KAUTILYA
SCHOOL OF
PUBLIC POLICY

# Issue Brief Series

**“Assessing China’s Role in State-Sponsored Hacking: Implications for India’s National Security”**

**Issue Brief: IB-2025-23**

**Submitted by:** Ms. Neelam (MPP Cohort 2024-26)

Under the Supervision of: Amb. D. B. Venkatesh Varma, Visiting Instructor at Kautilya School of Public Policy

**Cite this Report** as Neelam. Assessing China’s Role in State-Sponsored Hacking: Implications for India’s National Security (2025) [online]. Available at: htttps://kspp.edu.in//issue-brief/china’s-role-in-state-sponsored-hacking-implications-for-india’s-national-security

# Assessing China's Role in State-Sponsored Hacking: Implications for India's National Security


## Abstract

The rise of cyber warfare is a key component of modern conflict, and this case study explores this. It will focus on China's cyber strategy and its implications for India's national security. It will highlight the advanced tools of cyber warfare threats like artificial intelligence, ransomware, and state-sponsored hacker groups like APT41 and PLA Unit 61398. These are the main hacker groups working in China. this case study shows the major timeline of global and India-specific cyber-attacks. There is a comparison of India's readiness with China's capabilities and identifies the key national challenges and weaknesses in India's cyber infrastructure. Discuss with policy gaps and limited international coordination. At last, it will conclude with five actionable recommendations, which include finalizing a national cybersecurity strategy, infrastructure, critical security indicator, investment in cyber talent improvement for intelligence sharing and strengthening global cooperation. in this digital age, the national security for India is underscored by the urgent need for these cyber threats as a central component.


## Introduction

Cyber warfare is no longer fictional. It now allows countries to gain power without direct war. This is a new tool used by states to hack, disrupt or damage other country's systems (RAND Corporation, 2013). China has built a strong cyber strategy with a combination of intelligence, military, and civilian tech. China is a neighbouring country of India, where we share a land border of 3,488 kilometres. This border runs along the states of Jammu and Kashmir, Himachal Pradesh, Uttarakhand, Sikkim, and Arunachal Pradesh. Major incidents like the Equifax breach, Microsoft Exchange hack, and attacks on India's power grid show its

growing cyber strength. These actions show a clear threat to the Indian economy, polity, and military strategies at risk. While India has set up CERT-In and I4C, gaps remain. This case study reviews China's cyber actions and in response India's re-actions and policies to improve its cyber defences with global cooperation.

**What is Cyber?**

This term generally refers to computers, networks, and digital communications. The word cyberspace often describes the entire digital world; it includes the internet and other connected systems. "The online world of computer networks and especially the internet" is described by Merriam-Webster (Merriam-Webster, n.d.). cyberspace is a global network of information systems it includes the internet, telecommunication systems, computers and other digital devices (NIST, n.d.). In simple terms, this is all systems that are connected digitally, such as data centres, smartphones, and machines run by power plants. Working in cyberspace is exchanging information or controlling physical actions through networks. These systems, help to connect people, businesses and governments.

**Cyber Threat Type**

*Table1. This table lists major forms of cyber threats and explains how each method is used to compromise systems or users.*

| Cyber Threat Type | Description |
|---|---|
| Phishing | Tricking users into giving up sensitive info |
| Malware | Malicious software like trojans or viruses |
| Ransomware | Locking systems until a ransom is paid |
| Botnets | Hijacked networks of infected devices |
| Denial-of-Service (DoS) | Flooding systems to crash them |
| Spoofing & Spam | Faking identity or spamming users |

**What is Cyber Warfare?**

The Cyber warfare is used by countries to gain a military, political, or economic advantage over another country. It is kind of stealing important information, damaging infrastructure such as power plants, and spreading false information or news. It's different from regular war, as cyber warfare does not involve physical violence. Such attacks form part of without borders, and it's often done secretly without taking any responsibility.

For example, the Stuxnet virus damaged attack by Iran's nuclear centrifuges in 2010, (Zetter, 2014). Russia used cyberattacks to shut down power in Ukraine between 2015 and 2017 (Rid, 2020). This is part of multi-domain operations, where countries use air, land, sea, space, and cyber tools to gain full control in the conflict.

The **RAND Corporation (2013)** explains cyber warfare as actions taken by a country or group to harm another country through computer systems. These can include using malware to spy, denial-of-service (DoS) attacks to crash websites, or hacking into critical systems like hospitals or banks. this is different from traditional war, these attacks can be launched from anywhere and are hard to trace.

Cyber warfare is now a key part of a country's total power. Which often starts before an actual war begins and is used along with military and intelligence efforts. Since many attacks are hidden, it is difficult to know who is behind them. The line between spying during peace and sabotage during war is blurry. But the threat is real countries can attack important systems like banking, electricity, and defence from anywhere in the world (Sanger, 2018).

**China's Cyber Investments and Warfare Capabilities:** The extension of China's security sector is rapidly increasing; its market revenues are projected to rise from $5.33 billion in 2016 to increase by $31.41 billion by 2027. It clearly shows a strategic push for cyber dominance through military-civil fusion. The civilian tech and military operations are closely integrated to enhance national security power.

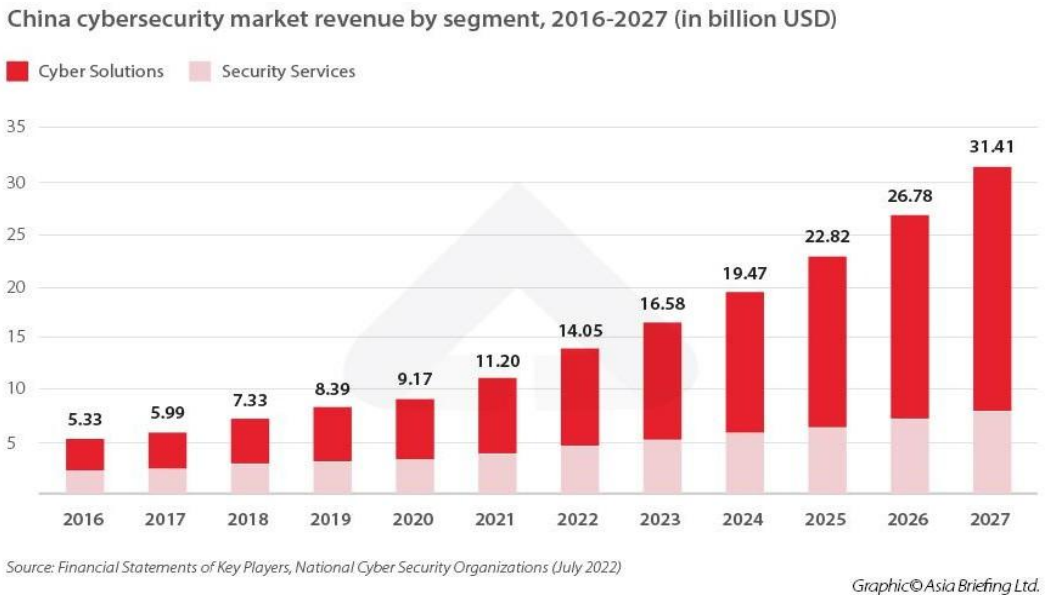



*Figure 1. Shows China's rising investment in cybersecurity, with steady growth in both solutions and services from 2016 to 2027.*

