MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Chinese Targeted Cyber Operations against Taiwan: Key Takeaways for India

Krutika Patil

September 28, 2022

Summary

Nancy Pelosi's visit to Taiwan in August 2022 led to a slew of threatening acts by China including military exercises near Taiwan and targeted cyber operations. Taiwan has a robust defensive strategy to counter malicious Chinese cyber activities, including its disinformation campaigns. China has a long history of launching cyberattacks against Indian government organisations, critical infrastructure, private sector, and human rights activists. India needs to have a robust strategy to detect and expose China's cyber espionage campaigns.

United States House of Representatives Speaker, Nancy Pelosi's visit to Taiwan in August 2022 led to a slew of threatening acts by China, including military exercises near Taiwan, and targeted cyber operations.[1] The primary objective of these cyberattacks was to disrupt or interfere in order to weaken the confidence of the government and create chaos. These cyber operations can be categorised into three types—low impact Distributed Denial-of-Service (DDoS) attacks and data leaks; cyber-enabled disinformation operations; and cyber espionage.[2] The Office of the President, Foreign Ministry, Defense Ministry, and Taoyuan International Airport websites suffered DDoS attacks.[3] Various Taiwanese organisations and citizens experienced data breaches where their data was leaked online, allegedly by the Chinese.[4] Taiwanese officials have attributed these attacks to the Chinese government.

While DDoS attacks and data leaks did not lead to much destruction, China mounted a significant cyber-enabled disinformation campaign. According to Taiwanese military officials, Chinese disinformation campaigns are "cognitive operations" aimed to harm the government's reputation, undermine military and civilian morale, and instil fear that China would invade Taiwan. There were several instances of said disinformation campaign on Taiwanese social media platforms following Pelosi's announcement that she was coming to Taiwan.[5] These included:

- The claim that the PLA shot down a Taiwanese fighter jet that was travelling with Pelosi's plane.
- The hacking of the official website of National Taiwan University, with the statement "There is only one China in this world" appearing on the site.
- Online rumours that the government was getting ready to ship tens of thousands of rare artefacts abroad for safekeeping.
- Disinformation images that suggested that the PLA had launched missiles over the island by using military photos from two years prior.

[1] Joyu Wang, **"China Extends Military Exercises as Taiwan Battles Cyberattacks"**, *The Wall Street Journal*, 8 August 2022.

[2] Erica Lonergan and Grace Mueller, **"What are the Implications of the Cyber Dimension of the China-Taiwan Crisis?"**, Council on Foreign Relations, 15 August 2022.

[3] **"Taiwan Defence Ministry: Website Hit by Cyber Attacks amid China Tensions"**, *Reuters*, 4 August 2022.

[4] For example, steel producer company Citrix, airline company TigerAir Taiwan, Tuobang construction company, sensitive data of Taiwanese and Hong Kong nationals, Taiwan Power Research Institute, and unauthorised Remote Desktop Protocol Access data of an electronics manufacturing company experienced data breaches. **"Could China – Taiwan Cyber Conflict Deepen the Global Chip Crisis?"**, SOCRadar, 15 August 2022.

[5] Hsia Hsiao-hwa and Raymond Chung, **"China Steps Up Cyberattacks, Disinformation Campaigns Targeting Taiwan"**, *Radio Free Asia*, 8 August 2022.

- China's state broadcaster CCTV claiming that China was expelling Taiwanese nationals before 8 August, which was also false.
- Hacking of 7-Eleven convenience stores with the message "Warmonger Pelosi, get out of Taiwan!"
- Displaying of a message calling Pelosi "an old witch" on digital signage at a railway station in the southern port city of Kaohsiung at a government office in Nantou County.
- Renaming of streets in Taiwan's cities after cities from mainland China on Baidu.

According to researchers, there was a lot of fake information on China's Weibo, some of which made its way onto Taiwanese social media platforms like Line and Facebook and spread rapidly on English language Twitter.[6] All of these incidents indicate the existence of elaborate Chinese cyber espionage campaigns because hacking websites and disinformation operations need considerable intelligence input that are most likely possible through these cyber espionage campaigns.

