CHINA'S HACKER KING

Wan Tao's journey from cyberwarrior to cybercop provides a rare glimpse into the underground world of Chinese hackers

BY HANNAH BEECH/BEIJING

Photographs by Zachary Bako for TIME

ON THE GRID Wan now runs an IT company that helps other organizations defend against cyberattacks

WAN TAO STABS THE KEYboard with his middle fingers. It's the only way he types—a defiant gesture expected of an online warrior who once led China's patriotic hacker brigade. For years, Wan, who was known by the online moniker Eagle, terrorized cyberspace, taunting anyone he believed wanted to humiliate his homeland. One of China's most famous *hongke*, or red hackers, he infiltrated everything from the inboxes of Taiwan politicians to a White House website, where he briefly planted the Chinese flag. "I was the ultimate angry young man," says the founder of China Eagle Union, a collective of Chinese hackers whose hit-and-run forays into foreign computer networks gained them the attention of Western intelligence agencies. "In cyberspace, I felt like I had complete freedom to express myself."

At a time of peace between the world's major powers, the rise of China's hackers points to a troubling new front in global conflict. The list of targets believed to have been infiltrated by Chinese hackers includes: the U.S. Chamber of Commerce, Google, American military contractors and power plants, Western foreign correspondents working in China, Amnesty International, the Tibetan government-in-exile, American drug manufacturers, the European Union, the New York City–based Council on Foreign Relations, even the Pentagon. Hacking out of China ranges from incursions by the state to malfeasance by patriotic individuals like Wan, and various shades in between. Last year General Keith Alexander, head of the U.S. Cyber Command, said China had stolen "a great deal" of American military technology through hacking. FBI Director Robert Mueller predicts that cybercrime by Chinese and other actors will soon replace terrorism as America's biggest threat.

Hacking a government or a company is hardly the exclusive domain of Chinese techies. Russia and Iran have been fingered by the U.S. government for their efforts to compromise top-secret American computer systems. It would be naive to expect the U.S. Cyber Command not to be interested in breaching China's online defenses. In 2011, China's People's Liberation Army (PLA) formed a so-called Blue Army of officers to combat what Beijing says are mounting attacks on its own computer networks. Nor are states the only actors in this shadowy war. Earlier this year, Anonymous, the antiestablishment global hacker group, broke into the computer systems of the U.S. Federal Reserve and the U.S. Department of Energy. Perpetrators of industrial espionage know no geographical boundaries.

Still, with an authoritarian regime overseeing a vast computer-savvy populace, China presents a unique menace in cyberspace. Chinese online espionage targets both foreign state secrets and technological innovations as well as organizations that are perceived to embarrass China, like NGOs critical of Beijing's human-rights record. It's impossible to estimate how many Chinese computer geeks work directly for the state. Beijing has repeatedly rejected accusations of official involvement in hacking. But China's denials run counter to the estimations of Western security experts and intelligence agencies, who have become more vocal in fingering Chinese hackers for sustained and sophisticated attacks on foreign IT systems. "[China has] so many more people who are able to hack than any other country," says Murray Jennex, a cybersecurity expert at San Diego State University. "This could get real serious, real fast."

When uncovering a months-long assault on global energy companies traced to Chinese computers, IT security firm McAfee noted that the hackers, who accessed massive amounts of confidential information, worked only on weekdays, logging in at 9 a.m. Beijing time and finishing at 5 p.m. McAfee added that "the attackers employed hacking tools of Chinese origin and that are prevalent on Chinese underground hacking forums." The U.S. security firm also blames Chinese hackers for well-coordinated attacks on Google, Yahoo and many other tech firms. A December intelligence report by another cybersecurity company, Mandiant, found that more than 30 employees of Western media organizations were being targeted by PLA-linked computers based in Shanghai, according to one of the hacking victims, the New York *Times*. Mandiant accuses China of using these same computers for earlier online strikes on more than 100 American firms.

WITH AN AUTHORITARIAN REGIME OVERSEEING A VAST COMPUTER-SAVVY POPULACE, CHINA PRESENTS A UNIQUE MENACE IN CYBERSPACE

It's not just China's official cyberarmy that has been dispatched to the front lines. Primed by heavy doses of nationalist education that emphasize how China was ravaged by Japanese and Western powers, a corps of angry young Chinese men—yes, most are men—have flocked online to flex their muscles and express their patriotism. Their actions could be dismissed as harmless pranks—defacing a Western government's website rather than, say, stealing nuclear data or industrial secrets. But *hongke* machismo feeds a more malicious form of state-sponsored hacking, and it is telling that China's patriotic hackers have not been punished at home for their overseas attacks. While Chinese hackers boast about their exploits online, it's rare to hear one articulate why he chose to hack for nationalist reasons. The story of Wan Tao, now 41, and his China Eagle Union—which at its height boasted hundreds of members who raided foreign computer systems with the government's tacit approval—gives an inside glimpse into the underground world of Chinese hackers: their motivation, exploitation and, in some cases, redemption.

Born in 1971, Wan was a dutiful only child, his mother a teacher and his father a cadre in the powerful Ministry of Railways. But in 1989, when he was in high school, the democracy movement began flowering in Beijing. Even in his small town in eastern China's Jiangxi province, the spirit of reform galvanized Wan. He ran away from home and made contact with local democracy activists. Then the tanks rolled into Tiananmen Square.