China has developed strong cyber capabilities over the past 20 years with the help of its military, intelligence agencies, and private groups. In the year 2015, China formed the **Strategic Support Force (SSF)** to bring together its cyber, space, and electronic warfare units under one military command (Erickson, 2016). it showed that China's increase in "information warfare" is a key part of modern conflict.

One major unit is **PLA Unit 61398**, also known as **APT1**. According to a report by **Mandiant (2013)** which linked this group to over 140 cyberattacks on companies worldwide, mainly to steal trade secrets. Later, the **U.S. Department of Justice (2014)** charged five Chinese military officers for hacking U.S. firms. The other group named **54th Research Institute**, was blamed for the **Equifax breach in 2017**, which exposed the personal data of 145 million Americans (U.S. Department of Justice, 2020).

China's spy agency, the Ministry of State Security (MSS), now plays a bigger role than the military in cyber operations. MSS-linked groups like APT41 and HAFNIUM have hacked

thousands of systems worldwide. They were also linked to attacks that misused Microsoft Exchange software (Microsoft, 2021).

China's cyber strategy has changed too. Experts at SIPRI (2021) say China now uses cyber tools actively even during peace, not just in war. President Xi Jinping has also said that China wants to be a top cyber power (Segal, 2020). Even though China agreed in 2015 not to steal business data using cyber means, many reports say it continues (U.S. Department of Justice, 2020).

China combines civilian technology with military goals through a policy called **"military- civil fusion."** It also follows ideas like **"Unrestricted Warfare"**, which means using cyber-attacks, media control, and legal tools to meet its goals. In short, China's cyber force includes military hackers, spies, and even private tech firms working together.

**China's Cyber Attacks: A Timeline of Major Incidents (2010–2024)**

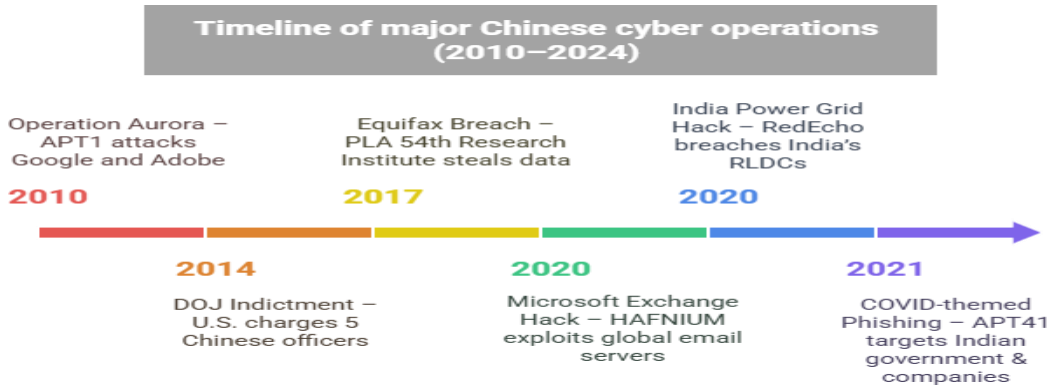



*Figure 2. Chinese cyber operations from 2010 to 2024, highlighting key attacks like Operation Aurora, Equifax breach, and RedEcho targeting India.*

**Global Case Studies**

China's government-backed hackers have carried out many majors cyberattacks around the world. The two key examples are the **Equifax breach** and the **Microsoft Exchange** hack. In the Equifax case, four officers from China's People's Liberation Army were charged in 2020

for hacking into the credit agency's systems in the year 2017. They stole the personal and financial data of around 145-147 million Americans, making it one of the largest data thefts in history (U.S. Department of Justice, 2020).

The second major case happened in 2021 when Microsoft revealed that hackers exploited unknown weaknesses in its Exchange Server email software. The attack was linked to a Chinese group called HAFNIUM. They accessed company emails and installed secret backdoors across thousands of networks worldwide. The U.S. and its allies formally accused China of being behind this large-scale operation (Microsoft, 2021).

These incidents are part of a larger trend. In 2009, Chinese military unit APT1 (also known as Unit 61398) was tied to "Operation Aurora," a series of attacks on Google and other tech firms. A report by FireEye showed that APT1 had been stealing sensitive company data for years (Mandiant, 2013). China has also been blamed for the 2015 U.S. Office of Personnel Management breach, which exposed millions of government records, as well as for cyber spying on governments in Australia, Southeast Asia, and other regions (Zetter, 2015; FireEye, 2013).

The table below summarizes some key China-linked cyber campaigns and their targets:

*Table 2 Lists major Chinese cyber operations from 2010 to 2021, identifying each attack's key actors, targets, and impacts, including incidents affecting the U.S. and India*

| Year | Operation/Incident | Chinese Actor | Target / Impact |
|---|---|---|---|
| 2010 | *Operation Aurora* | APT1 (PLA Unit 61398) | Google/Adobe (intellectual property, source code) |
| 2014 | DOJ Indictment (APT1) | PLA Unit 61398 | Multiple U.S. firms (energy, aerospace, etc.) |
| 2017 | Equifax Breach | PLA 54th Research Institute | Equifax (USA; data on 145M consumers) |
| 2020 | Microsoft Exchange Hack | HAFNIUM (China) | Email servers globally (email data, backdoors) |
| 2020 | India power grid hacks | RedEcho (China) | Indian power RLDCs (malware/trip outages) |

| | | | |
|---|---|---|---|
| 2021 | India COVID phishing | APT41 (China) | Indian govt/industry (COVID-themed phishing) |

This timeline shows China's campaigns against both foreign and Indian targets. In each case, U.S. and allied cybersecurity firms or governments publicly traced the intrusions back to Chinese sources.

