviation, Xu was also WeChatting a woman with whom he seems to have had an affair. There had been a quarrel, and Xu wrote that he wanted to hear her voice and see her in person. “It seems we are back to when we first fell in love passionately,” he said. But he was afraid she would cut off contact.

“Don’t you work for the Ministry of State Security?” she replied. “Isn’t it easy to find me?”

“Why can’t we have a normal relationship then?” he pleaded. “Do I have to use special methods?”

On May 19 a morose Xu took stock. “Agitated,” he began the day’s diary entry. “Feeling agitated in the past couple days. Feeling like I am abandoned by the whole world. Work, relationships, and money are not going in the right direction.” As far as Zha was concerned, “we will be using each other to our own ends. I will not help him anymore. It’s whatever now.” The extramarital romance was a shambles: “She wouldn’t even return my text messages. Breakup is real.” And he’d lost money in the stock market. “I got myself into this financial hole. I did it to myself. Sigh, not going to talk about these anymore. Feeling so bad. When is the end??”

That summer and fall brought new indignities. At a dinner in July, Zha “went nuts and said I am poor at management.” A new woman entered the picture, with predictable results: “Heartless,” one entry is titled. “Saw me in the rain yesterday morning, didn’t stop and she walked away with her umbrella.” Her WeChats were perfunctory. “This morning at breakfast, she did not sit next to me again.”

It was amid all of this that Zheng reached out from Cincinnati to propose a second visit. This time Xu, as “Section Chief Qu,” volunteered to handle the logistics for the GE Aviation engineer’s trip himself. Soon Zheng and Xu were in touch over WeChat, where Qu’s account icon was a plump blue cartoon rabbit. Zheng seemed less guarded now. On Jan. 11, 2018, he WeChatted Xu to ask if there was any special research he should do in advance of his next talk, to “try best to meet the need for the exchange.”

Two weeks later, however, Zheng sent worrisome news. GE had recently announced a major restructuring, and there was talk of layoffs at subsidiaries including GE Aviation. Zheng was concerned about losing his job. If that were to happen, he at least wanted to be of use to Section Chief Qu while he still could. “That’s why I am trying my best to collect as much information as possible,” Zheng explained. Xu encouraged his new source to focus on system specifications and design process data.

The document Zheng sent on Feb. 3 made it clear that he’d understood the request. The title was “GE9X Fan Containment Case Design Consensus Review,” and it was labeled “CONFIDENTIAL.” Zheng, it appeared, had access to high-level secrets about his employer’s marquee product. (The GE9X would the next year earn the title of the world’s most powerful commercial jet engine.) Two days later, Xu responded with a set of technical questions—“How are the allowed values for 3D braided structural material and allowed value for design obtained? What are the relevant criteria?”

It was the starting point for discussions with experts in Nanjing when Zheng came back for a second visit, as he was scheduled to do imminently, around the Lunar New Year. Xu also sent instructions for how Zheng could create and copy a directory of all the files on his GE Aviation computer. A little more than a week later, on Valentine's Day, Zheng sent back the results.