Based on data relating to state-sponsored cyber activity research,[7] there were 13 cyber operations between China and Taiwan, of which 12 originated from China. Interestingly, eight of these operations (or 79 per cent of the total) were cyber espionage operations while the remaining four were disruptive in nature which did not cause much physical damage.[8]

Taiwan's Cyber Defence Strategy

The flurry of cyber activities in Taiwanese cyberspace and Taiwan's successful cyber defence methods have gained considerable attention from security researchers. Taiwan's cyber defence has mainly aimed at countering Chinese cyber-enabled disinformation campaigns and defending its networks and systems infrastructure. In addition, successful cyberattack on Taiwanese semiconductor manufacturers would represent an attack on the tech industry and might disrupt the supply chain around the globe because Taiwan controls more than 60 per cent of the world's semiconductor manufacturing.[9]

Taiwan's semiconductor manufacturers have been targeted by China's state-sponsored hackers for years. In 2020, a series of deep intrusions known as Operation

[6] Ibid.

[7] **"The Dyadic Cyber Incident and Campaign Dataset"** (DCID) on state-sponsored cyber activity between 2000 and2020; Erica Lonergan and Grace Mueller, no. 2.

[8] Erica Lonergan and Grace Mueller, no. 2.

[9] **"True Spies: A Hack on Taiwan's Semiconductor Industry Could Lead to Chaos"**, Spyscape.

Skeleton Key was discovered with the goal of stealing as much intellectual property as possible, including source code, software development kits, and chip designs from Taiwanese semiconductor companies.[10] In February 2022, Fujimi Inc., a Japanese manufacturer of semiconductor-related products, and its Taiwan subsidiary, experienced unauthorised server access, which was later confirmed to be a malicious attack.[11]

Since Taiwan Semiconductor Manufacturing Corporation (TSMC) supplies more than 90 per cent of the global supply of the most advanced category of mass-produced semiconductors,[12] cyberattacks on TSMC could be detrimental to the electronic needs of the entire world and is one of the reasons why Taiwan has an aggressive cyber defensive strategy, made up of countering disinformation and protecting critical infrastructure.

Countering Disinformation Campaigns

Taiwan's model of countering disinformation is based on protection of freedom of expression while still protecting its citizens from disinformation in the time of crisis, as witnessed in the recent events. Taiwan has been consistently ranked as the world's biggest target for foreign disinformation campaigns for nine years in a row.[13] According to Taiwanese military officials, following Pelosi's visit, 270 instances of fake or misleading information were identified by them.

However, Taiwan has a very robust defence mechanism against disinformation campaigns which includes a community of non-profit fact-checking groups that act as the first line of defence that utilise artificial intelligence (AI) enabled fact-checking bots to crack down on fake news.[14] Further, Taiwan's most popular communication application, Line, has a custom-built fact-checking chatbot named MyGoPen (translated in English as "Don't fool me again") that sends alerts about rumours. The rumour on China planning to evacuate its nationals in Taiwan was debunked on MyGoPen.

Taiwan's Mainland Affairs Office, a government body that deals with China, also puts out urgent statements to curb the spread of disinformation that has the potential to induce panic. Taiwan's efforts to curtail cyber-enabled disinformation campaigns are taken very seriously by government officials. According to Taiwan's Investigative

---

[10] Andy Greenberg, **"Chinese Hackers Have Pillaged Taiwan's Semiconductor Industry"**, *Wired*, 6 August 2020.

[11] **"Chip-related Firm Fujimi Says it was Hit by a Cyberattack last month"**, *The Japan Times*, 2 March 2022.

[12] **"True Spies: A Hack on Taiwan's Semiconductor Industry Could Lead to Chaos"**, no. 9.

[13] Joyu Wang, **"Taiwan is Ground Zero for Disinformation—Here's How It's Fighting Back"**, *The Wall Street Journal*, 26 August 2022.

[14] Joyu Wang and Chuin-Wei Yap, **"Know-It-All Robot Shuts Down Dubious Family Texts"**, *The Wall Street Journal*, 28 February 2019.

Bureau, government investigators have proved around 900 cases of disinformation since 2019 and have filed prosecutions in 200 of these incidents. However, the Investigative Bureau has also stated that since the past two years, Chinese information operations have gotten increasingly sophisticated as most operations are hidden under many layers of "posting and reposting on social media that are difficult to peel back or counter".[15]

Taiwan benefits greatly from the support of tech companies to counter disinformation campaigns. Google has trained around 110 legislative and government officials on various tools to fight false information and its circulation. The company has also donated US$ 1 million to fund the Taiwan Fact Check Centre under its 'Intelligent Taiwan' initiative to help combat disinformation campaigns.[16] Line has spent US$ 5 million on 'Digital Accountability Program' where public chatbots are designed to flag suspicious content to users. The programme also has a database of more than 50,000 fact-checking claims that help authenticate or debunk news.[17] It is through above-mentioned initiatives that Taiwan was able to restrict Chinese cyber-enabled disinformation operations in August 2022.