**Global Comparison of Significant Cyberattacks (2006–2020)**

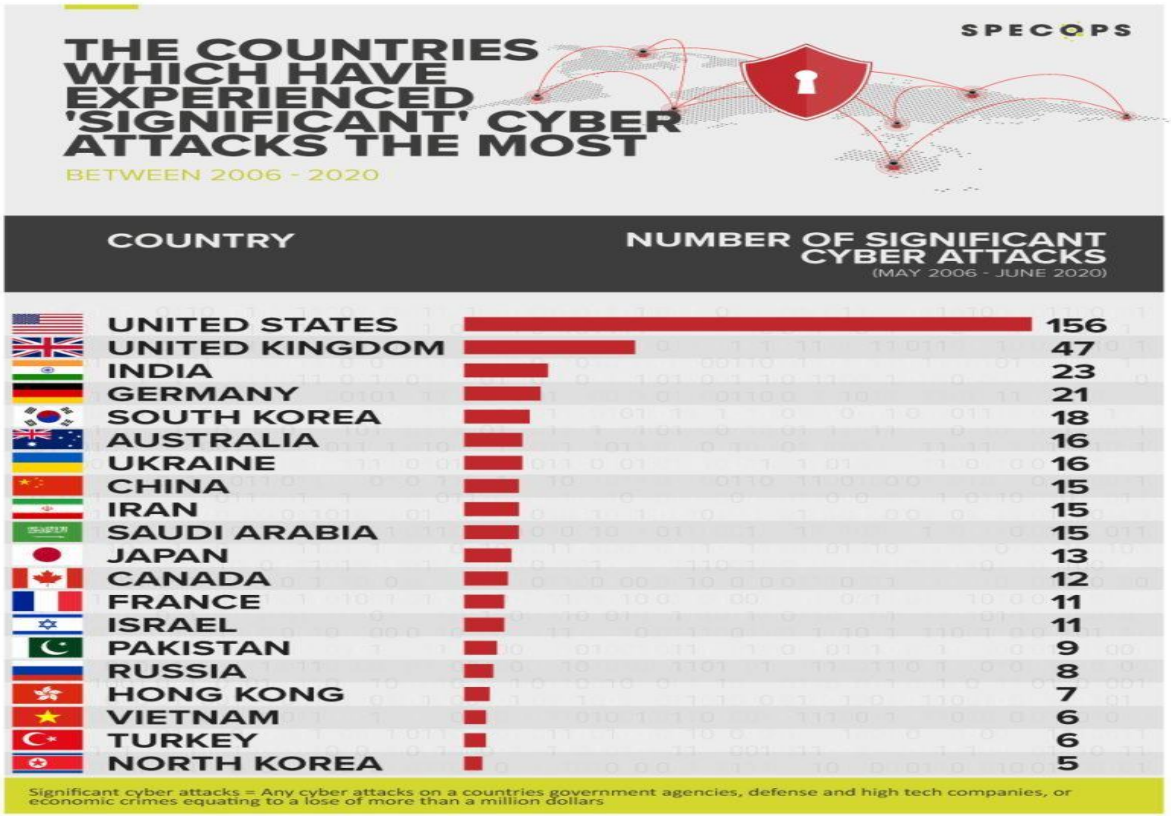



*Figure 3 Shows the number of significant cyberattacks faced by countries between 2006 and 2020, with the U.S., U.K., and India among the most targeted.*

This chart shows the number of significant cyberattacks in different countries that faced significant attacks between 2006 and 2020. The United States experienced the highest number of attacks (156 attacks), far more than any other nation. The United Kingdom comes next with 47 attacks, followed by India at 23. Similarly, Other countries like Germany, South Korea, and Australia faced 23, 21, and 18 attacks respectively. Surprisingly, China, often seen as a source of attacks, faced only 15 attacks. This suggests that advanced countries with large

digital systems are more repeated targets. While India's position shows it is among the top three countries under cyber threat and needs stronger cyber defences.

**India-Focused Case Studies:** While China has launched global cyber campaigns, India has also been directly targeted

1. RedEcho (2020-21): in the period of the Galwan Valley conflict, a Chinese group targeted India's power grid while using malware like ShadowPad to secretly access and monitor Regional Load Despatch Centres (Recorded Future, 2021). These cyber- attacks were used to apply pressure during military tensions.

2. **APT41 COVID Phishing**: During the COVID-19 pandemic, Chinese hackers mimicked Indian government agencies to send fake messages and trick people into installing malware. This tactic is known as **social engineering** (CyberScoop, 2021). This exposed both public and institutional systems to cyber risks which was used by china.

3. Mumbai Blackout (2020): Although the Mumbai power outage was officially blamed on technical faults, reports suggested that Chinese malware may have been present at that time, raising concerns of a cyber link (Recorded Future, 2021).

*Table 3 Summarizes major cyberattacks on Indian targets from 2010 to 2024, highlighting the methods used, sources of attribution, and the resulting impact on government and public systems*

| Year | Cyberattack | Target | Method | Attribution (Source) | Damage/Impact |
|---|---|---|---|---|---|
| 2010 | Shadow Network (Espionage) | Indian Government Systems | Malware and unauthorized remote access | Canada's IACC & Munk School (Toronto Star) | Espionage, classified documents stolen |
| 2012 | Indian Navy Eastern Command Breach | Indian Navy | Infected USB and phishing | The Indian Express / thehackernews.com | Sensitive naval data leaked during submarine trials |

| | | | | | |
|---|---|---|---|---|---|
| 2018 | EPFO Data Breach | Indian EPFO | Exploitation of Web Vulnerability | CERT-In (Business Standard) | Data of ~10 million citizens compromised |
| 2022 | AIIMS Ransomware Attack | Indian Healthcare | Ransomware via phishing or remote access | NPR & Government sources | Hospital operations halted, and patient data locked |
| 2024 | Immigration Data Theft | Indian Immigration Data | Spear-phishing and database exploitation | Indian CERT / Cyber Cell Reports | Sensitive immigration records leaked online |

Recently China directly targeted India's critical infrastructure and networks by cyberattacks. The major one is RedEcho campaign which happened in 2020-2021. The China's group called RedEcho hacked into 10 Indian power sector organisations including 4/5 of India's main power grid control reported by cybersecurity firm "Recorded Future" (The Hacker News, 2021). Used advanced malware such as PlugX and ShadowPad to be inside in these networks. China strategically did this as the time was the same as the violent India-China border clash in May 2020, suggesting the connection of a military standoff. In the year 2022 attacks had reached seven state-level power centres in the north side of India (CyberScoop, 2022). These attacks could have been used to cause blackouts or manipulate the power grid according to experts.