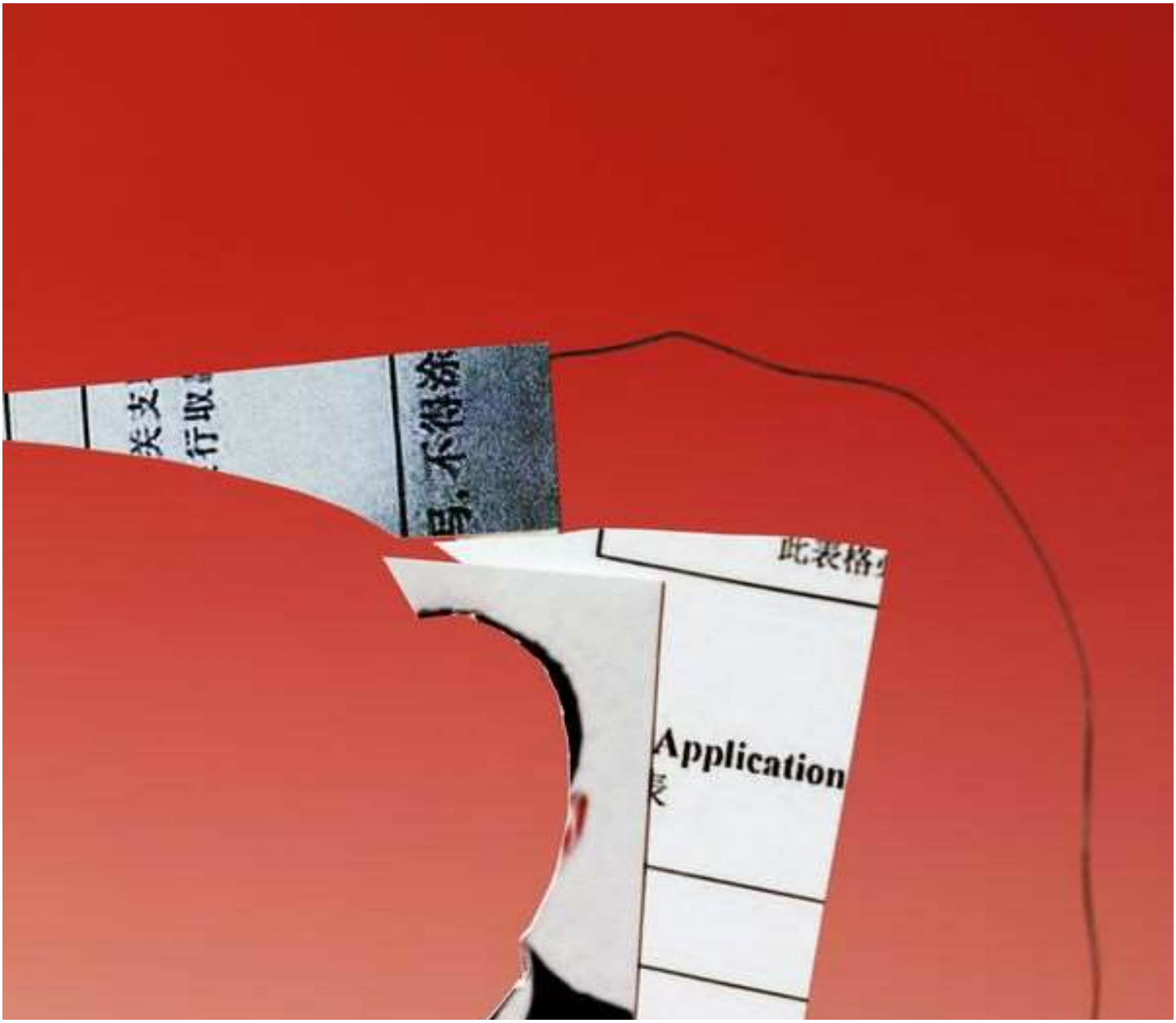
The two were communicating at least every few days, and Zheng's eagerness made him a potential gold mine. It was particularly frustrating, then, when Zheng announced that he couldn't come to China after all, not anytime soon. His boss, he reported, was sending him to France for work in March. "Since there are many things that need to be prepared, he thinks it's inappropriate to take a two-week vacation now," Zheng wrote. "I am so sorry about this!" Xu, a man well versed in the thoughtlessness of bosses, understood. But perhaps, he suggested, they could meet somewhere else? Regrettably, he couldn't come to the US, but if Zheng had time on his France trip, Xu might be able to meet him there.