Defending Critical Infrastructure

Based on lessons learnt from the ongoing Russia–Ukraine War, Taiwan aims to set up a satellite network in case China forces Taiwan to go offline, similar to Ukraine's usage of Starlink as a backup.[18] In order to ensure that Taiwan's communication networks continue to function in the event of a war or natural disaster, the government of Taiwan is creating a 'Communication Network Digital Resilience Reinforcement with Response or Wartime Application Emerging Technology Plan'.

In the event of damage or sabotage to submarine cables and telephone lines, Taiwan will be able to sustain communication services like video conferencing, Voice over Internet Protocol, and live streaming by deploying non-geostationary orbit (NGSO) satellite systems. The Ministry of Digital Affairs (MODA) will start deploying NGSO equipment in 700 domestic locations and three international locations for testing since Taiwan does not currently have a commercial NGSO network. The benefit of such a plan is that, once the infrastructure is in place, users' mobile phones can be switched to the NGSO network to ensure wireless reception, regardless of which telecommunications company they are tied to.[19]

---

[15] Joyu Wang, no. 13.

[16] **"Google Endows Fact Check Hub"**, *Taipei Times*, 8 November 2021.

[17] Joyu Wang, no. 13.

[18] Starlink is a satellite internet constellation operated by SpaceX, providing satellite Internet access coverage to 40 countries.

[19] Keoni Everington, **"Taiwan Building Backup Satellite Internet Network amid Risk of Chinese Attack"**, *Taiwan News*, 14 September 2022.

Furthermore, MODA has implemented Inter-Planetary File System (IPFS) technology to strengthen its cybersecurity defences against cyberattacks from China and other adversaries. With IPFS, users can store and backup files and web pages over a network of nodes, removing centralised points of failure and getting around censorship measures.[20] This is a crucial initiative considering the usage of wiper malware[21] by Russia against Ukraine.

Chinese Cyberattacks on India

Chinese cyber threat actors have a long history of attacking government organisations, critical infrastructure, private sector, and human rights activists in India. Since 2008, China has been accused of attempting to hack government organisations like the Ministry of External Affairs and National Information Centre (2008),[22] Prime Minister's Office (2010),[23] Defence Research and Development Organisation (2013),[24] and Air India (2021, before privatisation).[25] China has also been blamed for cyberattacks on multiple Indian critical infrastructure like the 2021 attack on India's power[26] and telecommunication infrastructure,[27] hacking attempt on India's vaccine makers, Bharat Biotech and Serum Institute of India,[28] and the 2022 power grid incident in Ladakh.[29] Furthermore, cyberattacks from China in the private sector include the 2018 compromise of Managed Service Providers and technology companies[30] and targeting of Indian media houses in 2021.

India has also been a victim of four major Chinese espionage operations along with other countries where their civil society, government, and private organisations have

[20] Jason Nelson, **"Taiwan Turns to Ethereum IPFS Tech to Thwart Chinese Cyberattacks"**, *Decrypt*, 12 August 2022.

[21] A type of malware that wipes out files from infected systems. See Tim Keary, **"Russia-Ukraine Cyberwar Creates New Malware Threats"**, *VentureBeat*, 17 August 2022.

[22] Indrani Bagchi, **"China Mounts Cyber Attacks On Indian Sites"**, *The Times of India*, 5 May 2008.

[23] Ashish Khetan, **"Chinese Hackers Target PMO"**, *India Today*, 14 January 2010.

[24] Mohit Kumar, **"Chinese Hackers Infiltrate Indian Defence Research Organisation"**, *The Hacker News*, 13 March 2013.

[25] Nikita Rostovcev, **"Big Airline Heist"**, Group IB, 10 June 2021.

[26] David Sanger and Emily Schmall, **"China Appears to Warn India: Push Too Hard and the Lights Could Go Out"**, *The New York Times*, 28 February 2021.

[27] Thomas Roccia, **"Operation Diànxùn: Cyber Espionage Campaign Targeting Telecommunication Companies"**, McAfee, 16 March 2021.

[28] Krishna Das, **"Chinese Hackers Target Indian Vaccine Makers SII, Bharat Biotech, Says Security Firm"**, *Reuters*, 1 March 2021.

[29] **"China Tried to Hack Power Grid Systems in Ladakh Thrice: R K Singh"**, *Business Standard*, 8 April 2022.

