ISSUE 230 11 AUG 2023 - 25 AUG 2023

China-India Brief

A publication of the Centre on Asia and Globalisation

Image Credit: iStock/Wanan Yossingkum

Guest Column

From the Border to Cyberspace: Investigating the Post-Galwan Escalation of Chinese Cyber Attacks against India

By Neeraj Singh Manhas

The India-China relationship has become increasingly complex and challenging, with bilateral tensions rising to their highest point in decades following the **Galwan Valley clash** in June 2020. The skirmish at Galwan sent shockwaves through both countries as it marked the first time since **1975** that soldiers were killed in combat along the border. The subsequent (and still ongoing) standoff only further contributed to the deterioration in bilateral ties. Today, though tensions have calmed somewhat, with both sides agreeing to mutual withdrawals along

Lee Kuan Yew School of Public Policy

Centre on Asia and Globalisation

The *China-India Brief* is a bi-monthly digest focusing on the relationship between Asia's two biggest powers. The Brief provides readers with a key summary of current news articles, reports, analyses, commentaries, and journal articles published in English on the China-India relationship. It features a Guest Column weighing in on key current issues in China-India relations.

Centre on Asia and Globalisation
cag@nus.edu.sg
469A Bukit Timah Road, Tower Block 10,
Singapore 259770
https://lkyspp.nus.edu.sg/cag

cont'd p2

parts of the border and engaging in ongoing talks to end the standoff, an undercurrent of hostility has remained.

Indeed, one significant development following the Galwan Valley clash has been a **surge** in alleged Chinese cyber attacks against India. These attacks have targeted a wide range of Indian government and corporate networks, and has caused significant damage. Though Beijing has **denied** any involvement in these attacks, cyber security companies like **Recorded Future** and **CyFirma** have reported cyber espionage activity by Chinese state-linked hacker groups targeting Indian assets and infrastructure.

If China is indeed behind these attacks, what could its motivations be? There are various possibilities. First, the attacks could be **retaliation** for the Galwan Valley clash—a way for China to punish India by inflicting economic and technological costs. Second, they could be aimed at **gathering intelligence** on Indian military and government operations. Such information could give China an edge either in a future military conflict or in diplomatic negotiations. Lastly, the attacks could be part of a larger strategy to undermine India's long-term development and stability. India is rapidly advancing in the **digital realm**, with more and more public and commercial services moving online. As such, India's economy is highly susceptible to disruption from cyber attacks. Indeed, attacks on critical infrastructure, government institutions, and corporations have the potential to cause **widespread disruption and economic damage**. A study by the Ponemon Institute estimated that the average cost of a data breach in 2022 to be **USD 4.35 million**.

Chinese Hacking Attempts

India witnessed a significant surge in cyber attacks almost immediately following the skirmish at Galwan. Over the course of just five days in late June 2020, Indian IT networks and banking infrastructure suffered more than **40,300 attempted** cyber attacks, most of which, were found to have originated from Chengdu in China, according to Indian police officials. Since then, several more significant attacks on India's critical infrastructure have been detected:

1. **Hacking of Bharat Biotech and Serum Institute of India**: In March 2021, it was reported that the hacker group **APT 10** (also known as Stone Panda), which has close links to the Chinese government, were planning to target the IT systems of Bharat Biotech and the Serum Institute of India, likely in an attempt to steal intellectual property and gain a competitive advantage in the development of COVID-19 vaccines.

2. **Targeting Indian power sector**: Beginning from mid-2020, another China-linked activity group, **RedEcho**, was detected conducting suspected network intrusions against Regional Load Despatch Centres (RLDCs) and State Load Despatch Centres (SLDCs) in India's power sector.

Image Credit: iStock/Marco VDM

RLDCs and SLDCs are responsible for maintaining a stable grid frequency and ensuring the proper functioning of the power grid.

3. **Phishing campaign and Mumbai power outage**: In February 2021, Indian government officials, including ministries, were targeted in a **phishing campaign** involving compromised government domain email addresses. Though the culprits were not ascertained, the incident bore marked resemblance to an earlier phishing campaign suspected to have been carried out by Chinese state-sponsored entities. In a separate incident, a **power outage in Mumbai** in October 2020 was suspected to be caused by malware planted by a Chinese state-linked group. Though again, this has not been substantiated.

