On January 19, 2021, the Centre for Social and Economic Progress (CSEP) organised a private, closed-door seminar titled 'China’s Tech influence in Social Media.'

The discussants for the event included Jacob Wallis, Senior Analyst at the Australian Strategic Policy Institute (ASPI), and Sanjana Hattotuwa, Special Advisor, ICT for Peace Foundation (ICT4Peace) and former Senior Researcher at the Centre for Policy Alternatives (CPA), Sri Lanka.

Constantino Xavier, Fellow at CSEP, provided introductory remarks and moderated the session.

The event was part of CSEP's project on China's new influence in South Asia, with contributors from several countries in the region.

The seminar focused on China's information operations and social media influence around the world. Jacob Wallis gave a presentation on his co-authored report titled ‘Retweeting through the Great Firewall' and discussed methodology and key findings. To bring in a regional perspective, Sanjana Hattotuwa, in a recorded video, discussed his work on the methods adopted by the Chinese embassy in Sri Lanka to disseminate information through social media platforms such as Twitter.

Overview of China’s information operations

Wallis’ research uses Twitter datasets to explain how China runs its information operations (both covert and overt). Wallis and his team analysed a dataset of 23,750 Twitter accounts and 348,608 tweets from January 2018 to April 2020. Twitter had deactivated some of these accounts for promoting misinformation. He described how China interweaves disinformation and propaganda into its diplomatic messaging through social media platforms. His research identifies state actors from China that target specific audiences and the prevalence of fake social media accounts that can be purchased or hired through multiple shadow markets online. He explained the aberrant nature and posting patterns of these fake social media accounts, specifically how these accounts tweeted in Mandarin, though their geo-location suggests that they are operated from many other countries, including India and Bangladesh. Governmental involvement may also be inferred from activity time patterns: these accounts routinely deliver messages on social media portals between Monday to Friday, mostly during regular office hours, and are dormant through the weekend.

According to Wallis, when China is faced with national security crises, such as the Hong Kong protests, the Taiwan Issue, or the COVID-19 pandemic, these accounts are re-purposed for information operations and influence campaigns. These accounts are also used to target political opponents or people critical of China. Wallis highlighted the challenges of attributing the fake accounts to Chinese state actors as Twitter does not publically provide the precise methodology used to block accounts.
Is China’s strategy effective?

Some of the participants questioned the effectiveness of the disinformation operations. Wallis, in response, mentioned that the volume of posts published online could be a performance metric for China. The ability to repurpose a large number of social media accounts to publish disinformation on a politically sensitive topic to counter international criticism against China is seen as a success story. Wallis explained how these accounts used the US government’s response to the Black Lives Matter protests to justify China’s own response to protests in Hong Kong. He suggested that Western countries are less likely to get impacted by the online content published on social media by these fake accounts, but mentioned that such content is being increasingly tailored to target specific audiences. In terms of message formats, image-based content or ‘memes’ posted online garner more attention and views from the audience than worded posts.

Can China’s information operations get more sophisticated?

Wallis described how the Chinese social media actors still lacked the sophistication to intelligently operate in an open Internet, despite being able to mobilize a large number of accounts. While delivering messages and disseminating information online, a number of linguistic errors were also noticed. China is at a nascent stage of handling the open internet and this may explain why it has, so far focused mainly on Mandarin-speaking audiences. But the Chinese government had also tried to tap foreign social media influencers who project China in good light. Wallis explained that China has not yet discovered the secret to influence Western social media and audiences but steady progress in using the open internet can be expected in the years to come.

The Case of Sri Lanka

Hattotuwa shared his research insights on the unique nature of Chinese social media accounts operating in Sri Lanka. His work focused on the official Twitter account of the Chinese embassy in Colombo, which was started in April 2020. He mentioned that the posts from the account generally revolve around diplomatic relations between China and Sri Lanka, their history, and refer to the work of both the countries’ foreign ministries, political figures, and journalists. In just the first month of operation, this account published six hundred tweets, compared to the United States embassy’s average 68 monthly tweets in the last eleven years.

Hattotuwa explained how unlike other diplomatic accounts in Sri Lanka, the Chinese embassy aggressively engaged other Twitter users with hostile undertones, including by tagging elected Sri Lankan leaders and other diplomatic representations. On the contrary, a parallel Sri Lankan account linked to China’s Belt and Road Initiative (BRI) is paradoxically more diplomatic and focuses on the positive economic aspects of both the countries. Hattotuwa also highlighted the issue of semi-automated and fully automated accounts, commonly called ‘sock puppet accounts’ whose primary role is to amplify the messages put out by the Chinese embassy’s account or the BRI account.