[30] **"Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information"**, U.S. Department of Justice, 20 December 2018.

been compromised. These include targeting of NGOs, political and law enforcement agencies in East and South Asia in 2019;[31] 2020 hacking of 75 organisations in India, Kazakhstan, Kyrgyzstan, Malaysia, Russia and Ukraine;[32] SlothfulMedia malware attack on India, Kazakhstan, Kyrgyzstan, Malaysia, Russia and Ukraine for espionage purposes;[33] and RedFoxtrot linked cyber espionage in Afghanistan, India, Kazakhstan, Kyrgyzstan, Pakistan, Tajikistan and Uzbekistan in 2021.[34]

Key Takeaways for India

While Chinese cyber operations in Taiwan did not lead to an escalation, it is useful to juxtapose the key takeaways from this event as against the cyber conflict between Ukraine and Russia. China has used cyberspace to gain classified information through cyber espionage and to construct false narratives through information warfare. In the Russia–Ukraine War, both Russia and Ukraine employed disruptive cyber offensive operations to target critical infrastructure along with cyber espionage and information operations.

China was therefore cautious of not launching more sophisticated cyberattacks that would damage critical access points hampering future cyber operations or existing cyber espionage efforts. This is a crucial distinction indicating their hesitation for an on-ground escalation. Even before Russia's announcements of "military operations" in Ukraine, Russia had undertaken disruptive wiper cyberattacks on 14 January on Ukrainian critical infrastructure networks which then led to an escalation. While offensive cyber operations by themselves aren't indicative of a possible military conflict, coercive cyber operations coupled with threats and warnings from officials, military exercises, and suspension of talks suggest possible escalation.

China might have learnt from the Russian example that offensive cyber operations like deployment of wipers blew Russia's access to Ukrainian networks even before the war started. Offensive cyber operations are extremely difficult to execute successfully and premature execution may result in loss of capability.[35] China could in foreseeable future launch more disruptive cyberattacks against Taiwan that could include targeting critical infrastructure and military assets and can be seen as a sign

[31] **"BRONZE PRESIDENT Targets NGOs"**, Secureworks, 29 December 2019.

[32] Christopher Glyer, Dan Perez, Sarah Jones and Steve Miller, **"This is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits"**, Mandiant, 25 March 2020.

[33] Shannon Vavra and Sean Lyngaas, **"Chinese Hackers Suspected in Cyber-espionage Operation Against Russia, India"**, *Cyberscoop*, 7 October 2020.

[34] **"Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries"**, Recorded Future, 16 June 2021.

[35] Tim Starks, **"Did Russia Mess Up its Cyberwar with Ukraine Before It Even Invaded?"**, *The Washington Post*, 4 August 2022.

for a possible invasion of Taiwan. This is due to China's military strategy that states that cyber operations play a crucial role early on in a conventional conflict.[36]

In the Indian context, there are some takeaways given the nature of Chinese cyber operations in Taiwan. Chinese mis-information operations in Taiwan were of an advanced nature. China might face difficulties to employ similar disinformation campaigns due to the complexities in language and social norms in India. Apart from the numerous cyberattacks launched against physical infrastructure and assets in India—some of which have been mentioned in previous sections—China–Pak collusion in the information warfare domain is well-documented and a cause for concern. China can further up the ante with its 'all-weather friend' to undertake disinformation campaigns.[37] China is also allegedly collecting voice samples using artificial intelligence from 'military sensitive regions of India', including Jammu and Kashmir and Punjab that can be later used for information and cyber espionage operations.[38]

India needs to have a robust strategy to detect and expose China's cyber espionage campaigns. Cyberattacks are enabled with critical intelligence gathered by Chinese government agencies. China has a long history of launching cyberattacks against Indian government organisations, critical infrastructure, private sector, and human rights activists. These attacks are indicative of an elaborate and existing cyber espionage campaign against India. The key to addressing such challenges is to reinforce intelligence gathering and enhance collaboration with private sector tech companies that have the technical expertise to help fight such operations.[39] Finally, there is immense scope for cooperation on cybersecurity between India and Taiwan, especially on information sharing on cyberattacks and technical assistance from Taiwan to set up semiconductor plants in India.

[36] Erica Lonergan and Grace Mueller, no. 2.

[37] Aditya Bhan and Sameer Patil, **"Cyber Attacks: Pakistan emerges as China's proxy against India"**, Observer Research Foundation, 15 February 2022.

[38] Ananya Bhardwaj, **"Chinese Company 'Sneaking' Voice Samples of Indians in Border States, US Think Tank Claims"**, *The Print*, 29 August 2022.

[39] See **"Open, Safe & Trusted and Accountable Internet"**, Ministry of Electronics and Information Technology, Government of India, May 2022.

About the Author

Ms Krutika Patil is Research Assistant for the Project on Cyber Security at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses