DIPLOMAT
11 December 2019

Vietnam's Internet Control: Following in China's Footsteps?

Vietnam's new cybersecurity law suggests that the government is attempting to follow China's model of internet control.

By Justin Sherman

On January 1 of this year, a new cybersecurity law entered into effect in Vietnam after its passage in the Vietnamese National Assembly in June 2018. The law (original; unofficial translation) had a number of concerning elements, which included granting the government relatively unchecked authorities to delete or block access to data infringing upon cybersecurity, defined as "national security, social order and safety, or the lawful rights and interests or agencies, organizations and individuals"; granting the government authority to inspect computer systems on the basis of working to improve cybersecurity; and criminalizing propaganda against the Socialist Republic of Vietnam. All in all, it ramps up government powers to monitor information and communications systems within Vietnam and to block and delete online content and data.

Vietnam does not stand alone. As noted in previous reporting by The Diplomat, "in recognition of the challenges that cyberspace could pose for the ruling regime, the Vietnamese government has been among the countries in Southeast Asia taking measures to increase control and regulation of this domain."

Over the last year, more and more countries around the world have begun to exert tighter control over the internet within their borders. These policy changes have been for a variety of reasons, including a desire to better protect the country from foreign cybersecurity threats, a desire to force data to be stored locally in order to bolster domestic innovation, and a desire to spy on and censor the internet with greater ease. Much attention in particular has been paid to the last of these possible motivations, where tighter technical and legal control of internet architecture within a country's borders is a way to better filter online traffic. Indeed, censorship and surveillance has been a direct result of many "sovereign and controlled" internet policies.

In fact, some analysts have compared Vietnam's new law to China's internet governance regime, one that is marked by pervasive internet control, censorship, and surveillance. Freedom House labeled China the "world's worst abuser of internet freedom" for the fourth year in a row. Vietnam isn't quite on the same level as China, but it appears that Vietnam's internet control is following in China's footsteps, despite some contention around other digital and geopolitical issues.

Is Vietnam Mimicking Beijing?

It's become somewhat of a cliché to compare any country's sovereign and controlled internet governance model to that of China. This comparison is accurate and valuable in some contexts, yes; the Chinese government leads the world in tightly controlling its domestic cyberspace. It blacklists IP addresses. It mandates the deletion of politically threatening internet content. It requires certain kinds of data to be stored within Chinese borders. Beijing is also quite active in

international forums to promote this model of internet governance as a globally accepted norm. All of these characteristics could be compared generally to certain other countries, such as Russia or Iran. In addition, China's approach can at least be considered representative of an end state for which many other countries strive.

However, certain things about China make its internet governance system unique. China's internet censorship regime is scaled and incredibly sophisticated. The government has the human power and the technological capability to implement manual content sorting, deep packet inspection, and machine learning applications, for instance (though those technologies are imperfect and always under improvement). The Chinese government also evolves its internet control practices relatively quickly in light of technological changes and censorship work-arounds.

Further, Beijing pumps resources into internet management and control in ways that are simply impossible for other nations. Not to mention that China's large population and global economic influence give it extra weight in promoting and enforcing its internet governance model, as evidenced by recent controversy around Apple and the NBA, and to what extent the Chinese government exerts undesirable influence on foreign-incorporated technology firms. Indeed, China's model of a growing digital economy in tandem with tight state control of information flows is quite attractive to many countries around the world.

But not every tight-control internet governance regime should be compared entirely to China. Moscow, for instance, desires censorship and control to the level achieved in China, but has faced challenges on the technical side. Moreover, the objectives of the current Russian government differ from those of the government in Beijing. As I recently discussed on Public Radio International, China's internet governance regime is fundamentally oriented toward balancing the economic benefits of internet openness with the political and security benefits of internet control; Beijing wants Chinese-incorporated companies to be globally competitive at the same time as it wants to closely manage information flows and their related risks to regime stability. The Kremlin, on the other hand, currently leans much more toward the internet control side of the story. As evidenced by Russia's domestic internet law, there is much less desire among Russian leadership to maintain internet openness, perhaps in part because of a much less prominent technology sector.

All of that said, a few critical details about Vietnam's push for greater internet control suggest that the government is attempting to follow in China's footsteps, even though the two nations may diverge on other geopolitical and technological issues.

A Few Key Considerations

First are the surveillance and censorship elements of the law. Not every country desiring tight control over the internet is only concerned about political speech; Russian lawmakers, for instance, were also pushing the Russian domestic internet law out of concern over cyberattacks from the United States. Vietnam's law rings more in line with Beijing's practices here in that it's quite blatantly about spying on citizens and controlling information flows and is less about minimizing vulnerability to cybersecurity threats like phishing attacks (while that may still be a concern).

Immediately after the law took effect, for example, the Vietnamese government said Facebook was violating the law by allowing "slanderous" content about the government to remain on the

platform. As clearly delineated in the legislation's text, slanderous or disruptive information is now considered in Vietnam to be "an infringement of cybersecurity." This law itself built on previous legislation that already granted the government explicit powers to filter the internet and take down politically undesirable content.

