The Hague Centre
for Strategic Studies

Defending the Digital Domain: The Effort to Build a Cyber Resilient India

Adam Meszaros, Alessandra Barrow, Kamalaeswari Raghu, Hana Masood, Konstantijn Rondhuis, Siddhardha Kollabathini, and Dr. Praveen Naidu Vummadisetty, Michel Rademaker, Márk Bulejsza, Dr. Sanjeevakumar M. Hatture, Nathan Lokhorst, Anna Sophie den Ouden
September 2024

Defending the Digital Domain: The Effort to Build a Cyber Resilient India

2023 Edition – Updated Version

Authors:

2022: Adam Meszaros, Alessandra Barrow, Kamalaeswari Raghu, Hana Masood, Konstantijn Rondhuis, Siddhardha Kollabathini, and Dr. Praveen Naidu Vummadisetty, Michel Rademaker
2023: Márk Bulejsza, Dr. Sanjeevakumar M. Hatture, Nathan Lokhorst, Anna Sophie den Ouden

Cover photo:
Canva

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl

Table of Contents

List of abbreviations

- **5G** – 5th Generation Mobile Network
- **AI** – Artificial Intelligence
- **AIIMS** – All India Institute for Medical Sciences
- **AR/VR** – Augmented Reality/Virtual Reality
- **CERT-In** – Indian Computer Emergency Response Team
- **DCR** – Declared Capabilities Rating
- **DCyA** – Defence Cyber Agency
- **DI** – Digital India
- **DLT** – Distributed Ledger Technology
- **DSCI** – Data Security Council of India
- **G20** – The Group of Twenty
- **GDPR** – General Data protection Regulation
- **HPC** – High Performance Computing
- **I4C** – India Cyber Crime Coordination Centre
- **ICT** – Information and Communication Technology
- **IISS** – International Institute for Strategic Studies
- **IoT** – Internet of Things
- **IT Act** – The Information Technology Act, 2000
- **IT Rules** – The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
- **MeitY** – Ministry of Electronics and Information Technology
- **ML** – Machine Learning
- **NCIIPC** – National Critical Information Infrastructure Protection Centre
- **NCRG** – National Cyber Resilience Game
- **NCSS** – National Cyber Security Strategy
- **NSCP** – National Cyber Security Policy - 2013
- **PCR** – Perceived Capabilities Rating
- **PDPB** – Digital Personal Data Protection Bill, 2022
- **PLA** – People's Liberation Army
- **PMO** – Prime Minister's Office, Government of India
- **SDI** – Serial Digital Interface
- **UAV** – Unmanned Aerial Vehicle
- **UNCITRAL** – United Nations Commission on International Trade Law

Sector-specific terms

Advanced Persistent Threat – APTs are highly organised and (state-)funded adversaries that tend to persist over time. They engage in sophisticated and coordinated cyber-attacks, relying on detailed preparation, study of the target, and the employment of considerable resources.[1]

Botnets – Short for "robot network". A botnet is a network of computers infected by malware controlled by a single party. The attacker is able to command every computer on its network to coordinate cybercrime in unison.[2]

Cyber- / Digital hygiene – The term(s) denote the set of practices undertaken by users and organisations with the intention to safeguard and improve the security of data and the online environment. Cyber hygiene is aimed at halting internal deterioration and defending against external threats alike.[3]

Cybersecurity / Cyber resilience – The term(s) denote the practices and surrounding theory and discipline of protecting networks, devices, and data from illegitimate access, or utilisation to criminal ends. Confidentiality, integrity, and information availability are often framed as core tenets of cybersecurity.[4]

E-governance – The utilisation of new information and communication technologies (ICTs) with the intention to outsource government and public administration. E-governance typically streamlines bureaucracy and facilitates ICT frameworks, which enable citizens to interact with their government in their preferred ways as well as governments to reach out to their populations with more ease.[5]

Proxies – A proxy may be either a hardware or software server. Its intermediary role consists of sitting between the website or server and end user. Proxies may serve the purposes of privacy, efficiency, or security.[6]

Ransomware – Refers to a type of malware that holds the target's data hostage (i.e. for ransom) or prevents user access to files or data by the target. Payment is usually expected from the target, in order to regain access to and control over the targeted data or files.[7]

---

[1] Information Technology Laboratory Computer Security Division, "CSRC Topic: Advanced Persistent Threats | CSRC," CSRC | NIST, February 25, 2020, https://csrc.nist.gov/Topics/Security-and-Privacy/risk-management/threats/advanced-persistent-threats.
[2] "Wat is een botnet?," accessed February 1, 2023, https://www.politie.nl/informatie/wat-is-een-botnet.html.
[3] "What Is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More," Text, Digital Guardian, accessed February 1, 2023, https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more.
[4] "What Is Cybersecurity? | CISA," accessed February 1, 2023, https://www.cisa.gov/uscert/ncas/tips/ ST04-001.
[5] "What Is E-Governance | IGI Global," accessed February 1, 2023, https://www.igi-global.com/dictionary/ cyber-capability-framework/8702.
[6] "What Is a Network Proxy? | Security Encyclopedia," accessed February 1, 2023, https://www.hypr.com/ security-encyclopedia/proxy.
[7] Stop Ransomware | CISA," accessed February 1, 2023, https://www.cisa.gov/stopransomware.