Another case between 2020 and 2021 during COVID-19 involves the APT41 Chinese cyber group. The messages looked like official Indian government communications and tricked people into giving away passwords and information. This showed how China mixes economic and intelligence goals in its hacking efforts. Social engineering played on public fear during the pandemic (CyberScoop, 2021). In 2020 large power outage happened in

Mumbai. A report from Recorded Future suggests that this outage happened during a larger Chinese cyber campaign they are targeting India's power grid Later technical review blamed equipment failure (Indian Express, 2021). This disrupts essential services in India and these incidents raise concerns about foreign hackers.

It clearly shows that China's focus is India's key sectors like power and government systems. According to experts, this part is a bigger strategy to use cyberspace as a weapon in the India- China rivalry. China aims to gather intelligence and putting pressure on India through cyber- attacks (The Hacker News, 2021; Recorded Future, 2021).

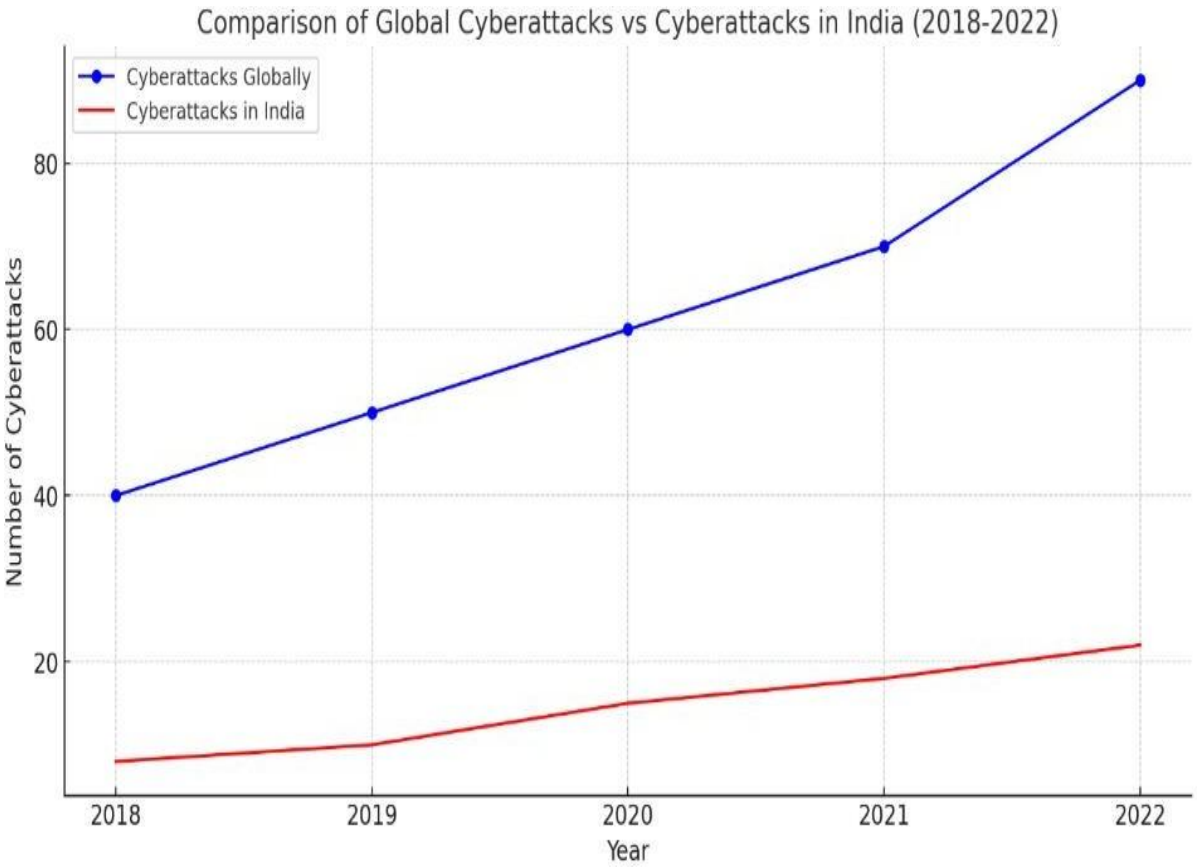



*Figure 4 Compares the rise in global cyberattacks with those targeting India between 2018 and 2022, showing a consistent upward trend in both.*

**Causes Behind China's Cyber Operations**

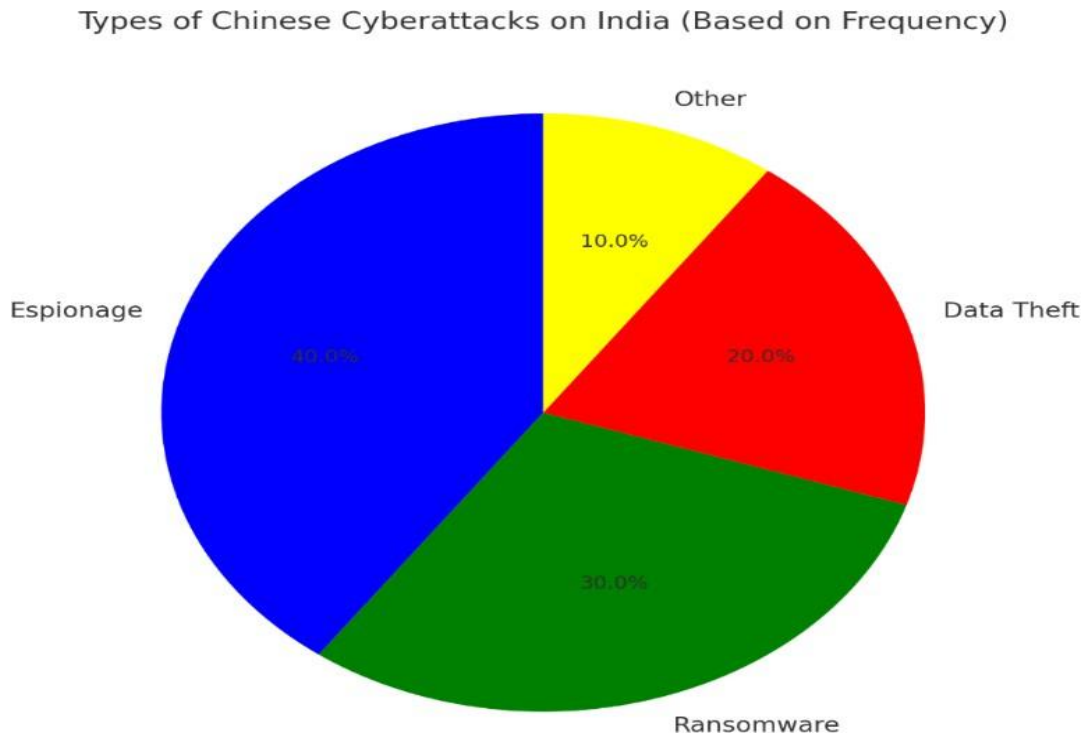



*Figure 5 utlines India's cybersecurity policy timeline, showing major initiatives and institutional developments from 2000 onward.*

