China Tries Its Hand at Pre-Crime

Shai Oster and Keith Zhai

March 7, 2016

China's effort to flush out threats to stability is expanding into an area that used to exist only in dystopian sci-fi: pre-crime. The Communist Party has directed one of the country's largest state-run defense contractors, China Electronics Technology Group, to develop software to collate data on jobs, hobbies, consumption habits, and other behavior of ordinary citizens to predict terrorist acts before they occur. "It's very crucial to examine the cause after an act of terror," Wu Manqing, the chief engineer for the military contractor, told reporters at a conference in December. "But what is more important is to predict the upcoming activities."

The program is unprecedented because there are no safeguards from privacy protection laws and minimal pushback from civil liberty advocates and companies, says Lokman Tsui, an assistant professor at the School of Journalism and Communication at the Chinese University of Hong Kong, who has advised Google on freedom of expression and the Internet. The project also takes advantage of an existing vast network of neighborhood informants assigned by the Communist Party to monitor everything from family planning violations to unorthodox behavior. A draft cybersecurity law unveiled in July grants the government almost unbridled access to user data in the name of national security. "If neither legal restrictions nor unfettered political debate about Big Brother surveillance is a factor for a regime, then there are many different sorts of data that could be collated and cross-referenced to help identify possible terrorists or subversives," says Paul Pillar, a nonresident fellow at the Brookings Institution.

Building a crystal ball to predict and prevent terror attacks is the ultimate goal of crime fighters the world over. But, so far, more data has just meant more noise, security experts say. "There are not enough examples of terrorist activity to model what it looks like in data, and that's true no matter how much data you have," says Jim Harper, a senior fellow at the Cato Institute. "You need yeast to make bread. You can't make up for a lack of yeast by adding more flour."

China was a surveillance state long before Edward Snowden clued Americans in to the extent of domestic spying. Since the Mao era, the government has kept a secret file, called a dang'an, on almost everyone. Dang'an contain school reports, health records, work permits, personality assessments, and other information that might be considered confidential and private in other countries. The contents of the dang'an can determine whether a citizen is eligible for a promotion or can secure a coveted urban residency permit. The government revealed last year that it was also building a nationwide database that would score citizens on their trustworthiness.

New antiterror laws that went into effect on Jan. 1 allow authorities to gain access to bank accounts, telecommunications, and a national network of surveillance cameras called Skynet. Companies including Baidu, China's leading search engine; Tencent, operator of the popular social messaging app WeChat; and Sina, which controls the Weibo microblogging site, already cooperate with official requests for information, according to a report from the U.S. Congressional Research Service. A Baidu spokesman says the company wasn't involved in the new antiterror initiative. Tencent and Sina's Weibo didn't respond to requests for comment.

China Electronics Technology, which got the antiterrorism job in October 2014, had operating revenue of 164 billion yuan ($25 billion) in 2015. Apart from supplying the Chinese military with radar and electronic warfare systems, the company has played a leading role in the country's ambitious space program.

Much of the project is shrouded in secrecy. The Ministry of State Security, which oversees counterintelligence and political security, doesn't even have its own website, let alone answer phone calls. Only Wu, the engineer at China Electronics Technology, would speak on the record. He hinted at the scope of the data collection effort when he said the software would be able to draw portraits of suspects by cross-referencing information from bank accounts, jobs, hobbies, consumption patterns, and footage from surveillance cameras.

The program would flag unusual behavior, such as a resident of a poor village who suddenly has a lot of money in her bank account or someone with no overseas relatives who makes frequent calls to foreigners. According to Wu, these could be indicators that a person is a terrorist. "We don't call it a big data platform," he said, "but a united information environment." In China, once a suspect is targeted, police can freeze bank accounts and compel companies to hand over records of his communications.

Another China Electronics Technology executive, who requested anonymity because he isn't authorized to speak publicly, says the antiterrorism software would first be tested in territories where Chinese authorities are struggling to stamp out sometimes violent opposition to Communist rule by ethnic minorities. He says the pilot had a better chance of success than a nationwide program, because it's focused on the 22 million residents of the sparsely populated Xinjiang territory in China's northwest and the 3 million in mountainous Tibet.

Brookings's Pillar is skeptical. "No system of surveillance and exploitation of intelligence can stop everything," he says. But Tsui, the Hong Kong professor, says if anyone has a chance of coming up with a workable high-tech Big Brother, it's the Chinese. The lack of privacy protections means that China's data sniffers are more practiced than those in the West. "The people who are good at this are good because they have access to a lot of data," he says. "They can experiment with all kinds of stuff."

The bottom line: *A top Chinese military contractor is building a data analytics platform to help authorities identify terrorists before they strike.*