China Information Operations Newsletter 3 August 2021

3 August 2021

The China Information Operations Newsletter is edited by Hannah Bailey and Hannah Kirk, researchers at the Programme on Democracy and Technology (DemTech) at Oxford University. This newsletter is a seven minute read.

Hacking for the Party?

The US attributed a recent hack of Microsoft email servers to China's Ministry of State Security. A report by *The BBC* notes that various countries including the US, as well as the EU and NATO, have condemned the Chinese state for collaborating with criminal hackers. These collaborative cyberattacks are more "thuggish" than Beijing's previous hacks, and focus on personal gain rather than intelligence gathering.

The Chinese government has also introduced new rules that require anyone in China who discovers a previously unknown cyber security weakness, or "zero-day", to inform the government. Previously, as *The Associated Press* reports, anyone who discovered a security vulnerability could sell the information to the police or private companies. But the Cyberspace Administration of China is now keen to wield greater control over its domestic cyber security infrastructures. Zero-day vulnerabilities have previously been used in Russian-linked hacks of private companies.

A recent government crackdown on digital currency transactions within China has forced most crypto miners offline. *The Economist* notes that several different considerations could have led to this decision, from concerns over the emissions and electricity usage involved in cryptocurrency mining, to a desire to reduce investment scams.

Crackdown on Grassroots Movements

In the aftermath of deadly flooding in the Henan province, *Protocol* details how Chinese social media users took to Weibo and Tencent to provide grassroots support for those who needed assistance. However, *The Economist* reports that official state media were keen to downplay the connection between the floods and climate change. Chinese leaders do not want grassroots mobilisation to drive climate policies.

Meanwhile, on July 6th the WeChat accounts run by many campus LGBTQ+ groups were banned from the platform. *The Guardian* reports that while China decriminalised homosexuality in 1997, the LGBTQ+ community continue to face discrimination from a growing nationalist movement. While it is unclear whether criticism by nationalists led to the removal of these accounts, it is a part of a broader trend of crackdown on online activism within China.

In an article published in *The China Quarterly*, authors Lotus Ruan et al. unpack China's intricate censorship system. While many believe China's censorship infrastructure is one of top-down monolithic state control, this is not always the case. Government censorship directives are passed down to media companies. However, these media companies can be heavy-handed in their implementation of these directives, sometimes over-blocking or unintendedly failing to comply with directives. It is important to note that any censorship action taken on social media is the result of the agendas and priorities of both government and private companies.

In Hong Kong, a pro-democracy protestor has been sentenced to nine years in prison for terrorism and inciting succession in the first sentencing under the Hong Kong national security law. *The Associated Press* reports that a 24 year old man was sentenced for driving into police officers at a rally in 2020 while carrying a flag reading "Liberate Hong Kong, revolution of our times".

In his book titled "The Party and the People: Chinese Politics in the 21st Century", Professor Bruce Dickson explores how the Party uses repression and responsiveness to maintain control. The author notes that the Party cannot solely rely on either repression or responsiveness, and that a combination of both is needed to govern. However, under President Xi Jinping, the Party is increasingly relying on repression to maintain legitimacy.

Expanding Regulatory Power

Chinese authorities are set to heighten regulatory scrutiny of Chinese companies listed in

overseas markets, following a high-profile investigation into tech company Didi Global. *Nikkei Asia* reports that an increase in government regulatory influence over Chinese companies could discourage these companies from expanding into international markets. Beijing seeks greater control over international data flows and data security.

Following its initially successful entry to the Chinese market, Tesla has faced unusually intense regulatory scrutiny and a wave of negative press coverage. The Chinese government ordered a recall most of Tesla's vehicles in China to resolve software concerns. Meanwhile, *Bloomberg* reports that government facilities have banned Tesla vehicles, citing concerns that the data from these vehicles could be sent to the US. Meanwhile, domestic car makers are filling the gap in the market.

China's expanding regulatory power is not limited to the car industry, in recent weeks Beijing has issued policy guidelines that aim to rein in private tutoring companies. *Protocol* notes that the central Commission for Discipline Inspection publicly criticised the online tutoring market and called for greater regulatory oversight to "prevent a messy capital bloodbath".

Learning to Localise Soft Power Narratives

In recent years, foreign vloggers have been using their platforms to defend China's government against "the West's alleged "lies"", the *BBC* reports. These vloggers also appear in videos on the Chinese state broadcaster CGTN. This is part of a wider movement by Chinese media organisations to localise their soft power messaging, in an attempt to appeal to international audiences.

In a recent book titled "Shaping the Future of Power: Knowledge Production and Network-Building in China–Africa Relations", Professor Lina Benabdallah unpacks China's emerging "soft power" in Africa. Notably, China aims to position itself as a peer developing country. From this position it can to make network building less confrontational, and effectively project its public diplomacy. By localising itself and adapting its soft power strategy to the target country, China can more effectively wield its influence.

Sign up for the DemTech Newsletters on COVID-19 Misinformation and China Information Operations

SIGN UP TO OUR NEWSLETTERS

RELATED CONTENT

War in Ukraine and Disinformation Newsletter 16 August

READ NOW

Post, 16 August 2022