China's reason for these operations is to gain an advantage over other countries without coming to it actual war. One reason is to close the technology gap with other countries like the U.S. Another is military and political power gain. During conflicts like the 2020 border tension with India. Cyber tools are also cheaper and less risky than other traditional warfare. China follows the doctrines of "*Three Warfare*" and "*Unrestricted Warfare*" This is China's strategy to use cyber-attacks, media control and legal tactics as a part of an overall plan to grow stronger without a straight fight.

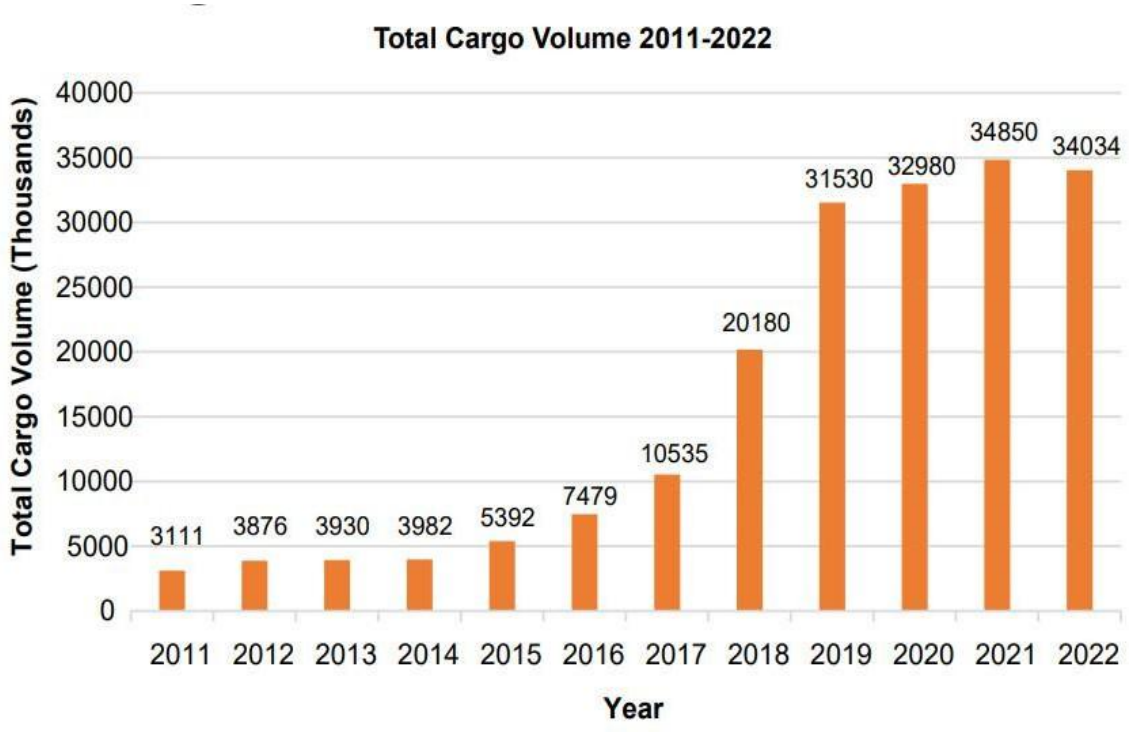



*Figure 6 Shows total cargo volume from 2011 to 2022, highlighting sharp growth after 2016, indicating improved logistics and rising trade activity.*

This graph shows the steady rise in total cargo volume from **2011 to 2022**. the volume was around **3,111 thousand units** in 2011, and it grew slowly until 2016. After that, there was a sharp increase from **7,479 thousand in 2016** to **20,180 thousand in 2018**, and further to over **34,000 thousand by 2022**. This data shows major growth in cargo handling, especially after 2017, suggesting showing improved logistics infrastructure and growing trade activity.

**Causes and Consequences of cyber-attacks for India**

China's cyberattacks are driven by a mix of strategic such as economic, and political goals. One major goal is to steal technology and sensitive information from other countries. U.S. officials have said that China uses cyber spying to give its companies an unfair advantage in global markets (U.S. Department of Justice, 2020). Chinese military papers also say that stealing intellectual property is important for China’s growth (Small Wars Journal, 2013). So,

Chinese hackers work not only for military reasons but also to help Chinese businesses compete with global companies.

So, China uses cyberattacks for military reasons. By hacking India's defence and infrastructure systems, though, they can collect important details like troop movements or communication plans, especially during tense times. For example, the RedEcho attacks on India's power grid happened around the same time as the 2020 border clash in Galwan Valley (The Hacker News, 2021). Chinese leaders see cyber tools as cheap and powerful weapons.

Their military writings like the idea of "*Unrestricted Warfare*" support using cyber-attacks to weaken enemies without fighting a war. They see cyber operations as a normal part of state power. Even during peacetime, China uses cyber tools. Overall, China uses cyber tools as a quick and quiet way to achieve its national goals (Sanger, 2018; SIPRI, 2021).

**Consequences for India.**

- National security compromise
- Economic damage to Indian R&D
- Public mistrust in digital services

The cyberattacks from China are now a serious threat for India. The Indian national security, which includes economic, and societal is under threat as China is growing in cyber technology. If China breaks into India's military or government networks, it can steal important information like troop movements or infrastructure plans. This can give it an edge during conflicts (Sanger, 2018). In terms of the economy, cyber theft can harm Indian companies by stealing their research and development (R&D), especially in key areas like medicine and telecom. This makes it harder for Indian firms to compete globally. Around the world, stolen intellectual property leads to losses worth hundreds of billions of dollars yearly

(WIPO, 2022). Socially, frequent cyberattacks reduce public trust in digital platforms. When personal data is leaked, it is difficult for people to feel safe using online services. For example, during the 2020 India–China border tensions, India banned 59 Chinese apps, including TikTok, to protect its digital space (CBS News, 2020). This shows how cybersecurity now affects both politics and trade.

