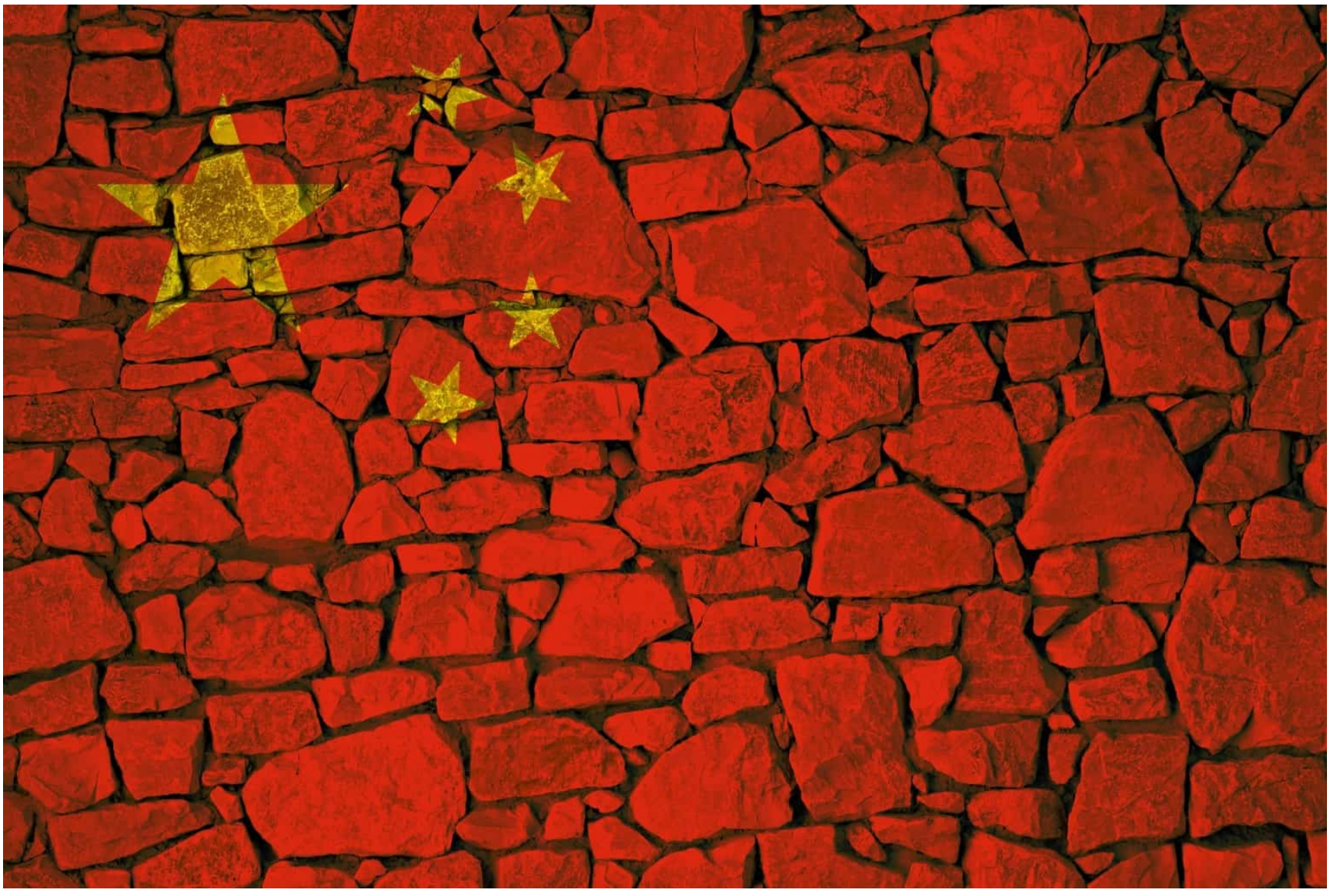
# Security Rift

The newest version of HTTPS's encryption conceals what website internet users are viewing — which is why China's censors blocked it.

By Katrina Northrop — August 30, 2020



*Credit: HealthWyze from Pixabay*

Last year, computer scientist Amir Houmansadr was writing a paper about the new version of TLS, the underlying encryption mechanism for HTTPS, which is used by the majority of websites to protect internet users' data. Houmansadr, an associate professor at University of Massachusetts Amherst, issued a sharp warning: be quick and quiet about the adoption of the newest encryption method or else censors in repressive countries across the world will start blocking it. If the new version was censored in

some countries before it had the chance to become widely popular, he worried, there would be less incentive for websites to adopt it globally.

This July, his prediction became reality when China started doing just that. According to a joint report published by three groups that track Chinese censorship — iYouPort, the University of Maryland, and the Great Firewall Report — the Chinese government has started blocking  HTTPS traffic that uses the most recent version of TLS, short for "Transport Layer Security."

Most websites today use the older version of  HTTPS encryption, which allows users to securely input sensitive data, such as email passwords or online banking information. Readers will likely recognize HTTPS, which stands for "HyperText Transfer Protocol Secure," by the little padlock icon on the far left side of your browser's address bar. But while 96 of the top 100 websites worldwide default to using HTTPS, according to data from the Google Transparency report, HTTPS that uses the new version of TLS, which was introduced in 2018,  is not yet widely adopted.