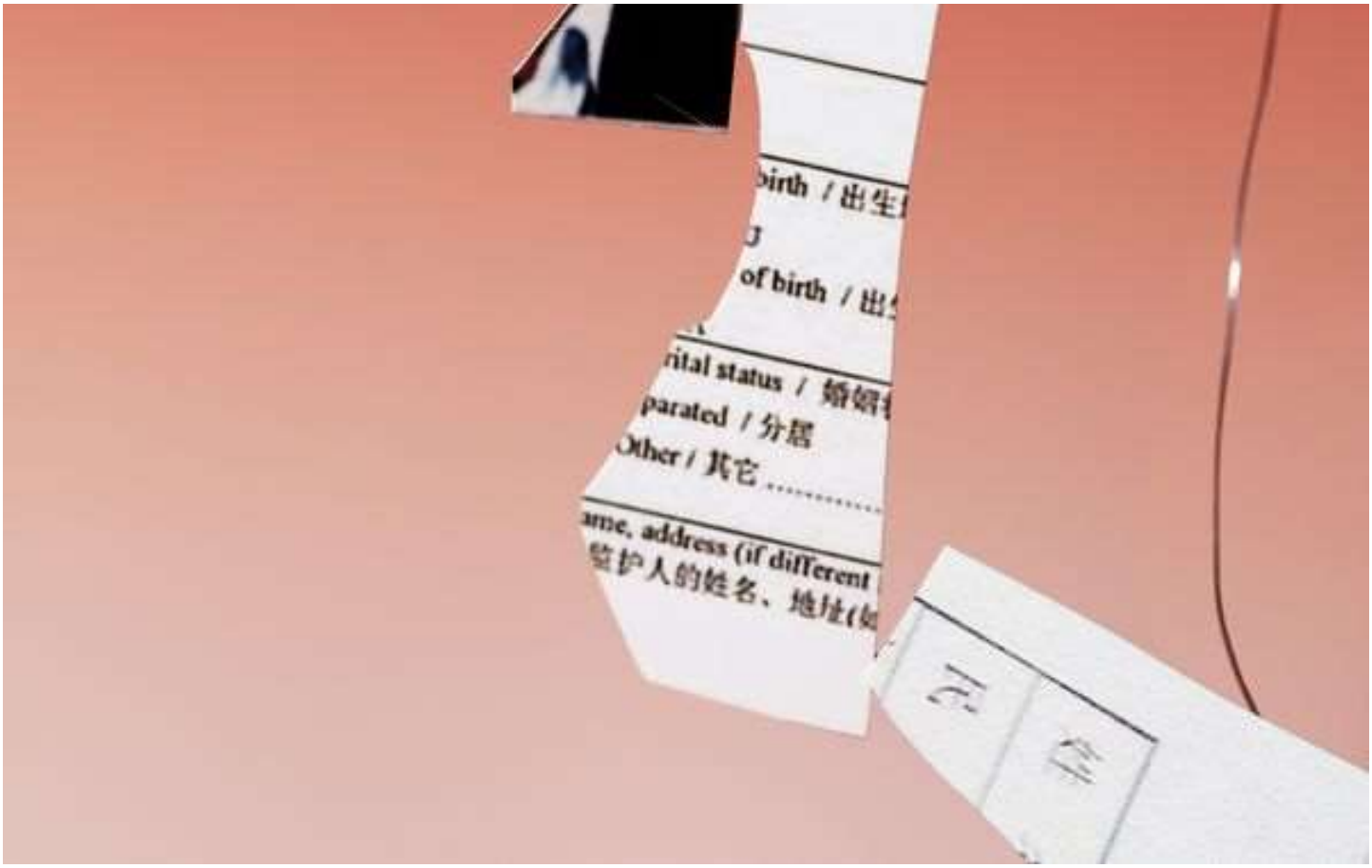
On Feb. 28 they discussed possibilities over the phone. In France, Zheng would be free on the weekends, and he'd always wanted to visit Belgium, the Netherlands, and Germany. Xu asked whether Zheng would have his work laptop with him. Zheng confirmed that he would, and he could easily export any files of interest. "Is there other information that you guys might be interested in?" he asked. "I mean, I can look around and prepare." Xu said that wasn't necessary. "We really don't need to rush to do everything in one time," he explained, "because, if we are going to do business together, this won't be the last time, right?"

Xu was wrong about that. As Zheng spoke on the phone, he was sitting next to Bradley Hull in the FBI agent's car. Hull was listening to and recording the conversation, and he'd scripted Zheng's half of it. Months before, the MSS officer had himself been handed off.

The previous summer, less than a month after Zheng's visit to Nanjing in June 2017, Hull had reached out to members of a special "insider threat" team at GE to inform them that the FBI was investigating an employee for potentially stealing secrets. That employee was Zheng. It's not clear how the FBI learned about him, but either his trip or his correspondence with Xu appears to have set off alarms. GE agreed to cooperate, and the company and the bureau began months of secret collaboration. On Oct. 25, Hull and a small team of agents and prosecutors came to GE Aviation's headquarters for three days of meetings about the case.

In the early afternoon of Nov. 1, Zheng was called into a large auditorium on the GE Aviation campus. There he found two men from the company's security arm. They spoke with him for 10 to 15 minutes, then Hull and another FBI agent walked in. The agents took Zheng's phone. When he asked to call his wife, they handed him one of theirs and asked that he speak to her on speaker, and in English. A search warrant was simultaneously executed at his house, where agents took away electronic devices and the Qu Hui business card from Xu. In the GE conference room, Hull and his colleague interviewed Zheng for seven hours, breaking midway for pizza. When Zheng went to the bathroom, one of the agents went, too. He was free to leave at any time, they told him. They didn't mention that his car had been removed from the parking lot to be searched.






*Photographer: Ina Jang for Bloomberg Businessweek*

After the meeting, Zheng retained an attorney and agreed under a nonprosecution agreement with the US Department of Justice to cooperate with the investigation. In preparing his NUAA presentation, Zheng had transferred onto his laptop five GE Aviation training files that were under export control protection. He hadn't shared the files with anyone in China, but in taking them with him, he'd broken the law. He'd also violated company policy by not informing GE Aviation of the talk. For this he would lose his job, and his $130,000 salary, but for the time being he was placed on unpaid leave. His colleagues weren't told what had happened, in case one of them, too, was an insider threat. To pay the bills, Zheng began driving for Uber Eats.