4. **Chinese attacks and phishing emails**: In June 2022, security experts from the Cyber Peace Foundation **reported** a wave of attacks targeting Indian individuals through phishing emails. The attacks were tied to domains registered in China's Guangdong and Henan provinces, attributed to an organisation named Fang Xiao Qing. The intention of these attacks appeared to be obtaining access to Indian devices for potential future attacks.

These incidents collectively **raised concerns** about the presence of Chinese malware within India's critical information infrastructure and the potential vulnerabilities in its cyber defences. In April 2021, India's most senior armed forces official, Chief of Defence Staff (CDS) Bipin Rawat, **noted** that China was capable of launching cyber attacks that could "disrupt a large amount of [India's] systems." He also warned that India's best defence against these attacks was to keep outage time limited when a breach did occur. These

warnings came at a time when tensions between India and China were already high following the Galwan clash. The increased cyber attacks from China were a further reminder of the threat that the country posed to India's security.

Response of the Indian Government

Over the last decade, the Indian government has adopted a number of measures to strengthen its cyber security architecture. The most notable was the 2013 establishment of the **National Cyber Security Coordinator (NCSC)** position under the **National Security Council Secretariat**. The NSCS plays a crucial role in coordinating with other central-level agencies on matters related to national cyber security. One of its key responsibilities is to monitor communication metadata, providing valuable inputs to law enforcement agencies for investigating potential cybercrime cases. Presently, the NCSC is actively involved in updating and replacing the 2013 National Cyber Security Strategy.

The forthcoming **National Cyber Security Reference Framework (NCRF)** will replace the outdated strategy and adopt a common but differentiated approach. While the overall cyber security goals will remain consistent for all stakeholders, the framework will tailor specific objectives for government organisations, private institutions, academia, and other relevant entities. There has also been other measures such as the creation of **Cyber Swachhta Kendra** (Botnet Cleaning and Malware Analysis Centre) which is a new desktop and mobile security solution for cyber security in India. It was launched by the Indian government's **Computer Emergency Response Team (CERT-in)** in 2017 to combat cyber security violations and prevent their increase. CERT-in also functions as the nodal agency for the coordination of all cyber security efforts, emergency responses, and crisis management. It is responsible for monitoring and responding to cyber threats, providing technical assistance to organisations, and disseminating information about cyber security best practices.

Way Forward

The threat of increasing cyber attacks poses a significant challenge to India's national security. India needs to step up its efforts to safeguard itself from attacks of this nature. The attacks demonstrated meticulous planning, precise targeting, and use of sophisticated techniques, and based on third party reports, were likely orchestrated with the support of the Chinese government. Moreover, the timing of these attacks indicates a deliberate intent to disrupt and destabilise India, particularly following the clash at Galwan.

When it comes to **defending** the country against cyber attacks, the Indian government, corporations, and ordinary

citizens all have important roles to play. The government must proceed with the implementation of measures to further bolster the country's cyber defences. In addition, people and businesses in India need to be vigilant of the danger posed by cyber attacks and incorporate cyber security best practices into their daily activities. This includes the use of robust passwords, caution when deciding what information to give online, and awareness of the most recent risks to online security. It is imperative for government agencies to also strengthen post-breach strategies, including the potential to counterattack the hackers, and to partner with other countries in the development of cyber defences.

Neeraj Singh Manhas is the Director of Research at the Indo-Pacific Consortium at Raisina House, New Delhi. He has authored and edited four books and has various research interests covering Sino-Indian border issues, China in the Indian Ocean, India-China foreign policy, water security, defence, and Indo-Pacific studies. His most recent edited book, *Analysing the Current Afghan Context* **was published in 2023 by Routledge. He has published his writings for renowned institutions such as the** *Institute for Security & Development Policy (ISDP), Observer Research Foundation (ORF), Centre for the Joint Warfare Studies (CENJOWS), Jamestown Foundation, The Hindu BusinessLine, The Pioneer, Financial Express, Firstpost, The Millennium Post*, **and other online platforms. He tweets at @The_China_Chap.**