亞洲策 | Asia Insights

The India-Taiwan Imperative for Cybersecurity Cooperation[1]

Sameer Patil

Fellow, International Security Studies Programme
Gateway House: Indian Council on Global Relations
Mumbai, India

Globally, cyber-attacks are the new normal in geopolitical ambitions and rivalries. Exploiting their adversaries' dependence on information, communication and digital technologies, states have breached computer networks, stolen sensitive data and proprietary information and disrupted critical infrastructure operations. In many cases, states have used non-state actors as proxies to carry out cyber-attacks. This has blurred the distinction between state and non-state actors, thereby making cyber warfare the most significant new threat to international security. Adversarial states and cyber saboteurs have also capitalized on the opportunity offered by the COVID-19 pandemic to expand their destabilizing activities in cyberspace.

For years, India and Taiwan have been at the receiving end of China's offensive cyber operations. They face similar threats and cannot tackle them on their own, given these threats' transnational character. This makes it essential for New Delhi and Taipei to initiate bilateral cybersecurity cooperation, even if informally.

China's offensive cyber operations have been an extension of its territorial disputes with India and Taiwan. In the last few years, Beijing has adopted an increasingly confrontationist attitude in asserting its territorial claims – as most evident by the June 2020 violent clash between Indian and Chinese armies during the border standoff in eastern Ladakh and China's egregious and repeated violations of Taiwan's Air Defense Identification Zone.

During the Ladakh standoff, India faced an escalated offensive cyber campaign from China-based hackers. Recorded Future, a US-based cybersecurity firm, noted that since

[1] This article is based on the remarks delivered at the webinar on "India-Taiwan Collaboration in the Post-COVID-19 Era: Opportunities and Challenges" hosted by the Center for South and Southeast Asia Studies, FLAME University on March 15, 2021.

mid-2020, a China-linked hacker group called RedEcho had targeted India's power sector, ports and parts of the railway infrastructure.[2] Another report from a Singapore-based company, CyFirma, highlighted that a Chinese-state backed hacking group had targeted computer networks of two Indian vaccine makers – Bharat Biotech and the Serum Institute – whose vaccines are part of not just domestic vaccination program but also India's vaccine diplomacy.[3]

India has witnessed the remarkable persistence of China's offensive cyber operations. One of the most significant and sophisticated operations was the APT30 operation, carried out by a China-based group, which was most likely state-sponsored.[4] This decade-long espionage operation harvested information from Indian computer networks on geopolitical issues relevant to the Chinese Communist Party, including the India-China border dispute and Indian naval activity in the South China Sea. A related challenge is what all democracies face from authoritarian regimes – the disinformation campaigns. India saw instances of this during the Doklam crisis of 2017 and the latest Ladakh standoff.

Despite facing these sustained attacks, India has not publicly attributed them to China. However, in the face of the mounting frequency and intensity of these attacks, India may have to revisit its position.

Taiwan faces similarly persistent and penetrating cyber-attacks from China. For instance, in 2020, as compared to 2018, cyber-attacks – likely from Chinese sources – against the Ministry of Foreign Affairs increased 40-fold.[5] As per media reports, the frequency of attacks was staggering – 2100 per day, demonstrating the hackers' determination to breach the ministry's cyber defenses at any cost. Likewise, in August 2020, authorities had stated that the Chinese government-linked hacking groups had attacked since 2018 at least ten government agencies and some 6000 email accounts of government officials to steal classified information. Targets included at least four tech companies that had been providing information services to the government.[6]

Such confrontation in cyberspace is a critical element of China's hybrid warfare and intimidation campaign against Taiwan. As an American scholar, Ryan Hass from Brooking Institution recently noted, Beijing has used many tools to pursue this strategy, including "squeezing Taiwan's economy to suffocating its connections to the outside

---

[2] Insikt Group, "China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions", *Recorded Future*, February 28, 2021 at https://www.recordedfuture.com/redecho-targeting-indian-power-sector/

[3] "Chinese Hackers Target India's Serum Institute, Bharat Biotech: Report", *NDTV*, March 1, 2021 at https://www.ndtv.com/india-news/chinese-hackers-target-india-s-serum-institute-bharat-biotech-report-2381309

[4] "Threat Research: APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation," *Fireeye*, June 15, 2020 at https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

[5] Matthew Strong, "Cyberattacks on Taiwan's Ministry of Foreign Affairs increased 40-fold in 2020", *Taiwan News*, March 3, 2021 at https://www.taiwannews.com.tw/en/news/4164261

[6] Yimou Lee, "Taiwan says China behind cyberattacks on government agencies, emails", *Reuters*, August 19, 2020 at https://www.reuters.com/article/us-taiwan-cyber-china-idUSKCN25F0JK

world."[7] And as he added, "Above all, Beijing seeks to persuade the people of Taiwan that they are isolated and vulnerable, and that their future security and prosperity can only be assured by Beijing."

