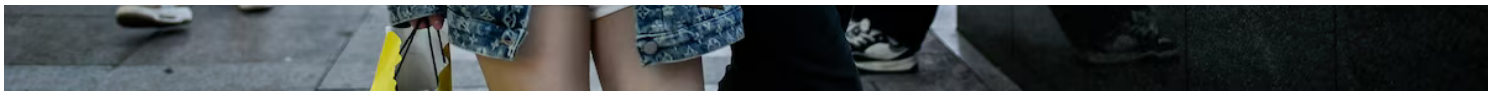
Leaked files show a Chinese company is exporting the Great Firewall's censorship technology

JAMES GRIFFITHS > ASIA CORRESPONDENT
HONG KONG
PUBLISHED SEPTEMBER 8, 2025



The Great Firewall, China's nationwide system of online censorship and surveillance, was developed by Chinese company Geedge Networks. The Globe, along with a group of other researchers and reporters, reviewed a leak of more than 100,000 internal documents linked to the company.

WANG ZHAO/AFP/GETTY IMAGES

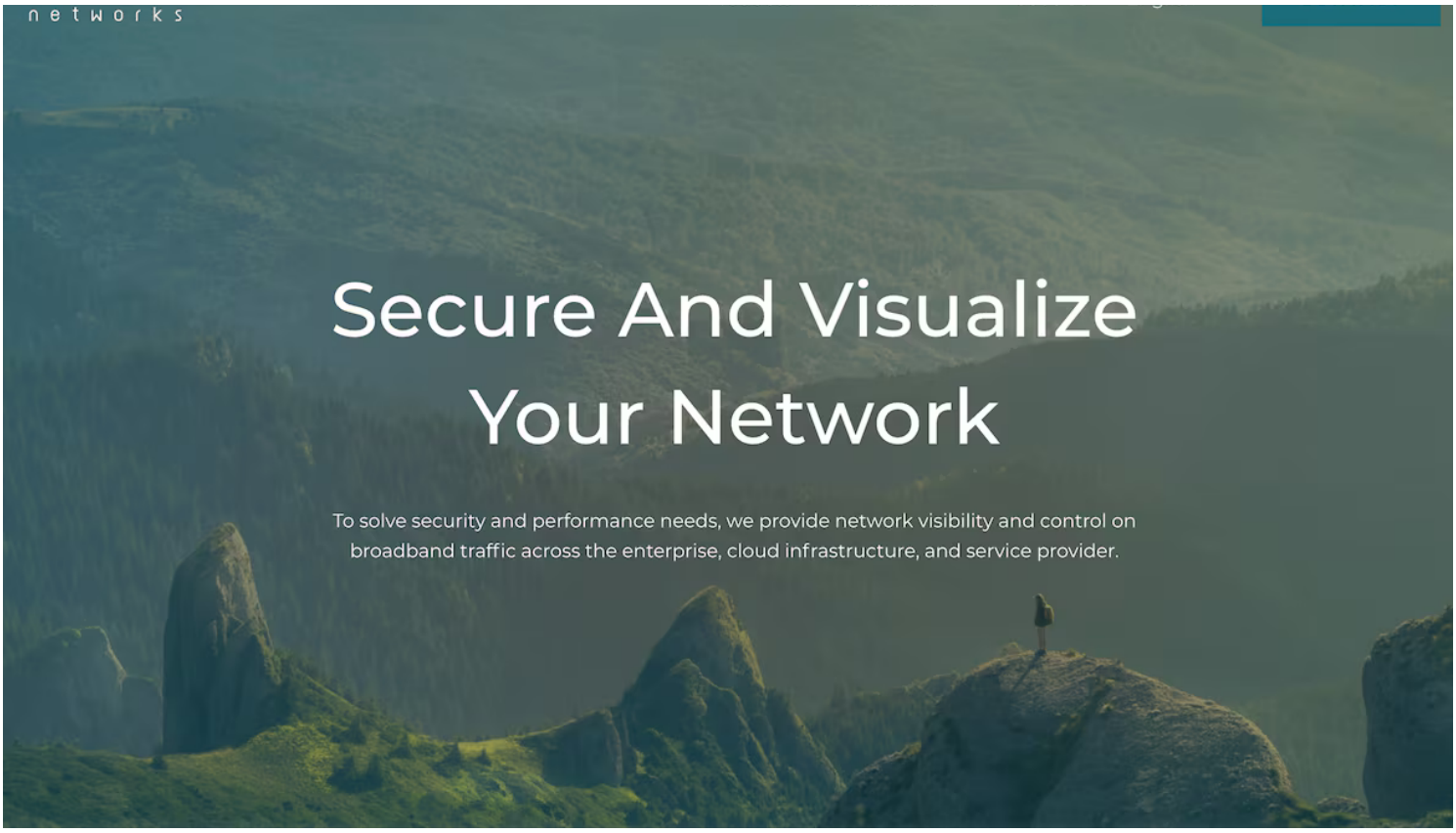
In July, 2024, a group of Chinese technologists and researchers met at an office in Urumqi, capital of the Xinjiang region, to discuss efforts to stop internet users bypassing the Great Firewall, China's vast online censorship and surveillance apparatus.