1. Background

1.1 Introduction

With a population of 1.4 billion people, India is the world's largest and most diverse democracy. As such, keeping Indian people secure within cyberspace and all other domains is of paramount importance. If India's cybersecurity is endangered, it sets an alarming precedent for the ability of cyber-related threats to undermine democratic processes, national resilience, and the e-governance of states around the world. Conversely, if the creativity and cyber expertise of the Indian people can be channelled into developing India's cybersecurity capabilities, this in turn may serve as an aspirational precedent for other states. This report is part of the Indo-Dutch Cybersecurity School 2023 (IDCSS23).[8] Its goal was to contribute to this endeavour through educational and professional lectures that were provided to both Indian and Dutch students and young professionals in the field of cybersecurity.

Beyond the immediate context of healthy democratic discourse, cybersecurity has vast implications across all other fields of national resilience. India is currently undertaking efforts to digitise its economy and infrastructure. Initiatives such as Digital India (DI) aspire to link all Indian citizens to the cyber domain. Consequently, the number of users to be safeguarded by the securitisation of the cyber domain is rapidly rising. To become an economically developed, digital nation, India must also adopt a holistic approach to tackle the challenges to its cybersecurity. For instance, regarding India's geopolitical strategic posture, the cyber domain provides a large surface area for malicious foreign actors to attack India.

The urgency to boost India's resilience in the cyber domain is increasing. The sobering return of great power competition to the forefront of international relations discourse exacerbates the threats posed by revisionist powers such as Russia and China in the cyber domain. Cyberspace has become an arena for unwelcoming foreign influence on democratic processes and social discourse in liberal democracies. 'Big Data' companies and their corresponding social media platforms now serve as drivers and forums of social and political discourse in modern democracies. Social media platforms' allocation of users into consumer avatars based on their online footprints is often exploited by companies themselves and bad-faith domestic and foreign actors who seek to radicalise online discourse, thereby deepening communities' sense of disillusionment and alienation. The Cambridge Analytica controversy around the Brexit referendum, or the role of Russia-adjacent social media accounts for the rising prominence of populism in liberal democracies, both of which illustrate the magnitude of potential dangers in cyberspace.

Conversely, in the private sphere, individuals and companies face an ever-increasing threat of ransomware attacks, adding up to increasing financial damage each year. To make matters worse, a significant proportion of cyber-attacks go unreported, thereby preventing authorities from gaining comprehensive oversight on the security of the cyber sphere. Individual privacy has never been more important. Notions such as the right to be forgotten and net neutrality are important priorities on

---

[8] HCSS, "The Indo-Dutch Cyber Security School", accessed June 06, 2024.https://hcss.nl/indo-dutch-cyber-security-school/#:~:text=HCSS%20is%20proud%20to%20announce,October%20to%2010th%20of%20November.

legislators' agendas. Innovations in quantum computing and developments in artificial intelligence (AI) have furthered the potential to enhance the effectiveness of ethically questionable practices. For instance, quantum computers may undermine the security of the encryption infrastructure, which is meant to protect user privacy.[9] Therefore, in liberal democracies, no large-scale implementation of quantum computers shall take place until the corresponding quantum encryption practices are available. Revisionist powers, particularly China, have no such commitment to privacy, setting a worrying precedent in social engineering. AI, in turn, may enhance both the Chinese social credit system's effectiveness and private corporations' questionable handling of users' data. [10]

All the above risk areas have the potential to enable India's economic and socio-political growth, as well as to undermine these processes. To secure a safe and innovative society for the Indian people, cybersecurity must be maintained as a top priority. For example, transitioning from an agriculture- and production-based economy to a service-based economy requires a secure set of financial institutions along with their corresponding financial infrastructure. The role of an active state apparatus in the Digital Age relies heavily on the nation's cyber infrastructure. Large areas of healthcare, education, welfare, and administration infrastructure are outsourced to cyberspace. Consequently, should the cybersecurity of these domains be endangered, the state's ability to respond to crises, conduct developmental schemes, or simply deliver government services is undermined. Our report enumerates examples from India of the above risk areas and draws attention to the existing frameworks already in place, which could in turn serve as promising platforms for mitigating cybersecurity threats.

