China-India Conflicts in Cyberspace

Chen-Yi Tu
Assistant Research Fellow

Division of Cyber Security and Decision-Making Simulation

1. News Highlights

While it's been more than a year after the June 2020 clashes between China and India in the Galwan Valley, the gradual shift from armed conflicts at the border to disengagement has received much attention. However, little discussion has been focused on the sustained cyber campaign from CCP-related hacker groups. According to the research report released on Sept. 21 by Recorded Future, a US cybersecurity firm, the CCP-affiliated hacker group TAG-28 has attacked Bennett Coleman & Co Ltd., known as "The Times Group of India", the Unique Identification Authority of India (UIDAI) and the Madhya Pradesh Police Department in February.[1] This series of attacks is likely a follow-up action to the October 2020 attack on India's energy sector by RedEcho, another CCP-affiliated group. These series of incidents show sustained CCP cyber operations even as armed conflicts gradually "disengage" with troop withdrawal; the acquisition of valuable personal identifiable data through cyber espionage also implies a prolonged China-India conflict in cyberspace.

2. Security Implications

2-1. Cyber-attacks unceasing

As the timeline of events have shown, the cyber intrusion efforts from CCP-affiliated groups against the Indian government and other organizations

[1] Dina Temple-Raston, "Report: China-linked Hackers Take Aim at Times of India and a Biometric Bonanza," *The Records*, September 21, 2021, https://therecord.media/report-china-linked-hackers-take-aim-at-times-of-india-and-a-biometric-bonanza/.

did not abate even though the two sides were negotiating and initiating actual troop withdrawal. The first attempt to "disengage" was in May 2020. On July 5, 2020, after three rounds of high-level military and diplomatic negotiation between China and India, both reached a consensus to de-escalate with both forces "disengaging" in areas such as the Galwan Valley. However, the analysis by Recorded Future indicates that the CCP-affiliated group RedEcho was still registering domains on July 11, which indicated attempts for further cyber action.[2] The actual attack on India's regional power grid centers occurred around October. According to a follow-up investigation by Indian local government authorities, at least the outage in Mumbai on the morning of October 13 may have been related to the RedEcho.[3]

On February 10, 2021, China's Ministry of National Defense announced that it would follow the consensus of the ninth round of bilateral negotiation and would go further to immediately "disengage" with the Indian side on the southern and northern shores of Pangong Lake. At the same time, however, TAG-28 also launched intrusions against Bennett Coleman, UIDAI and the Madhya Pradesh Police Department. All these incidents prove once again that cyber attacks are not only a precursor to conflict but also a crucial component across the full spectrum of conflict.

2-2. CCP attacks on India extended to media and personal IDs

Although this is not the first incidence that a CCP-affiliated group targets media, the fact that the Times of India has been critical of CCP's actions and they have covered CCP-affiliated groups targeting the Uyghur, clearly shows that the CCP is very concerned about media coverage and its international image. Therefore, TAG-28 was trying to obtain reports, the contact information of relevant journalists

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

[3] "Mega Mumbai Power Outage May be Result of Cyber Attack, Final Report Awaited," *India Today*, November 20, 2020, https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20.

and even their information sources. Although the Recorded Future report doesn't provide any clue on exactly what information was obtained by TAG-28, it's known that about 500 MB of data has been transmitted to hacker-controlled infrastructure outside the corporate network. The attacks against media may have become a standard procedure in CCP-affiliated cyber operations.[4]

However, the intrusion of UIDAI may serve purposes well beyond gaining intelligence. UIDAI is the managing authority of Aadhaar, which is India's digital identification system. UIDAI issues every Indian citizen a 12-digit identifier along with a Aadhaar card after recording their fingerprints, iris scans and mugshots. Aadhaar covers 89% of India's population, so this Personal Identification Information (PII) is extremely valuable and will help hackers identify high-value targets such as government heads. The PII can also be used for social engineering such as fraud and threats; and it can be used to generate new insights when combined with other intelligence.[5] In particular, all Indian government services currently require biometric information such as fingerprints and iris scans, and the data can be accessed from Aadhaar's single database. Unlocking the database will grant hackers access to confidential data from other government agencies to further extend their reach.