Even by Chinese standards, internet controls in Xinjiang are intense, a legacy of a years-long crackdown by the authorities targeting Uyghurs and other ethnic minorities. Preventing people from dodging these controls – to access banned websites or download secure messaging apps – was a key government priority, part of a "long-term struggle and technical confrontation" vital to nationwide "anti-terrorism" efforts, according to minutes of the 2024 meeting.

That record, reviewed by The Globe and Mail, is contained in a leak of more than 100,000 internal documents linked to Geedge Networks, a little-known Chinese company that has quietly assumed a key role in developing the Great Firewall and providing similar censorship capabilities to governments around the world, including in Myanmar, Pakistan, Ethiopia and Kazakhstan.

The Globe – along with researchers at InterSecLab, Amnesty International, Justice For Myanmar, the Tor Project and reporters at Paper Trail Media – has spent months combing through the leak. The files offer a key insight not only into how Geedge exports cutting-edge censorship technology to its authoritarian clients, giving them capabilities they might not otherwise have, but also into the evolution of the Great Firewall itself.

This includes solutions for filtering websites and apps, real-time online surveillance, throttling internet data to certain regions or enacting internet blackouts, identifying anonymous users by their online footprint, and blocking tools used to bypass censorship, including virtual private networks (VPNs).



A screenshot of Geedge Networks's website.

SUPPLIED

Geedge's technology suite has been used by client governments to "supercharge their control apparatus" and provide "unprecedented surveillance and censorship capabilities," write researchers at InterSecLab, a digital forensics laboratory that provided key technical support for the team working on the Geedge leaks.

Geedge did not respond to a detailed list of questions about findings in this article or by The Globe's publishing partners. China's Ministry of Foreign Affairs and the Cyberspace Administration of China also did not respond.

On its website, Geedge boasts of its technology being used by more than 40 "global service providers," without naming any country it works with. Even employee induction materials, contained within the leak, are vague, referring only to projects in "East Africa" and "South Asia."

Other documents, however, paint a fuller picture of Geedge's global footprint.

CSIS cautions tech startups about pitching at events organized by China

After its founding in 2018, one of Geedge's first clients was the government of Kazakhstan, to whom the company sold its flagship Tiangou Secure Gateway (TSG), which provides functions similar to China's own Great Firewall, monitoring and filtering all web traffic that passes through it, as well as attempts to bypass such censorship.

The same tool has been rolled out in Ethiopia and Myanmar, where it has been instrumental in enabling that country's military junta to enforce a ban on VPNs. In many cases, Geedge works with other private companies, including internet service providers (ISPs) such as Safaricom in Ethiopia, or Frontiir and Ooredoo in Myanmar, to enact government censorship, the documents show. No ISPs that have partnered with Geedge responded to a request for comment.

The government of Kazakhstan was one of the first to make use of Geedge's flagship technology, the Tiangou Secure Gateway. The governments of Ethiopia and Myanmar have since adopted the same tool.

SAI AUNG MAIN/AFP/GETTY IMAGES

In all three countries, Geedge was providing technology previously unavailable to its clients, expanding their internet censorship capabilities. By contrast, in Pakistan, the Chinese company appears to have stepped into a vacuum created by the exit of one of its Western competitors: Waterloo, Ont.-based Sandvine.

In February, 2024, Sandvine was placed on a U.S. sanctions list for "facilitating human rights abuses" by providing "mass web-monitoring and censorship" to authoritarian regimes around the world. The company – now rebranded as AppLogic Networks – was removed from the list in October after it exited several dozen countries and promised to "focus on servicing democracies."

Sandvine quit Pakistan in 2023 amid growing scrutiny of its work there, and was quickly replaced by Geedge, which the documents show apparently utilizing existing Sandvine installations as well as providing new technology to power Islamabad's Web Monitoring System, as the country's national firewall is called.

In a statement, AppLogic said it was not aware of Geedge and any hardware repurposed by the company was off-the-shelf equipment "that does not contain any special capability that is unique to Sandvine's solution."

As well as the countries named above, the Geedge leaks show the company works with government agencies in at least three regions of China – Xinjiang, Jiangsu and Fujian – as well as with an as-yet-unidentified national client labelled in the data as A24.

Chinese President Xi Jinping appears on a screen on the streets of Kashgar, in Xinjiang region, in 2019. Xinjiang, where internet controls are especially intense, is one of at least three regions where Geedge works with government agencies.

GREG BAKER/GETTY IMAGES

It has ambitions to go further. In a speech last year, Geedge co-founder Fang Binxing – known in China as the "father of the Great Firewall" – said the company was "expanding into international markets, promoting Chinese solutions and technologies globally."