Much of the rest of his time was spent with Special Agent Hull. An atypical G-man, the Ohio native has an archeology doctorate in stabilized isotope geochemistry from the University of Oxford. He came to the FBI in 2008 as a researcher at the laboratory division in Quantico, Va., where he looked at how to use isotopes in teeth to identify where corpses had come from. After a couple of years, though, he got bored. "I realized I was a very educated ditch digger," he said when asked about it at Xu's trial. He applied to be a special agent and started working counterintelligence, first in Boston, then back in Ohio.

Hull still had the patience of a lab-bench scientist. As his investigation turned toward Zheng's interlocutors in China, it was painstaking and unhurried. Starting with the Nov. 21 WeChat to NUAA's Chen Feng reestablishing contact, each message was written by Hull in consultation with FBI analysts and linguists. The FBI team also benefited from an unusual degree of cooperation from GE. Companies typically try to make insider threats go away as quietly and quickly as possible, even if that means forgoing a real investigation. GE, by contrast, was keen to help. The files Zheng

sent Xu—the ones that so impressed the experts he consulted with—were genuine GE Aviation technical documents, carefully chosen and edited to be highly suggestive but free of actual secrets.

By early March of 2018, Xu and Zheng were down to two potential meeting spots: the town of Fontainebleau, outside Paris, and Amsterdam. "Let's meet at Amsterdam on the 31st," Xu WeChatted. He even settled on a venue: Lasergamen Amsterdam, a laser tag facility west of the city center. Zheng and Hull sent back a screenshot of a hotel reservation in Amsterdam and a train ticket from Paris. On March 21 they sent another tantalizing document, titled "GE Containment Analysis Technical Deep Dive." On the same day, the FBI filed a sealed criminal complaint against Xu. It connected him to more than one of his aliases, quoted extensively from his emails and texts, and mentioned photos that had allowed Zheng to confirm Xu's identity. The strong implication, which would go undiscussed at trial, was that investigators had by this point already gained access to Xu's iCloud account. One logical route in would have been the Gmail addresses he'd used for years to recruit both MSS job applicants and sources—and, it turned out, to register with Apple.

Then, two days before the planned meeting, Zheng WeChatted with one last change: His boss was sending him to Belgium that weekend, he said, to provide some technical support to the Safran branch there. That meant Amsterdam was out. But could Xu meet in Brussels on April 1, Easter Sunday? Xu had little choice but to accede.

Still, he knew he was taking a risk by arranging a source meeting far outside the security of China's borders and on someone else's terms. On March 30, preparing for the trip, he exchanged WeChats with a username most likely belonging to his wife. After a mundane exchange—no, she hadn't seen his special travel pillow—he wrote, "I put a USB drive in the eyeglass box in the middle of the bookcase, and it contains some encrypted documents. If something happens, someone will come to you and tell you the password." The response came within a minute: "Oh my God. Don't scare me like this." The next day, March 31, Xu and a colleague, Xu Heng, flew to Amsterdam and took the train to Brussels, two hours south across the low coastal plain.

That evening, Zheng messaged that he'd just arrived in Brussels. There was a Le Pain Quotidien near his hotel that would be perfect, he reported, in the Galeries Royales Saint Hubert, a collection of stately 19th century shopping arcades in the city center. The cafe upstairs was quiet. "Okay," Xu responded. "I will let you know when I am about to be there."

Zheng was in Brussels, that much was true, but he hadn't just arrived. The hotel room he was writing from was the base of operations for Hull's team. The FBI had settled on the city a while before. Belgium's extradition treaty with the US is part of an overarching set of agreements with each European Union country, some of the strongest and most comprehensive of their type in the world. The drawn-out discussion of different European cities had been a ruse, paced to draw Xu further and further out of his comfort zone.

The next day, April 1, Xu and his colleague arrived at Le Pain Quotidien more than two hours early; he texted Zheng to say they were there at 12:43 p.m. A half-hour later, Zheng replied pretending

that he'd just finished up Easter Sunday lunch with his boss and team. Then at 3:12 p.m. he wrote, falsely, that he'd arrived at the cafe: "I am here now, are you here?"