3. Trend Observation

3-1. China-India conflict in cyberspace is for long term

According to Recorded Future, the intrusions from CCP-affiliated groups to Indian organizations and companies rose steadily from 2019 to 2021. Particularly, there is an increase of 120% from 2019 to 2020, and 2021 saw an even greater surge of 261% from 2020.[6] This indicates that the conflict between China

[4] Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tension," *Recorded Future*, September 21, 2021, https://go.recordedfuture.com/hubfs/reports/cta-2021-0921.pdf.

[5] "Aadhaar Covers Over 89% Population," *India Today*, March 7, 2018, http://timesofindia.indiatimes.com/articleshow/63202223.cms.

[6] See Note 4.

and India in cyberspace is a long term one. Furthermore, the biometric data may be used not only to conduct more sophisticated attacks, but also to train its artificial intelligence algorithms for better image recognition capabilities to strengthen its surveillance on India.

In addition to evidence discovered from analyzing hacker behavior through network traffic and monitoring data, there are specific instances of continued CCP infiltration into India. In June 2021, the Indian Border Security Force arrested Han Junwei, a Chinese national, in West Bengal for illegal entry and recovered nearly 1,300 cell phone SIM cards from his possession. Han testified that several CCP units have "targeted a company in Bangalore that is associated with the Indian Defense Ministry and telecommunications companies, as well as several aerospace companies," and have "repeatedly tried to hack the official Indian Defense Ministry website in order to spy on the Indian defense system." Although the Indian Special Task Force was unable to confirm the relationship between Han and any CCP agency, the SIM cards were allegedly used to hack accounts or commit fraud.[7] *The Global Times*, an official CCP media, reported on the incident, emphasizing only Han's role as a businessman and his affection for India, but completely avoiding the details of the arrest and the smuggling of SIM cards.[8] This low-profile approach, which avoids drawing attention to the incident, may indicate that the CCP has tacitly acknowledged its intelligence activities in India.

3-2. India's cyber security units need restructuring and integration urgently

In response to the deteriorating cybersecurity situation and growing threats, the Indian military established

[7] "Arrested Intruder Says China Trying to Hack Defence Ministry Websites: Official," *Hindustan Times*, June 23, 2021, https://www.hindustantimes.com/india-news/arrested-intruder-says-china-trying-to-hack-defence-ministry-websites-official-101624405729228.html.

[8] "A Chinese Businessman Who Considered Indian Healthcare Better Suspected as a Spy, Arrested by the Indian Army," *Global Times*, June 12, 2021.
https://www.hindustantimes.com/india-news/arrested-intruder-says-china-trying-to-hack-defence-ministry-websites-official-101624405729228.html.

the Defense Cyber Agency (DCA), a dedicated cybersecurity task force, on September 28, 2018. DCA is a tri-services command of the Indian Armed Forces, with its head of two-star rank and who reports to the Chief of Defence Staff through the Integrated Defense Staff. The original plan for the DCA aimed at obtaining Full Operational Capability (FOC) by August 2021. Indian Defense Minister Ajay Bhatt also confirmed this at a press conference in August and mentioned that the Indian Army, Navy and Air Force had each established their Cyber Emergency Response Teams. However, Gen. Bipin Rawat, India's Chief of Staff, said earlier on April 7 that China already has the capability to attack most Indian systems over the network, and that the best India can do to protect itself is to minimize the downtime when hacked — somewhat in contradiction to Ajay Bhatt's claim. In the face of the increasing number of cyber incidents and the prolonged conflict between China and India, it's clear that capacity building and integration of India's cyber security capabilities have become an pressing issue that the Indian military must address.[9]

(The original article was published in the INDSR National Defense Security Bi-weekly Report on October 15, 2021)

[9] " 'GOI in Final Stage of Formulating National Cyber Security Strategy' ," *The Statesman*, October 12, 2021, https://www.thestatesman.com/india/goi-national-cyber-security-strategy-1502990178.html; "The Chinese Cyber Threat is Real — and India's Best Defence Right Now is to Keep its Outage Time Limited," *Business Insider India*, April 9, 2021, https://www.businessinsider.in/defense/news/the-chinese-cyber-threat-is-real-and-indias-best-defence-right-now-is-to-keep-its-outage-time-limited/articleshow/81981886.cms.