THE AUSTRALIAN

Our new world war

The hunt for a crack team of Chinese hackers reveals a terrifying glimpse of the future.

By **DAVID E. SANGER**

FROM **THE WEEKEND AUSTRALIAN MAGAZINE** July 14th, 2018 12 MIN READ

"There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."

– James Comey, then FBI director, October 5, 2014

The boxy 12-storey building along Datong Road on the outskirts of Shanghai was easy to overlook. In a city of 24 million people – China's most populous, and among its most high-tech – it was just another bland, white high-rise. The only hint that the unmarked building was actually a base for the People's Liberation Army and its pioneering cyber force, Unit 61398, came if you looked at the protections surrounding the tower – or the security forces who came after you if you dared to take a picture of it. The digital addresses of many of the hackers stealing terabytes of data from US corporations – everything from the designs of the F-35 aircraft to the technology of gas pipelines, from data collected by healthcare systems to Google's algorithms and Facebook's magic formula – pointed straight back to Pudong, the run-down neighbourhood of massage - parlours and noodle joints surrounding the building.

But the trail of evidence fizzled out there, at the level of the neighbourhood. The Chinese had so clouded the final termination addresses of the hackers' systems that it seemed impossible to trace the thefts back to any one building. That was driving Kevin Mandia – a former air force intelligence officer leading one of the several private investigations into Chinese intrusions – absolutely crazy. It seemed impossible that the hacks he was tracing came from anywhere but the highly defended high-rise. He just couldn't prove it. Yet.

While Mandia was building a client base of more than 100 companies for his cybersecurity firm Mandiant, he had been tracking a Chinese hacking group with clear ties to the country's military. His firm called the group "Advanced Persistent Threat 1 (APT1)", the awkward term the industry uses to identify and number malicious state actors in cyberspace that aren’t going away. Mandia was certain the hackers were part of Unit 61398, but he also knew that accusing the Chinese military directly would be a huge step. Over seven years he had compiled a list of the unit’s suspected attacks on 141 companies across nearly two dozen industries and he needed solid evidence before he could name them. Yet as long as none of his investigators could get inside the building, whether physically or virtually, to identify the thieves, the Chinese would keep denying that their military had been tasked with stealing technology for state-run Chinese firms.

Kevin Mandia. Picture: AFP

Ever resourceful, Mandia’s staff of former intelligence officers and cyber experts tried a different tack. They might not be able to track the IP addresses to the Datong Road high-rise itself, but they could actually look inside the room where the hacks originated. As soon as they detected Chinese hackers breaking into the private networks of some of their clients (mostly Fortune 500 companies), Mandia’s investigators reached back through the network to activate the cameras on the hackers’ own laptops. They could see their keystrokes while actually watching them at their desks. (Mandiant, now a part of FireEye, has since denied that it “hacked back” or turned on the cameras, insisting that everything it saw the hackers do was because its investigators had permission from the victim companies to observe the traffic the hackers were sending into their systems. In other words, they argue that the hackers themselves exposed their own activities, and that Mandiant was just a passive observer.)

The Chinese hackers, just about all of them male and most in their mid-20s, carried on like a lot of young guys around the world. They showed up at work about 8.30am, checked a few sports scores, emailed their girlfriends, and occasionally watched porn. Then, at 9am, they started methodically breaking into computer systems around the world, banging on the keyboards until a lunch break gave them a moment to go back to the scores, the girlfriends and the porn.

One day I sat next to some of Mandia’s team, watching the Unit 61398 hacking corps at work; it was a remarkable sight. “They were such bros,” says Andrew Schwartz, a communications specialist. “But they were prodigious thieves.” They were also thieves with multiple employers: some moonlighted as hackers for Chinese companies, making it unclear whether they were stealing on government or corporate orders.

This was what the new cold war between the world’s two largest economies looked like up close. It bore no resemblance to the more familiar conflicts of past decades. China understood the keys to re-emerging as a global power after a -centuries-long hiatus: artificial intelligence, space technology, communications, and the crunching of big data. And of course, outmanoeuvring its only real challenger, the US.