Faced with such rampant cyber threats, Taiwan has created an extensive network of institutions, including the Information, Communications, and Electronic Force Command under the Ministry of National Defense and Cybercrime Investigation Unit under the Ministry of Justice Investigation Bureau.[8] Similarly, India has established dedicated agencies to deal with growing cybersecurity challenges. It operates under the Ministry of Home Affairs, the Indian Cyber Crime Coordination Centre, the lead agency for tackling cybercrimes in India.[9] Most recently, New Delhi activated the Defence Cyber Agency, a tri-service command of the Indian military to handle cyber threats.[10]

There are opportunities for the two sides to build on these shared threats and common synergies. Taiwan has established itself as a hub of technological innovation, and India has become an IT and software hub. Cybersecurity presents an excellent avenue for hardware and software cooperation between the two countries.

One critical area for bilateral cooperation is to create a "framework for attribution". This will comprise technical analysis of threat vectors, the role of non-state actors and applicable legal frameworks. Evolving such a framework will help to delineate China's reliance on proxies for its offensive cyber operations. Another area for cooperation is encouraging informal collaboration between respective law enforcement and technical agencies like National Computer Emergency Response Teams (CERT) bilaterally and regionally at the Asia-Pacific CERT level.

The third area of potential collaboration is critical infrastructure protection and share best practices on how government and businesses in both countries are working to mitigate this threat. Fourth is cyber hygiene and cybersecurity awareness to increase the resilience of both the populations against cyber threats, cybercrimes and propaganda and disinformation campaigns. Finally, under their respective policy frameworks of Act East and New Southbound, both countries can explore potential opportunities to work together for cyber capacity building programs in the Indo-Pacific region countries.

Undeniably, there are certain political realities that this cooperation will encounter, like Taiwan's lack of membership from most global multilateral institutions and platforms, including Interpol. Moreover, any potential bilateral collaboration risks further escalating

---

[7] Ryan Hass, "A broad view provides the best insight on Taiwan's strengths and vulnerabilities", *Brookings*, March 22, 2021 at https://www.brookings.edu/blog/order-from-chaos/2021/03/22/a-broad-view-provides-the-best-insight-on-taiwans-strengths-and-vulnerabilities/

[8] Huang Ming-chao, "Taiwan Is Crucial to the Global Fight Against Cybercrime" *The Diplomat*, December 3, 2020 at https://thediplomat.com/2020/12/taiwan-is-crucial-to-the-global-fight-against-cybercrime/

[9] "Details about Indian Cybercrime Coordination Centre (I4C) Scheme", *Ministry of Home Affairs* at https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

[10] "Raksha Mantri Reviews Defence Cooperation Mechanism", *Press Information Bureau*, June 6, 2019 at https://pib.gov.in/Pressreleaseshare.aspx?PRID=1573610

offensive cyber operations by the Chinese Communist Party against India and Taiwan. It is precisely this hostile Chinese attitude that such partnership seeks to counter. While hostility and dispute with China may define the urgency of this cooperation, it should not define its endurance.

Asia Insights is an online magazine and newsletter dedicated to the analysis of international relations and regional dynamics in Asia. It is published jointly by the Institute of International Relations and the Center for Southeast Asian Studies at National Chengchi University in Taiwan and the Center for South and Southeast Asian Studies at FLAME University, India.

Institute of International Relations @ National Chengchi University
No.64, Wanshou Rd., Wenshan District
Taipei City, 116, Republic of China (Taiwan)
http://iir.nccu.edu.tw

Center for Southeast Asian Studies @ National Chengchi University
No.64, Wanshou Rd., Wenshan District
Taipei City, 116, Republic of China (Taiwan)
http://iir.nccu.edu.tw

Center for South and Southeast Asia Studies @ FLAME University
Gat No. 1270, Lavale, Off. Pune Bangalore Highway,
Vadzai, Dist. Pune - 412115, India
http:// www.flame.edu.in/research/centres/centre-for-south-and-southeast-asia-studies