Nation States versus globalization: The question of TikTok bans

hindustantimes.com/ht-insight/international-affairs/nation-states-versus-globalization-the-question-of-tiktok-bans-101721114660906.html

July 16, 2024

With the end of World War II, countries and communities across the globe looked for paradigms, norms, legislations, and mechanisms in general to ensure that the horrors of the two World Wars are never witnessed again. International relations as a field of study grappled with questions of what causes wars and devastations. Soon enough the questions of why countries go to war started being replaced in international relations with how to ensure states do not have conflict with each other. Trade, investments, and free flows of capital, ideas, and people were seen as being capable of creating mutual dependencies between states; which could ensure states seek cooperation with each other due to complex interdependence; over conflict. The forces of globalisation became advantageous to the global community at large as large-scale inter-dependencies started being created.

FILE PHOTO: U.S. flag is placed on a TikTok logo in this illustration taken March 20, 2024. REUTERS/Dado Ruvic/Illustration/File Photo(REUTERS)

However, what also emerged was illicit trade, and soon enough illegal started creating further arenas for conflict between States. While trade in itself maybe State or non-State led, fact remains that illicit trade, which may or may not be State-supported creates weaknesses in recipient States and causes further friction between States. The advent of technology-led globalisation added another level of complexity to inter-state dynamics and the increasing possibilities of conflict. An example of how technology flows can create conflict is that of the bans of the Chinese app TikTok across the world.

TikTok, an app launched by the Chinese technology company ByteDance in 2016 allows users to watch, create and share short videos online. It is now available in more than 150 markets, and has offices in Beijing, Los Angeles, Moscow, Mumbai, Seoul, Tokyo and others. However, governments across the world are increasingly barring TikTok from staff devices over privacy and cybersecurity concerns. In some countries, including in India, there are nationwide bans on the app. The United States (US) is the latest in this list of countries, and in March this year, the US House of Representatives approved a bill that would force TikTok to cut ties with its China-based parent company ByteDance, or face a ban in the US. Concerns that the Chinese government could access sensitive user data through the app prompted the US government to pass the legislation banning the app, unless it is sold to a government approved buyer.

India was the first country in the world to ban TikTok, in 2020. India was TikTok's biggest market, as it built an audience of 200 million users. In June 2020, the Indian government banned TikTok, along with an immediate ban on 58 other Chinese apps. This took place as the Chinese People's Liberation Army attacked Indian Army soldiers on the border. In 2020, an investigation found that a company based in Shenzhen, with links to the Chinese government, was monitoring over 10,000 Indian individuals and organisations that were part of a global database of foreign targets. The firm, Zhenhua Data, with links not just to the Chinese government, but also to the military, was monitoring 2.5 million individuals across the world, which included 10,000 Indians as well. Given the gravity of the situation, compounded with China's actions at India's borders, it was but natural that the State had to prioritise national security over technological flows from China.

According to Strike Source, about 20% of the world's global population are being either directly or potentially set up for the Chinese government to collect all of their primary data. There are 4.57 billion Internet users in the world and 31% of them use a virtual proxy network (VPN). Most VPNs used are Chinese-owned, enabling the Chinese government to have access to massive sets of data like private emails, messenger conversations, and personal records. Earlier this year, a data breach from three years ago was reported, wherein a dataset including user details of Bharat Sanchar Nigam Ltd (BSNL), Reliance Jio, and Air India were found on GitHub, a popular developer community platform, and is reportedly the handiwork of the spyware agency I-Soon group, lined to the Chinese government.

In such scenarios, wherein the choice is between national security and globalised technology flows, the State always chooses to secure itself and its citizens, since its primary role is to safeguard its existence and that of its citizens. The Chinese State, on the other hand, has found interesting ways to weaponise technology and to push its own national interests. Given the massive investments China is undertaking in upgrading its technology, States will only become more inward-looking to shield themselves from the fallouts of malicious technology linked to malicious State actors. Unless there are universally accepted

regulations that define the norms around technology usage and data harvesting, States will only become more suspicious of each other and technological flows, reminiscent of a world order based on mutual trust and suspicion, as it existed before and during the two World Wars.

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