How Activists Are Fighting China's Censorship Machine

Shelly Banjo @sbanjo More stories by Shelly Banjo

The face of dissent isn't easy to recognize in modern China. Laborer Quan Shixin spends most days planting trees and spraying pesticide in a man-made forest on the outskirts of Beijing. She makes less than $10,000 a year and never went to university—not the kind of person you'd expect to be steeped in such things as end-to-end encryption, virtual private networks, or cryptographic authentication. But in her spare time, Quan has learned to bypass the country's Great Firewall, the digital blockade separating the global internet from China's 800 million web users. With such a set of web tools, she fights what she calls unfair actions by her local government.

The 43-year-old says she had to get more tech savvy after local officials seized her village's land for commercial development without what she viewed as proper compensation. Friends introduced her to digital tools to help her communicate with like-minded people. She uses what she's learned to file petitions appealing to the central government to intervene in local cases and to blow off steam on social networks such as Twitter that are banned inside China. "The wall is becoming higher and higher," says Quan, who was jailed twice last year for posting controversial remarks on social media. "But if I don't speak out, I feel suffocated. Expression is a basic right."

Quan's progression from frustrated peasant to digital dissident is one example of the cat-and-mouse game that activists, software engineers, and everyday web users play to stay a step ahead of Beijing's censors. President Xi Jinping's government is one of the most restrictive regimes the internet has ever seen. Thirty years after the pro-democracy protests in Tiananmen Square, China spends about $180 billion a year on surveillance, security, police, censorship tools, and other forms of domestic security. Activists with once-robust accounts on social media have gone silent. Hundreds of VPN providers, which help web users circumvent internet controls, are no longer available. The country's tech giants employ tens of thousands of content reviewers and artificial intelligence-enabled blacklists to screen out banned words and images.

Yet a community of digital dissidents continues the fight, maneuvering to stay ahead of the Great Firewall by convening on open-source coding platforms such as GitHub and on private messaging services, including Signal and Telegram. Their efforts include operating platforms that republish social media posts that were initially blocked, web browsers that allow Chinese users to access barred websites, and blockchain-based messaging services that make it almost impossible to delete controversial posts. Some activists teach persecuted groups,

such as the Muslim-minority Uighurs, how to use encrypted messaging software to communicate with human-rights groups.

"Any tool we can get out there, even if it just works for the moment, that makes it harder or more expensive for the censors will show them that we're still fighting," says Arturo Filastò, founder of the Open Observatory of Network Interference, a global internet censorship monitoring project under the Tor Project, which created the popular private encrypted web browser Tor.

Censoring Speech About China's President

Number of censored terms related to President Xi Jinping that were added to blacklists employed by the Chinese livestreaming and chat app YY since June 1, 2016

Data: Citizen Lab

One of the longest-running censorship fighters is GreatFire.org, a website started by a team of anonymous activists in 2011 to track and evade China's cyberpolice and call attention to blocked websites. Among other tools, the group created a web browser downloaded by more than 1.1 million people—Chinese web users make up 86% of the site's traffic—and FreeWeChat, a website that tracks censored posts on the ubiquitous WeChat messaging app. To bypass the Great Firewall, the group hosts its sites via Android apps that run on Amazon Web Services, the online retailer's cloud service. AWS encrypts all its web pages so Chinese censors can't pick and choose what it blocks without blocking everything hosted on AWS servers, including data hosted online by banks.

"Imagine cutting off access to online entertainment, gaming, banking, finance, e-commerce," a man who identifies himself as a GreatFire co-founder and goes by the online pseudonym Charlie Smith said in emailed responses. He declined to give his real name because he still lives in China and fears Beijing's reprisal. "They simply cannot stop what we are doing, because it would have a huge knock-on effect." He said the government's censorship infrastructure is "fundamentally flawed" and that will become increasingly apparent as more Chinese internet users find their way to GreatFire.org.

The cracks in China's internet barricade are also apparent in Beijing's VPN crackdown. Since 2017, a number of VPN users and service providers have been sentenced to prison, and Apple Inc. has removed hundreds of VPN apps from its app store, according to media watchdog Freedom House. Yet since the crackdown, the number of people in China using VPNs has risen. In the first quarter of 2019, 35% of Chinese web users utilized a VPN, up from 31% two years ago, according to market research firm GlobalWebIndex. That compares with 60% of web users in Indonesia, the highest share of VPN users globally, and 22% in the U.S. More than half of Chinese VPN users do so for routine activities such as accessing better music and TV shows; 41% of them use VPNs to access social networks or blocked news sites.

"Maintaining VPNs is like building sand castles on a beach. They keep getting washed away," says Harold Li, vice president of ExpressVPN, a provider incorporated in the British Virgin Islands. (He declined to disclose where the company is based.) Li says his strategy has been to "build those sand castles more quickly and in more hidden spots." It's about more than making money, he says. The company is working to "protect key freedoms online

—of expression, association, access, and privacy."

Quan, the Beijing laborer, first started using VPNs a decade ago to read news and watch YouTube videos. After the government seized her village's land in 2013, she says formal petitions to Beijing asking for rightful compensation from local authorities were ignored. She took to Chinese social media accounts to complain, but her accounts were suspended on platforms such as microblogging site Weibo in 2015. China's Office of the Central Cyberspace Affairs Commission didn't respond to a faxed request for comment.

Quan resorted to using a VPN to access Twitter in 2016 and has gained 11,000 followers. Last year she posted comments critical of Chinese leaders. Days later, she says, authorities showed up at her door and threw her in jail for 10 days. Quan was arrested a second time a few months later for discussing petitions filed against the government in a WeChat group of 500 people. The second time, she says, she was imprisoned for almost a month.

Quan says she remains vigilant in her pursuit of justice. She never married and has no children, and her parents have died. She alone will suffer the consequences of her activism. When police officers ask her to give up social media and the tools she uses to bypass China's censors, she refuses. "What difference would there be between us and animals if we didn't even have a voice?" she says.