Yet Washington had struggled to define exactly what China was in relation to the US: a potential adversary? A sometime partner? A vital market for US goods? An investor? China was all of these, and more, which is what made it such an intractable and fascinating foreign policy problem.

Naturally, Unit 61398 – formally the 2nd Bureau of the People's Liberation Army's General Staff Department's 3rd Department – existed almost nowhere in the Chinese organisational charts. But by 2013 it had been in the sights of US intelligence agencies for several years. The day before Barack Obama was elected president in 2008, another State Department cable voiced official concerns about how frequently the unit was breaking into US government sites. Obama himself had felt the sting: the Justice Department contacted him during his 2008 campaign to explain that the Chinese were deep inside his own campaign computers, presumably looking to understand how their country's complex relationship with Washington would change with the election of a young senator who had barely been on China's radar. "That was our early taste of this problem," Denis McDonough, who became Obama's chief of staff, later told me.

By 2012, Mandia's staff were looking at Unit 61398's actual Chinese hackers, watching them log in and steal blueprints and identification numbers from RSA, the US company best known for making the SecurID tokens that allow employees at military contractors and intelligence agencies to access their email and corporate networks. The hackers then used the data stolen from RSA to get into Lockheed Martin.

While Mandia was keeping an eye on this, another hack – perhaps the most troubling and mystifying – was taking place out of his view in Canada. The target was a subsidiary of Telvent, a company that designs software that allows oil and gas operators to turn their pipelines on and off remotely and to control the flow of energy supplies. Telvent held the blueprints for half the oil and gas pipelines in the Western hemisphere. In September 2012, the company had to admit to its customers that an intruder had broken into the company's systems and taken project files. No one could quite figure out whether this was the work of Unit 61398, which looked probable, or some other Chinese group. Nor was the motive clear. Were the hackers planning to take control of the pipelines, perhaps in time of war? Or were they simply industrial thieves, looking to steal the software so that they could replicate similar pipelines in China or elsewhere? While the US and the Canadians investigated, the findings, if any, were never made public. The mystery remains.

John Brennan. Picture: AP

Even while the Telvent hack was under way, the Chinese government was preparing another, far more sophisticated covert operation in Washington. It would ultimately yield them a map of how the US government operates, populated with the most intimate details of the lives of 22 million Americans – almost seven per cent of the country's population. The data was extracted from a rather boring corner of the US Government, the Office of Personnel Management – a vast bureaucracy that acts as the record-keeper for the millions of people who have worked, currently work, or have applied to work for the government whether as employees or as contractors.

OPM was responsible for gathering the information needed to perform background checks on almost anyone who needed a "secret" or "top secret" security clearance. Five million Americans held those clearances in 2014, when China cracked the repository wide open. To obtain a security clearance from the US government, prospective employees and contractors have to fill out an exhaustive 127-page form – Standard Form 86, or SF-86 – in which they list every personal detail about their lives. Every bank account, every medical condition, every illegal drug they used in college. They must detail information about their spouses, their kids, their ex-spouses, and their affairs. They even have to name every foreigner they have come into close and continuing contact with for the past decade or so.

The data provided in the SF-86 – and the reports of the investigators who subsequently use that information to conduct background checks – constitute a treasure trove for any foreign spy agency. Here, in one place, resides an encyclopaedia of America's national-security elite: not just names and Social Security numbers, but information about where people work, where they have been posted around the world, and whether they are so deeply in debt that they may be easy marks for recruitment. The personal histories offer a wealth of potential blackmail information, as well as clues about how to impersonate a family member or friend online.

From the start, OPM director Katherine Archuleta and her staff were clueless about what was happening in their networks. The agency's computers had no warning system to alert them that a foreign intruder was lurking in the system and had begun to siphon data out of it at night. The best guess of the investigators, who later spent over a year trying to piece together a timeline of the hack, was that the hackers most likely cracked OPM’s systems repeatedly in late 2013. For about a year they operated undetected in the network and systematically exfiltrated the SF-86 forms and written reports on background investigations. At some point during the summer of 2014, the SF-86 forms for 21.5 million people were copied from OPM’s network. By December, 4.2 million personnel files for current and former federal employees, with their Social Security numbers, medical histories and marital status, had been stolen. And by March 2015, 5.6 million fingerprints had been copied and spirited away. OPM itself never noticed how much data was flowing from its systems, possibly because the Chinese politely encrypted the data on the way out the door, a step that OPM itself hadn’t taken to protect the mountain of sensitive information it held.

It wasn’t until April 2015, when a security contractor working for OPM flagged an error on a domain name – in this case “opmsecurity.org” – that the agency’s cyber team began to investigate in earnest. The domain had been operating for about a year, but no one at OPM had created it. Worse, it was registered to “Steve Rogers” – a fictional character whose superhero alter ego, Captain America, is one of the Avengers. A second website, discovered shortly afterwards, was registered to “Tony Stark”, aka Marvel superhero Iron Man. Connoisseurs of hacking techniques immediately observed that a Chinese military group had, in the past, left similar odes to the Avengers. Fifty days of radio silence followed as OPM scrambled to understand what had happened. The security company Cylance helped sort through the wreckage; a technician working on the case wrote a pithy email to the company’s chief executive: “They are f--ked btw.” That was a decent summation. But the damage wasn’t limited to the employees whose data were retained by OPM.

While the intelligence agencies knew better than to keep the records of their operatives on the OPM system – partly because they didn’t trust it – the top two officials at the CIA, director John Brennan and deputy director David Cohen, quickly came to the conclusion that scores of their operatives abroad were now vulnerable. Many had been posted to China under “official cover”, meaning they were posing as diplomats. To make that cover convincing, they had a State Department history and a file, but sometimes with career gaps or other clues the Chinese might pick up on.

It became apparent at the CIA and other intelligence agencies that the problem was even more complex. In an age of big-data techniques, the database was far more valuable than its millions of individual files. It allowed the Chinese to compare the OPM files to their own intelligence resources and even to Facebook profiles and the digital dust that diplomats and spies left in their past postings. It was easier than ever before to unmask CIA operatives. And the problem was not limited to existing officers: those still in training, or awaiting assignments, could also be identified. Soon dozens of postings to China were cancelled. As Robert Knake, a former director of cybersecurity policy issues in the Obama White House told me, "a whole bunch of CIA case officers" could be "spending the rest of their careers riding desks".

View of the building of Unit 61398. Picture: AP

The OPM hack offered a glimpse of the future, of what happens when old-fashioned espionage meets the new world of data crunching. Investigators looked at the hack of Anthem, a health-care company, in a new light; while the OPM hack was still under way, Chinese hackers had been caught stealing upward of 78 million records – raising the possibility that all of these databases were being combined to get a deeper picture of Americans.

This was entirely new territory for the intelligence community and terrifying in its scope. But, at least in public, the Obama administration never levelled with the 22 million Americans whose data was lost – except by accident. Federal employees were sent letters telling them some of their information might have been compromised, and they were offered several years of free credit-monitoring, as if the information had been stolen by criminals. The White House refused to blame Beijing.James Clapper, the director of national intelligence, even admitted his grudging respect for the hackers in an interview. "You have to kind of salute the Chinese for what they did," he said.

In the cyber world today, we are somewhere around World War I. A decade ago there were three or four nations with effective cyber forces; now there are more than 30. The production curve of cyber weapons produced over the past 10 years roughly follows the trajectory of military aircraft. The new weapon has been fired, many times, even if its effects are disputed. The best estimates suggest there have been upward of 200 known state-on-state cyberattacks over the past decade or so – a figure that describes only those that have become public. And, as in World War I, this glimpse into the future has led nations to arm up, fast. The US was among the first, building so-called "Cyber Mission Forces"; 133 teams totalling more than 6000 troops were up and running by the end of last year.

There are the "Seven Sisters" of cyber conflict – the US, Russia, China, Britain, Iran, Israel and North Korea – although nations from Vietnam to Mexico are getting involved. Many have started at home by testing their cyber capabilities against dissidents and political challengers. But no modern military can live without cyber capabilities, just as no nation could imagine, after 1918, living without airpower. And now, as then, it is impossible to imagine fully how dramatically this invention will alter the exercise of national power.

Edited extract from The Perfect Weapon – War, Sabotage and Fear in the Cyber Age, by David E. Sanger (Scribe, $32.99), out Monday.