These incidents have made people in India more aware of online dangers. While this may help improve defences, it also raises questions about how secure India's digital systems really are. Overall, China's cyber activities have pushed India to make cybersecurity a national policy priority (The Hacker News, 2021).

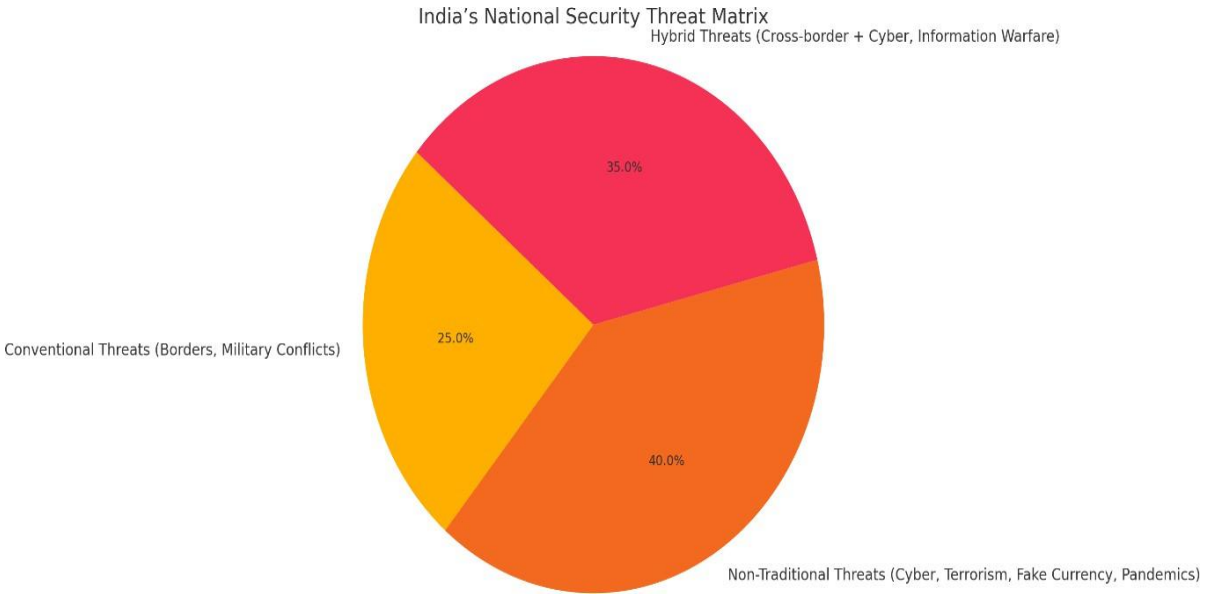



*Figure 7 illustrates India's national security threats by type, showing the growing share of non-traditional and hybrid threats alongside conventional military risks.*

Here is the pie chart which shows India's National Security Threat Matrix, is divided into:

- Conventional Threats (25%) – such as military conflict and border tensions
- Non-Traditional Threats (40%) – including cyberattacks, terrorism, pandemics, and fake currency

- Hybrid Threats (35%) – combining physical and digital dimensions like cross-border cyberattacks and information warfare

**Why the World Is Not Able to Handle These Attacks**

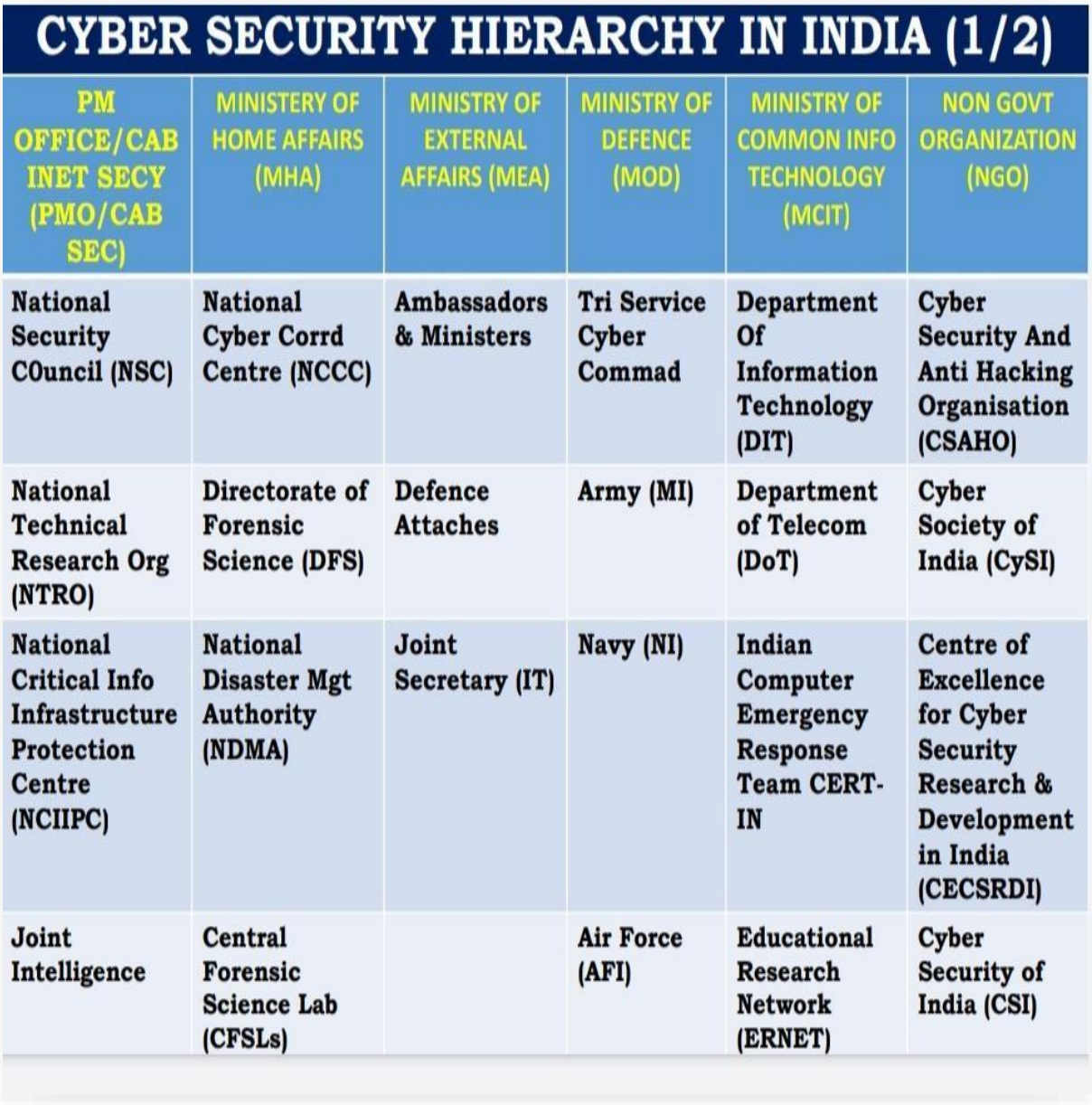
The world finds it hard to stop cyberattacks because it is difficult to know who is behind them. Hackers often hide their identities or route their attacks through other countries, which makes it hard to trace them (Rid and Buchanan, 2015). Also, global laws on cybercrime are weak and outdated. There is no worldwide agreement on what counts as a cyberattack or how to punish countries that sponsor them (Hathaway et al., 2012). Because of this, most countries respond on their own, and often too slowly. The lack of trust and cooperation between powerful nations makes it even harder to create strong global rules on cyber threats (Sanger, 2018).

