Cyber warfare, influence operations, and TikTok bans

hindustantimes.com/ht-insight/future-tech/cyber-warfare-influence-operations-and-tiktok-bans-101715590168403.html

May 13, 2024

BySriparna Pathak

This article is authored by Sriparna Pathak.

While a concrete and foolproof solution is yet to emerge on preventing conventional conflicts, a peculiar situation has emerged wherein warfare has become grey zone warfare--somewhere between peace and conflict. As the world has moved and adapted to information technology, the domain itself has become a tool for waging warfare against entities ranging from State to non-State actors. Influence operations, cyber warfare, data theft among a long list of others have amalgamated to pose national security concerns to States across the globe. The peculiar part of it is that it is leveraged by state and non-state actors against others, while on the ground, there is no warfare and states are technically ‘at peace’. The usage of technology for malicious purposes has become heated up once again as the United States (US). Senate in April, passed a legislation giving TikTok’s Chinese owner, ByteDance roughly nine months to divest the US assets of the short video app, or to face a countrywide ban. In addition to the U.S. there are at least 13 other countries that have banned TikTok to varying degrees; and examples range from Afghanistan to Nepal to India to Belgium to Canada to Denmark. India was among the first countries to ban TikTok in 2020.

In response to the new legislation in the US, TikTok and its parent ByteDance of China have sued to block the law. The lawsuit was filed against the US government in the court of appeals for the District of Columbia, arguing that the law is unconstitutional and violates free speech protection. Last year, in 2023, TikTok took similar legal actions to stop a ban on the

app in the state of Montana, where a preliminary injunction was guaranteed. In light of the lawsuit filed by TikTok stating that the legislation violates free speech, it becomes pertinent to analyse why the US took the step in the first place.

While freedom of speech in democracies including India and the US is sacrosanct, the state also has to ensure its own security and protection of its own citizens, and its own sovereignty over and above everything else. TikTok, owned by ByteDance is a Chinese internet technology company headquartered in Haidian, Beijing and incorporated in the Cayman Islands. ByteDance was founded by Zhang Yiming in 2012 in Beijing. As per a press release from TikTok in May, roughly 60% of ByteDance is owned by global investors such as Carlyle Group, General Atlantic and Susquehanna International Group, 20% by employees and the rest by Zhang. Nevertheless, Zhang holds over 50% of ByteDance's voting rights. As is the case with most Chinese companies, the Communist Party of China (CPC) set up a party branch at ByteDance in 2014, which was stated by Chinese State media itself. Concerns over ByteDance increased after the CPC government took a 1% stake in its local subsidiary, Beijing ByteDance technology in 2019, which awarded the CPC government a board seat at the subsidiary. ByteDance was targeted by the U.S. government even under the Trump administration that needed ByteDance to sell TikTok's U.S. assets or face being banned in the country. The orders were blocked by federal courts. The concerns over TikTok are in the realm of security and privacy, suggesting that user data might be shared with the CPC government. TikTok is used by about 170 million Americans.

The second concern is that the CPC government will use influence operations through TikTok to create narratives against political parties that do not toe China's political lines and will interfere in US elections. Microsoft earlier this year has already come up with a detailed report on how democracies are at risk from disinformation, including from foreign sources. Chinese handles with direct and indirect links to the CPC government have tried pushing out narratives against social stability in democracies ranging from India to the US to Japan to the Philippines to Malaysia. Another pertinent concern in the US is that downloading TikTok on devices allows for the injection of malicious software by China, putting bank accounts and financial transactions of citizens at risk.

The threat to democracies from these three primary threats, which want to uphold freedom of speech and expression, but must protect their citizens and sovereignty over and above anything else is real. In 2020, when India, banned TikTok, the Government of India had raised similar privacy concerns, as the US does now; stating that the Chinese app posed a threat to the country's sovereignty and security. India is also one of the countries named in Microsoft's report that is at risk of disinformation, including from foreign sources. TikTok was not a one-off case in India. As of date, India has banned more than 500 Chinese apps to date. An example of how Chinese apps can be predatory is from Hindenburg Research's

report stating that China-owned Opera is running four Android apps aimed at India, Kenya, and Nigeria which are in direct violation of Google Play Store policies, forbidding predatory loans and deceptive descriptions. The apps claim to offer rates of 33% or less on loans but the actual rates were much higher, climbing to 438% in some cases. While they offered loan repayment durations ranging between 91-365 days, the real duration was no more than 29 days on average. In the case of denial of payment, the apps would morph images gathered from the user's phones and indulge in blackmail tactics.

In the internet age, safeguarding citizen rights from foreign actors is extremely difficult. Lines between peacetime and conflict blur even more, enabling malicious actors, in the list of which China tops the list to unleash damage on countries' democratic processes as well as their citizens. As was the case in traditional warfare, wherein states were responsible themselves for protecting their citizens and sovereignty, so is the case even in the current epoch of history wherein states, be it India or the US must protect their sovereignty and citizens against the onslaught of malicious actors now using tools of the internet age, such as apps.

This article is authored by Sriparna Pathak, associate professor, Chinese Studies and International Relations, Jindal School of International Affairs, OP Jindal Global University, Sonipat.