In combination, this is part of the reason why the Committee to Protect Journalists, in October 2019, ranked Vietnam as one of the 10 most censored countries on earth. Its "raft of repressive laws and decrees," they wrote, "sharply [curtail] any media criticism of the one-party government, its policies, and its performance" via digital technologies. Surveillance and censorship are clear motivations for this legislation.

The second reason Vietnam's internet control push is similar to China's is the data localization element of the law. Data localization, broadly speaking, requires specific types of data to be stored in particular geographic locations and/or handled in certain ways (like not transmitted outside those locations, for instance). China has strict data localization laws that use broad definitions of "critical information infrastructure" to define what kinds of data can be regulated under existing provisions. Vietnam's action looks quite similar: it forces companies to "save/maintain system logs" should the government desire to access digital information, and it mandates that certain foreign enterprises collecting data within the country open offices within Vietnamese borders.

Other countries have taken notice of the similarities. Per The Wall Street Journal, the U.S. embassy in Hanoi has suggested this data localization law "might not be consistent with Vietnam's international trade commitments" in the World Trade Organization and elsewhere — imposing unfair restrictions on data needed to perform services. This is a claim also leveled against China's data localization policies. In both cases, data localization is presumably a way, at least in part, to increase government access to others' stored data.

The third reason there may be similarities here is the outsized role of the Ministry of Public Security in cybersecurity regulation in both countries. In China, the MPS is involved in everything from internet regulation to personal information protection; even with the reorganization of Chinese cyberspace authorities, the MPS retains a prominent role in domestic internet governance. In Vietnam, the same can be said — and it was in fact the Vietnamese Ministry of Public Security that drafted and proposed the new cybersecurity law in the first place. This could again underscore the intent of the law as aimed more at online content control than other possible motivations (i.e., shielding citizens from cybersecurity harms).

Finally, it's worth noting that Vietnam has been a notable recipient of Chinese government funding, previously through the "Two Corridors, One Belt" initiative and now through the Belt and Road Initiative (BRI). Beyond just a mechanism for general influence-building, the BRI can also be a way for Beijing to promote its vision of the internet within other countries. This is financial, political, and technological. After all, exports of certain kinds of surveillance technologies to certain kinds of governments can encourage the adoption of authoritarian internet control practices, especially when the recipient government may already lack checks and balances on digital censorship and surveillance. Still, it remains to be seen how much Vietnam is being influenced by the BRI today versus just following in Beijing's net control footsteps — including because these investments may have so far concentrated in sectors like transportation and energy.

Despite this mimicking of China's internet governance approach, it's critical to note that Vietnam is resisting Chinese influence in other dimensions. For instance, Vietnam is beginning to deploy 5G technology absent the equipment of Chinese telecommunications company Huawei, which Washington has been trying to convince allies and partners to ban from their critical infrastructure systems due to purported security concerns. There are economic factors involved here, such as Vietnam's desire (like many other countries) to use domestic technology suppliers in an effort to boost domestic industry, but there may also be geopolitical and security factors at play.

Hanoi has not banned Huawei from 5G systems, but it's possible that as Vietnam tries to better its relationship with the United States, not including Huawei in critical infrastructure is a nod to American concerns about the company. Or, as The New York Times puts it, the Vietnamese government's current strategy toward Beijing, including around 5G technology, could be described as one of "close but not too close." This is true even outside the digital sphere. While "Vietnam remains careful not to provoke China while expanding relations with other powers," Brookings' Jonathan Stromseth writes, "the Vietnam-China relationship nevertheless remains fragile."

All in all, Vietnam appears to be mimicking China's approach to internet governance out of a desire to better control cyberspace and particularly information flows within its own borders. But it's critical to note these points of contention between the two nations and their policy stances on other geopolitical and digital issues.

Looking Forward

It's unlikely that Vietnam will abandon its pursuit of tighter internet control anytime soon. Our research at New America already found Vietnam to quite strongly embrace a "sovereign and controlled" internet model, and that was even before this law took effect. Freedom House's 2019 report, in a further indication of this unrelenting push for cyberspace control, marked Vietnam's internet as extremely restricted. Vietnamese authorities already violate political rights and civil liberties offline.

Hanoi will likely continue to push for greater legal and technical control of the internet architecture within Vietnam's borders, with the aim of better controlling — and filtering — data and information flows, similar to the Chinese internet governance strategy. (This is without even mentioning how Vietnamese state-sponsored hackers are copying elements of China's offensive cyber playbook.)

China's global influence on internet governance remains strong, and it continues to grow through foreign investments, political pressure, diplomatic engagement in international forums, technology trainings and exports, the leveraging of China's economic power, and other mechanisms. While not every country exerting tight internet control should be compared entirely to China — and while Vietnam in particular is resisting Chinese influence in many domains — Vietnam's tightening internet regulation demonstrates just what could happen when a country has the capability and the will to begin to follow in China's internet control footsteps.

Justin Sherman (@jshermcyber) is a Cybersecurity Policy Fellow at New America, a Fellow at the Duke Center on Law & Technology at Duke University's School of Law, and a student at Duke University.