And the new version takes data privacy one step further, encrypting not only the exchange of personal information, like passwords, but also the destination website, making it impossible to discern what website the user is viewing.

"The goal of the censors," Houmansadr says, "is to push the users to keep using the older, less secure version of the HTTPS protocol, so that they're able to intercept connections and identify the destinations."

For internet users across the world, the new HTTPS encryption version allows greater data security and ensures that no one can eavesdrop on private communications. But for Chinese government censors, the new encryption mechanism makes it harder to identify their population's internet activity, which then prevents them from restricting access to websites that they deem to be politically sensitive, like Facebook, Twitter, and the *New York Times*. So, they blocked the new HTTPS encryption method.

“The Chinese have had a massive surveillance campaign for the internet and telecommunications for decades. When they adopted the internet in 1994, they designed it in a way that would allow them to block traffic and monitor communications,” says James Lewis, a senior vice president and director of the Technology Policy Program at Center for Strategic and International Studies (CSIS). “This is another of a series of measures to ensure that they can control the online environment in China.”

The recent block is deployed through the Great Firewall of China, a massive web of censorship that restricts Chinese access to foreign websites that the government deems politically sensitive. Given this already existing infrastructure, analysts say, blocking encrypted HTTPS traffic that uses TLS is a relatively simple addition.

Though this represents a continuation of decades of online censorship in China, the recent block is a little different. “This is important because what they are targeting is not an anti-censorship activist tool, it is an evolution and improvement of an internet standard,” says Nathan Freitas, the director of Guardian Project, a collective of cybersecurity and privacy experts. “China is proposing a new vision for internet protocol, which is different from the rest of the world’s protocol. More and more we see this divergence in the global internet.”

> *This is important because what they are targeting is not an anti-censorship activist tool, it is an evolution and improvement of an internet standard.*
>
> *Nathan Freitas, the director of Guardian Project*

This block does not necessarily mean that Chinese users cannot access

websites that use HTTPS's most recent encryption method, experts say. In most cases, the browser will automatically downgrade to the older version, which the Great Firewall does not block, and users may not even notice a difference.

But under the surface, this wholesale restriction leaves Chinese users' personal data, like banking or medical information, vulnerable to hacking or cyber attack. "Basically all traffic going through the Great Firewall now is using a lower kind of level of security — not the latest and greatest. That has risks to the average user," says John Conwell, principle data scientist at Domain Tools, a data security firm.

Though this restriction only applies to internet users in China attempting to access websites outside of China using encrypted HTTPS, authors of the recent joint report note that this block will also likely impact websites inside China, both from a technical perspective and from a self-censorship perspective, because domestic Chinese websites may choose not to update to the latest version of TLS.

As with most forms of censorship, there are methods to circumvent the recent restriction, and anti-censorship researchers are working hard to identify them. "This is always an arms race — a cat and mouse game where censors start blocking something, evaders add some new feature that makes it harder for them to block it, and then censors start blocking more," says Kevin Bock, a researcher at University of Maryland and one of the authors on the report.

One method is to use a VPN, or "virtual private network," which has long been a method to evade censorship in China by connecting to a server located in another country. Once users connect to a VPN, they can then access HTTPS with the latest encryption method. Though some popular VPN companies — like NordVPN, according to a spokesperson — can be used to get around the block, other VPN companies actually use TLS as part of their operations to disguise the locations of their users. As a result,

they cannot be used as a circumvention tool for this particular restriction.

Another anti-censorship tool called Geneva can be used to get around the recent block. A research prototype developed by University of Maryland researchers and tested in China, India, Iran and Kazakhstan, Geneva automatically adapts to circumvent censorship using an AI algorithm that finds gaps and bugs in the censor's operations. After it was discovered that China was blocking the latest HTTPS encryption method, for example, it took under two hours for Geneva to find ways to circumvent the block, according to Bock, who is also the lead developer of Geneva.

But these evasion tactics are only for the privileged few, including international business people and foreigners living in China. The vast majority of the Chinese population, for example, do not have a VPN. "It is important to remember that people who circumvent the Firewall are very much in the minority," says James Griffiths, a journalist and author of *The Great Firewall Of China: How To Build And Control An Alternative Version Of The Internet* (2019). "Methods like this [the block of TLS] ensure that for ordinary people, there are enough roadblocks that it isn't worth the bother to try to circumvent it."

Because few Chinese people will be able to evade this new block, the fissure between the Chinese internet and the global internet will only become more pronounced. And the recent move, analysts say, only underscores the Chinese government's commitment to sectioning off the Chinese corner of the internet, regardless of the cost. "People always ask, is this the bifurcation of the internet? The answer is that it was always kind of bifurcated, because the Chinese government doesn't let its people connect," says CSIS's Lewis. "This move continues the bifurcation that was already there."

Katrina Northrop is a journalist based in New York. Her work has been published in *The New York Times, The Atlantic, The Providence Journal,* and *SupChina*. @NorthropKatrina