**Indian Cybersecurity Framework**

**Information Technology (IT) Act, 2000 (amended in 2008):** Main law for cybercrimes and electronic transactions in India.

**National Cyber Security Policy, 2013:** Aims to protect public and private infrastructure from cyber threats.

**Pending Data Protection Bill:** A proposed law to protect personal data and improve user privacy, still awaiting approval.



| CYBER SECURITY HIERARCHY IN INDIA (1/2) | | | | | |
|---|---|---|---|---|---|
| PM OFFICE/CAB INET SECY (PMO/CAB SEC) | MINISTERY OF HOME AFFAIRS (MHA) | MINISTRY OF EXTERNAL AFFAIRS (MEA) | MINISTRY OF DEFENCE (MOD) | MINISTRY OF COMMON INFO TECHNOLOGY (MCIT) | NON GOVT ORGANIZATION (NGO) |
| National Security COuncil (NSC) | National Cyber Corrd Centre (NCCC) | Ambassadors & Ministers | Tri Service Cyber Commad | Department Of Information Technology (DIT) | Cyber Security And Anti Hacking Organisation (CSAHO) |
| National Technical Research Org (NTRO) | Directorate of Forensic Science (DFS) | Defence Attaches | Army (MI) | Department of Telecom (DoT) | Cyber Society of India (CySI) |
| National Critical Info Infrastructure Protection Centre (NCIIPC) | National Disaster Mgt Authority (NDMA) | Joint Secretary (IT) | Navy (NI) | Indian Computer Emergency Response Team CERT-IN | Centre of Excellence for Cyber Security Research & Development in India (CECSRDI) |
| Joint Intelligence | Central Forensic Science Lab (CFSLs) | | Air Force (AFI) | Educational Research Network (ERNET) | Cyber Security of India (CSI) |

*Figure 8 Displays the cybersecurity institutional structure in India, showing key government and non-government bodies involved across ministries and sectors.*

As India has taken many steps to improve its cyber defence, but the challenges remain the same. The main agency in CERT-In (Indian Computer Emergency Response Team), which is under the Ministry of Electronics and Information Technology monitors cyber threats, issues the same warning and manages major attacks. It also helps to alert companies about new malware and asks to fix known

software issues quickly and fast (Microsoft, 2021)

Another key body the National Critical Information Infrastructure Protection Centre (NCIIPC), it offers solutions as well as protects critical sectors like energy, banking and telecom by identifying risks. On the law side, in 2018 India set up the Indian Cyber Crime Coordination Centre (I4C) under the Home Ministry. I4C works with state police and international partners. India signed an agreement with the U.S. in 2025 with the Department of Homeland Security to share cyber intelligence and forensics tools (North East Herald, 2025).

India also created the National Cyber Coordination Centre (NCCC) to gather signals intelligence from different departments. The government launched Bharat NCX In 2023, It is a national cyber drill with participation from the police, military and industry (PIB, 2023).
During this exercise, an urgent need for a new National Cyber Security Strategy that strengthens laws and improves cooperation between the public and private sectors according to the experts (PIB, 2023). The current policy from 2013 is outdated.

Our private companies must, India follows the Information Technology Act (2000, amended in 2008), and CERT-In's 2022 guidelines, which require companies to report any data breach. The pending Personal Data Protection Bill this aims to improve user privacy. New telecom rules also make 5G networks follow strict security standards, limiting equipment from risky foreign sources.

Still, some problems continue. Many Indian agencies work in isolation, and private companies often see cybersecurity as just a legal requirement rather than a real priority. After the 2020 Mumbai blackout, a government panel called for better enforcement of cyber protocols (Indian Express, 2021). Groups like NASSCOM and the Data Security Council of India (DSCI) are now helping, but stronger collaboration is needed.

In short, India has created a strong base for cyber defence with CERT-In, NCIIPC, I4C, and NCCC. It is working with countries like the U.S. and running national drills. However with fast digital growth and increasing cyber threats from China, India must keep improving its policies, coordination, and funding for cybersecurity (Northeast Herald, 2025; PIB, 2023).

**Comparison Table – China vs India in Cyber Strategy**

*Table 4 Compares China and India's cyber strategies across key areas like policy, command, military integration, and global cooperation, highlighting China's offensive lead and India's defensive gaps*

| Aspect | China | India |
|---|---|---|
| Cyber Strategy | Offensive, proactive strategy focused on dominance | Defensive posture, reactive approach |
| Policy Framework | Well-defined, state-led policies (e.g., Cybersecurity Law 2017) | Lacks a final national cyber strategy (pending since 2019) |
| Command Structure | Unified under Strategic Support Force (SSF) | Disjointed command across multiple agencies |
| Military Integration | Full military-civil integration (Military-Civil Fusion) | Limited coordination between military and civilian sectors |
| Use of Civilian Tech | Aggressively leverages tech giants (e.g., Huawei, Alibaba) | Emerging but uncoordinated engagement with the private sector |
| Cyber Talent Development | Heavy investment in education and state-sponsored training | Shortage of skilled cybersecurity professionals |
| Cyber Threat Intelligence | Dedicated intelligence units (APT1, APT41, MSS) | No central fusion centre; scattered reporting systems |
| Public Awareness & Resilience | Controlled media, centralized awareness campaigns | Low public awareness and preparedness |
| International Collaboration | Bilateral pacts, strategic silence in norms debate | Active in global forums (Quad, UN) but reactive in norms shaping |
| Cyber Doctrine | Shifted from active defence to continuous cyber pressure | No clear public doctrine; follows conventional defensive stance |

**Recommendations**

India must prepare for future cyber threats through the development of new technologies like artificial intelligence (AI), computing drones, quantum, and synthetic biology. These tools help to improve both attack and defence methods. For example, AI helps in faster decision- making, while quantum tech could break current encryption systems.