Mr. Fang, who has previously advised other countries – most notably Russia – on their own online controls, referenced the Belt and Road Initiative (BRI), a key priority of Chinese leader Xi Jinping that involves building infrastructure and energy networks connecting Asia with Africa and Europe. A recent job ad posted by Geedge also mentioned the BRI. That ad sought candidates "able to speak English or another foreign language," and willing to go on three- to six-month business trips to "Pakistan, Malaysia, Bahrain, Algeria, and India."

Michael Caster, a researcher at Article 19, a British-based human-rights organization, compared Geedge to other Chinese technology companies involved in the "Digital Silk Road," a BRI project which Article 19 has described as a "platform for advancing China's model of digital authoritarianism."

"It's about normative and narrative change," Mr. Caster said, noting that the concept of "cyber sovereignty," developed in part by Mr. Fang, has "gained traction in autocratic states, and we're unfortunately seeing similar language in democratic countries too."

"States are setting up centralized national gateways that control the flow of data in and out of the country," he said. "This fuels internet fragmentation and strikes at the core principles of a free, open and interoperable internet."

Filtering and blocking online traffic is relatively simple, and companies – including many Western tech firms – have been providing technology to authoritarian regimes to do so for decades. A key capability provided by Geedge's suite of products is the ability to block the means of circumventing such controls, from VPNs to specialized tools such as Tor, software most widely used for accessing the

dark web.

The leaks show employees at the company working to reverse-engineer many popular tools and find means of blocking them. One set of documents lists nine commercial VPNs as "resolved," and provides various means of identifying and filtering traffic to them. Similar capabilities have long been demonstrated by the Great Firewall, with most commercial VPNs inaccessible from within China and many dedicated anti-censorship tools also hard to access.

Keith McManamen, a strategic analyst at Toronto-based Psiphon, which provides a free VPN to users in countries where the internet is censored, said authoritarian regimes have long invested in means of "fingerprinting our traffic."

"We have a history of battling the censors in some of the most dire spaces online," he said.

regimes to filter and block online traffic for decades.

ARIF ALI/AFP/GETTY IMAGES

After the 2021 Myanmar coup, the documents show Geedge developed a tool to detect which servers Psiphon's app connected to, enabling them to be blocked nationwide. Access to Psiphon was highly limited from June, 2024, to March, 2025, according to data from the Open Observatory of Network Interference.

Mr. McManamen said that despite this, during the worst of the internet disruptions in Myanmar, Psiphon actually gained users, as "although our tool was being hit hard, other tools were being hit equally hard if not harder."

Commercial VPNs are often the first circumvention methods to fail, as they do not generally invest in anti-censorship technology. But free tools such as Psiphon or Tor are highly dependent on support from grants and donors, a situation that has been complicated in

recent months by a freeze on much U.S. funding for internet freedom.

The increasing sophistication of censorship tools shows why such funding is desperately needed, Mr. McManamen said.

In the past, ISPs might have bought off-the-shelf censorship software in response to government orders, implemented a simple list of banned websites, and left it like that, he noted. Under the new paradigm enabled by companies like Geedge, however, "now the government is paying someone directly, they'll bring in a team, install it on the ISP infrastructure, and make their own rules."

"The client demands certain things and the vendors are trying to keep them happy," Mr. McManamen said. "These secrets can be shared, software can be updated with new capabilities, features rolled out. The scary part is that if you're a country that's new to the game of information control, you no longer have to earn the expertise yourself."

This can be seen in the Geedge documents, as features developed for one area of operation eventually trickle down to all the company's clients. (Though not always: The documents mention efforts to block Psiphon in Ethiopia, but this does not seem to have happened, despite Geedge's tests in Myanmar.)

Opinion: China held a parade to send a message about its power. Message received

Mr. Fang is described proudly in the Geedge documents as "father of the firewall." Other top company personnel, such as chief executive Wang Yuandi and chief technology officer Zheng Chao, are listed as co-authors of papers on internet censorship and creator of patents applied for by Geedge. The company also has a close relationship with the Massive and Effective Stream Analysis Laboratory (MESA Lab) at the Chinese Academy of Sciences, with the documents showing regular collaboration between personnel at both entities.

It was a MESA Lab researcher who took notes at the July, 2024, meeting in Xinjiang, where attendees spoke of using technology to "strike at the use of tools" to bypass the Great Firewall and establish the "Xinjiang Branch Centre" as an "anti-terrorism vanguard" and "demonstration of provincial capabilities."

Such capabilities, Geedge's history suggests, may soon roll out to the company's clients all over the world.

Geedge has ambitions to extend its reach even further. In a speech last year, co-founder Fang Binxing said the company was 'expanding into international markets, promoting Chinese solutions and technologies globally.'

GREG BAKER/GETTY IMAGES

Report an editorial error Report a technical issue Editorial code of conduct

Related stories

CSIS cautions tech startups about pitching

China says Nvidia violated antitrust law

Bessent says final TikTok deal could be