In Zheng's place were officers of the Belgium Federal Police, who arrested Xu right after he received the message. Xu Heng was also taken into custody. He was carrying multiple SIM card readers and brown envelopes containing €7,720 ($7,814) and $7,000. Because he wasn't part of the arrest warrant, he was soon released. The two men had brought along a 1-terabyte hard drive and some mostly empty memory cards. Xu Yanjun, who was traveling under his real name, had his passport and national ID and was carrying two phones. One was a Huawei Mate S (password: xuyanjun1980) containing, among other things, a list of questions about fan blades. The second was the iPhone with which he had so diligently documented his life.

At his trial, which began on Oct. 18, 2021, in Cincinnati's Potter Stewart U.S. Courthouse, Xu didn't testify. He barely spoke. At one point, Stijn Berrevoets, the Belgian police chief inspector who'd arrested him, stood up from the stand and identified him. At another point, Zheng did the same. But otherwise, the real-life Xu sat on the margins of the proceedings, silently listening to his court-appointed translator as his innermost thoughts were read out loud in a foreign language and parsed in a courtroom 7,000 miles from his home. He did not respond to letters, in English and Chinese, sent to him in jail asking him to speak for this story, and ultimately declined through his attorney to comment.

In the indictment, unsealed when Xu was extradited to the US in 2018, the Justice Department charged him with conspiring and attempting to commit economic espionage and steal trade secrets. “The evidence in this case, nearly all of it, came from his own words. There’s hardly another case like this,” Assistant US Attorney Timothy Mangan said in his closing argument to the jury. “You don’t have to resolve any kind of he-said, she-said dispute. These are his own statements, his admissions.” FBI search warrants to Apple and Google had opened up his iCloud and multiple Gmail accounts, and digital forensics experts at the bureau had mined the contents of the phones recovered at the arrest. (Investigators were not able to recover anything, however, from the iPhone Xu Heng had been carrying. The day after the arrest, someone remotely accessed the device and wiped it clean.)

At trial, Xu’s attorneys didn’t deny that he was an intelligence officer. “He’s a recruiter,” said Ralph Kohnen, of Taft Stettinius & Hollister, in his own closing argument. “He’s affiliated and works for MSS. Nobody’s ever hidden from that.” But that doesn’t mean he succeeded in stealing any actual secrets, or that he was even trying to. The defense was at pains to underline Xu’s flouting of basic espionage tradecraft. “How does a man who is a superspy travel under his own identity?” Kohnen asked the jury. Xu, with his envelopes of cash, his detailed technical questions, and his malware, may have gone right up to the line, his lawyers argued, but he didn’t cross it. “There were no requests for secret information,” Kohnen told the jury. “There was no ‘ask’ there.” And when Zheng suddenly began forking over internal GE documents, it wasn’t up to Xu to tell him what was or was not OK.

“What’s happened here is Mr. Xu, my client, has become a pawn,” Kohnen concluded, “a pawn in the tense place between US industries trying to exploit China and trying to get along with China, right?”

On Nov. 5, 2021, the federal jury convicted Xu on all counts. He faces a maximum sentence of 50 years in prison and $5 million in fines when he’s sentenced this coming Nov. 15. His case also brought resolution to the investigations triggered years before by the Safran hack. Federal prosecutors in San Diego indicted Xu’s MSS supervisor Zha Rong, along with Gu Gen and Tian Xi of Safran Aircraft Engines Suzhou, and seven others connected to the Jiangsu branch of the MSS for a conspiracy to hack more than a dozen aerospace companies. The Safran workers were, unsurprisingly, fired. Unless they leave China, none of those defendants are likely to face trial.

GE and Safran, which both cooperated with federal authorities and whose employees testified at Xu’s trial, declined to comment for this story. Chen Feng, the NUAA administrator alleged to have collaborated with Xu, did not respond to messages, nor did the university. *Bloomberg Businessweek* could not find contact information for the other alleged MSS conspirators.

In Arizona, Honeywell’s Arthur Gau was also indicted and pleaded guilty to exporting controlled information without a license. On March 10, 2022, four months after testifying in Xu’s trial, and three years after being fired by Honeywell, he was sentenced to three years’ probation and a $10,000 fine. Gau’s federal public defender did not respond to messages, and Honeywell did not respond to requests for comment. The FBI’s Hull was promoted in early 2020 to supervisory

special agent, in large part because of his work on the case. Zheng found a new job shortly after GE Aviation let him go, though at his request the new employer was not named at trial. He's less interested in sharing information than he once might have been. He declined through his attorney to speak for this story. And he didn't respond to messages on LinkedIn. –*With Crystal Tse*

*Read next: Russia's Conspiracy-Theory Factory Is Swaying a Brand-New Audience*