Wan had the qualifications to enter prestigious Peking University to study history. But his family knew that particular academic department was one of the crucibles of the crushed student democracy movement. Instead, his parents instructed him to study at Beijing's Jiaotong University. The major forced upon him? Accounting. Wan found solace in the college's computer lab, where a primitive virus happened to be devastating

Security code *A sensor door lock at Wan's new operation. He says he used to hack foreign outfits out of nationalistic pride—and just to show that the Chinese were technologically capable of it*

ZACHARY BAKO FOR TIME

hard drives. Wan was fascinated. "A virus was such a small thing, but it could have such power," he recalls. "I wanted my own power." In 1992, Wan designed his first virus and unleashed it. A few months later, his formatting virus had spread nationwide. Even his mother's office computer in Jiangxi was infected.

Hot Shot

AFTER GRADUATING FROM COLLEGE IN 1993, Wan worked for PricewaterhouseCoopers as an auditor. It was a decent job, but Wan nursed anger at his ideologically pliant parents and at a society he felt was "full of lies." He spent his nights on Internet bulletin-board systems—an exhilarating space where patriots expressed themselves freely. "I took my hatred of society and transferred it to Japan, to countries that were humiliating China," he says. "This was the only acceptable way to be angry in China." In 1997, on the 60th anniversary of Japan's brutal invasion of China, Wan says he flooded the Japanese Prime Minister's inbox, causing it to malfunction. The 1999 NATO bombing of China's embassy in Belgrade fired him up even more. Wan left a taunting note on a U.S. Army website. "I never stole information," he contends. "But I wanted to prove that China could compete with the West."

By the late '90s, Wan established his own IT company and began compromising the freedom he so cherished as part of the hackers' rebellious ethos. He helped the local Public Security Bureau monitor and censor Internet chat rooms. In 2000, he formed a club that would become the China Eagle Union. Patriotic businessmen donated cash for the hackers' online raids. "We thought it was our responsibility to defend China," he recalls.

Yet for a rebel who teethed on dissent in high school and reveled in the independence afforded by the Internet, Wan also realized he was being used by the state. Just as his hacking union was attracting more members—mostly male acolytes who followed him with the intensity of boy-band fans—he began questioning its mission. In 2005, anti-Japanese protests broke out again in China. This time, however, Beijing clamped down on the anti-Japanese fervor, lest it morph into a broader movement against the Chinese government. Once given free rein by the authorities to fulminate against foreigners, Wan was ordered by authorities to delete inflammatory content from his website.

The Chinese Internet is a different place from when Wan began hacking in the 1990s. Then, a computer was a rarity, one of the few ways for Chinese to reach out to the world and express their individuality. Now more than half a billion Chinese have Internet access—albeit in a censored form—and most are logged on to social media. While China's new leader Xi Jinping seems intent on harnessing nationalism for what he calls a "great renewal," the Chinese appear more preoccupied these days with domestic issues, like official graft, income inequality and environmental degradation. In recent months, online exposés have brought down a clutch of overfed, mistress-laden Communist Party officials. "The only way to solve China's problems is to face internal problems first and then external problems," says Wan. "We can't always blame outside forces." Today, he publicly disassociates himself from red hacking. "The most important thing about being a good hacker is being independent," says Wan. "If you do something for the government, you have lost a heart filled with freedom."

Some of China Eagle Union's original members are now successful businessmen who outgrew planting malware on foreign websites. Another is a waitress. But a number of Eagle's hackers met more complicated fates, especially when they fell prey to avarice. Several, admits Wan, were pressured to hack officially for the state after being caught doing something illegal online by Chinese cyberpolice. One took money from a Chinese state-owned enterprise that stole online data from a competitor. Little Dragon, one of Wan's closest friends, was sentenced to seven years in jail for endangering national security. Is Wan ever tempted to joust again with cyberwarriors across the globe? He shakes his head. Yet, he adds: "I'm still a hacker in spirit. I always will be."

Wan now runs an IT security company called Intelligence Defense Friends Laboratory, which counts top Chinese tech firms and NGOs among its clients. Half his employees, who crowd cubicles in an office on the fringes of Beijing, used to be members of China Eagle Union. One is Pei Weiwei, a 24-year-old who writes Internet security software and admits to having created a couple of computer viruses. (He says he has never released them.) Although Pei thrilled to the idea of being a *hongke*, he also knew the limits imposed by his nation's political system. "The culture and spirit of hackers can only develop well in a free environment," he says. "Chinese society doesn't tolerate unique people."

The only sign that Wan's office is not just another Chinese start-up comes from a closet-size lair accessed by a fingerprint sensor pad. Inside the darkened space, one screen churns out paragraphs of code. Another displays a world map dotted with red circles. Each circle, says Wan, represents a place being targeted by hackers. "It's like they're all shouting, Look at me!" says one of China's most notorious former red hackers, pointing to the flares of online espionage. "Don't worry, I'm watching you." —WITH REPORTING BY CHENGCHENG JIANG/BEIJING ■