1. Finalize a New National Cybersecurity Strategy

It must include laws to handle ransomware and cyber spying, which will help to secure national cyber security. India now needs to release an updated strategy to replace the 2013 cyber policy version. This should clearly define the roles of the military, intelligence, government bodies and private sector. (PIB, 2023).

2. Secure Critical Infrastructure

The key sectors for critical infrastructure are energy, telecom, banking, and transport should follow strict cyber safety rules. Organizations must do regular security checks, run live drills like red-teaming, and build quick-response systems to handle attacks (PIB, 2023).

3. Improve Threat Intelligence Sharing

India's CERT-In should be given more authority and resources to gather cyber threat data. And our private companies must share anonymised information on attacks. India should also create a Cyber Threat Fusion Centre and sign more agreements with friendly countries to track groups such as the APT41 (PIB, 2023).

4. Build Cyber Skills and Awareness

India should build our Cybersecurity education in schools and universities. These programs like Cyber Surakshit Bharat should be expanded. Scholarships and funding should support students, local startups, and research in AI, encryption, and for network safety (PIB, 2023).

5. Strengthen Global Cooperation

The India must work with international partners like the Quad and the UN to set global rules and run joint cyber drills. India now should also promote transparency by encouraging open reporting of attacks and acting against foreign hackers such as sanctions or travel bans (PIB, 2023).

By following these steps, India can build a strong and fast cyber defence system. As cyber threats from countries like China grow, experts agree that ongoing preparation and teamwork are the keys to national security (PIB, 2023).

**Conclusion**

Cyber warfare has become one of the most serious security challenges of the current time situation. As this report shows, China's state-sponsored cyber activities which range from global data theft to direct attacks on India's power grid and government systems. It poses a real and growing threat. These attacks are not just about stealing information, they aim to weaken India's defence, disrupt its economy, and shake public trust in digital systems.

India has made progress by creating strong institutions like CERT-In, NCIIPC, and I4C, and by improving cooperation with countries like the United States. However, these efforts must go further. The Chinese threat is not only advanced but also persistent. This is the call for a unified national strategy, stronger laws, better protection of critical infrastructure, and more investment in cyber skills and innovation.

In today's world, cyber security is national security, and India must act decisively and quickly not just to defend its networks, but also to lead by example. India needs to Build a secure, resilient, and forward-looking cyber ecosystem. this is not an option for India anymore it is a necessity for protecting India's sovereignty, economy, and democratic future in the digital age.

## References

CBS News. (2020, June 29). *India bans 59 Chinese apps including TikTok and WeChat.* https://www.cbsnews.com/news/india-bans-tiktok-other-china-made-apps-as-border-dispute-drags-on-today-2020-06-30/

CyberScoop. (2022). *Chinese hacking groups mimicked Indian government domains during COVID-19.* https://cyberscoop.com/chinese-hackers-india-power-grid-recorded-future-red-echo/

Erickson, A. S. (2019). China's Strategic Support Force: Integrating space, cyber, and EW capabilities. *China Brief, 16*(18), 1–5. https://www.andrewerickson.com/2019/07/china-defense-white-papers-1995-2019-download-complete-set-read-highlights-here/

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817–885. https://law.yale.edu/sites/default/files/documents/pdf/cglc/LawOfCyberAttack.pdf

Indian Express. (2021). *Panel reviews Mumbai blackout amid cyberattack concerns.* https://indianexpress.com/article/india/mumbai-blackout-no-cyber-attack-but-human-error-singh-7211789/

Mandiant. (2013). *APT1: Exposing one of China's cyber espionage units.* https://services.google.com/fh/files/misc/mandiant-apt1-report.pdf

Microsoft. (2021, March 2). *HAFNIUM targeting Exchange Servers with 0-day exploits.* https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Merriam-Webster. (n.d.). *Cyberspace.* In *Merriam-Webster.com dictionary.* https://www.merriam-webster.com/dictionary/cyberspace

National Institute of Standards and Technology. (n.d.). *Cyberspace definition.* https://www.nist.gov/

North East Herald. (2025). *India and U.S. sign cybersecurity cooperation agreement.* https://neherald.com/national/india-usa-sign-mou-to-enhance-cooperationin-cybercrime-investigations

Press Information Bureau. (2023). *Bharat NCX cyber drill: Enhancing India's cyber readiness.* Government of India. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1970225

Recorded Future. (2021). *China-linked RedEcho targets Indian power sector amid border tensions.* https://www.recordedfuture.com/research/redecho-targeting-indian-power-sector

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1– 2), 4–37. https://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age.* Crown Publishing.

Segal, A. (2020). *China's vision for cyber sovereignty.* Council on Foreign Relations. https://www.cfr.org/expert/adam-segal?tab=blogs&page=12

Small Wars Journal. (2013). *China's strategic approach to cyber warfare.* https://books.google.co.in/books?hl=en&lr=&id=x2Y2DgAAQBAJ&oi=fnd&pg=PR5&dq=Small+Wars+Journal.+(2013).+China%27s+strategic+approach+to+cyber+warfare&ots=6ltYuQQhhw&sig=KVIb3GinTTmsl91z7stlv48-sic#v=onepage&q&f=false

Stockholm International Peace Research Institute. (2021). *China's growing role in cyber warfare: Trends and doctrine.* https://www.sipri.org/sites/default/files/2022-12/2212_cyber_postures_0.pdf

U.S. Department of Justice. (2014). *U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage.* https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

U.S. Department of Justice. (2020). *Four Chinese military hackers charged in Equifax breach.* https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer- fraud-economic-espionage-and-wire-fraud-hacking

World Intellectual Property Organization. (2022). *World Intellectual Property Report 2022: The direction of innovation.* https://www.wipo.int/en/web/world-ip-report/2022/index

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon.* Crown Publishing.