Policy makers' responses to these challenges are comparably significant, albeit arguably incomplete. The European Union's recent adoption of the General Data Protection Regulation (GDPR) aims to mitigate threats to citizens' privacy and data security within the cyber landscape.[11] Similar legislation in the form of the Digital Personal Data Protection Bill (PDPB) has been set to follow in India.[12]

Having organised the IDCSS for the sixth consecutive year in October and November 2023, this HCSS paper is a comprehensive assessment of the cyber landscape in India, drawing on open source and desk research, as well as on the results of an HCSS National Cyber Resilience Game (NCRG) executed by the students at the school. The game is a gamified analytical tool that is suited to the context of cybersecurity in India. The aim was to gain insight into players' views on how India's cyber resilience can be enhanced. Cybersecurity is the key cornerstone of a resilient national strategic posture in the digital age. To safeguard 1.4 billion Indian people's data, privacy, democratic processes, and enterprises in the cyber domain are therefore of paramount urgency. Therefore, the results of the NCRG offer valuable lessons regarding strategically crucial areas.

[9] National Cyber Security Centre, "Quantum-safe cryptography", NCSC: Whitepaper. 2020. Accessed February 10 2023. https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography.

[10] Kendra Schaefer, "China's Corporate Social Credit System: Context, Competition, Technology and Geopolitics". U.S.-China Economic and Security Review Commission: Trivium China. 2020. Accessed February 10, 2023. https://www.uscc.gov/research/chinas-corporate-social-credit-system-context-competition-technology-and-geopolitics

[11] Data Protection in the EU". European Commission. Accessed February 10, 2023. https://commission.europa. eu/law/law-topic/data-protection/data-protection-eu_en.

[12] The Digital Personal Data Protection Bill, Ministry of Electronics and Information Technology, Government of India (2022). https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022.

1.2 Research aim

This paper aims to achieve three objectives: 1) to present an overview of the current cyber threats and the overall cyber environment in India; 2) to discuss the strategic and legislative frameworks related to cybersecurity in India; and 3) to provide an analysis of India's cyber resilience by combining the results of the National Cyber Resilience Game (NCRG) and qualitative research findings, and offering lessons and recommendations based on recent developments in cyberspace.

1.3 Readers' guide

The paper is structured to align with its stated objectives; therefore, Chapter 2 offers a comprehensive overview of the cyber threats facing India and the overall cyber environment in the country. Chapter 3 summarises India's cyber-strategy, policies, and legislation. Chapter 4 focuses on assessing India's cyber capabilities in both the defensive and offensive areas. Chapter 5 examines the findings of the National Cyber Resilience Game (NCRG) to gain insights into the perceptions of cybersecurity among young Indian professionals. Finally, Chapter 6 presents observations and recommendations that can be useful to both Indian and international policymakers.

2. India's position in cyberspace

2.1 Cyber threats in India: incidents and actors

India is facing cyber threats at an already major and still growing scale. In December 2022, *Tribune* reported that cyber-attacks in India have tripled over the past three years. It is elaborated that the Indian Computer Emergency Response Team (CERT-In) reported handling as many as 1,402,809 cyber-attacks in 2021 alone.[13] With nearly 700,000 cyber-attacks having been reported by CERT-In by June, 2022, *The Print* went on to label 2022 as "its worst year of cyberattacks", implying that 2023 would likely showcase a further increase.[14] This worrying trend has considerable implications for various strategic sectors. Worse still, while CERT-In's capacity to respond to cyber-attacks is considerable, it lags behind the estimated 18 million instances of cyber-attacks in the first quarter of 2022 alone.[15] According to Google's Vice President-Engineering for Privacy, Safety and Security, Royal Hansen this amounted to around 200,000 cyber-attacks every single day during the same period.[16]

NPR reported last December that "[c]yberattacks on hospitals thwart[ed] India's push to digitize health care".[17] In November, Chinese and Hong Kong-based cyber criminals held data of the All India Institute of Medical Science (AIIMS) for ransom, causing considerable disruptions to the institution's operating capacity. CERT-In diagnosed that five servers of the medical institution were compromised, with nearly 1.3 TB of data having been affected by the attacks.[18] This came at a time when India was undergoing large-scale digitisation efforts, with the federal government's aspiration to issue a digital health ID for every Indian citizen. Cybercrime poses comparable disruptions to other sectors of public administration in India, with e-Sign, e-Governance, and other services already having entered a developed stage of their implementation.

Government agencies are not safe from cyberattacks. *Mint* reported based on a study of the cybersecurity firm CloudSek that 2022 saw a 95 percent year-on-year increase in cyber-attacks on government agencies.[19] This increase cemented India as the single most-targeted country in terms of cyber-attacks on government agencies. CloudSek also found that India, the US, Indonesia, and China together accounted for 45 percent of all cyber-attacks targeted at governments globally in

13 Tribune News Service, "Cyber Attacks in India Triple in Last Three Years, but Security Funds Underutilised," Tribune India News Service, accessed January 23, 2023, https://www.tribuneindia.com/news/nation/ cyber-attacks-in-india-triple-in-last-three-years-but-security-funds-underutilised-457692.

14 Anupriya Chatterjee, "India's Had Its Worst Year of Cyberattacks, but 2023 Will See Govt & Firms Ramp up Defences," The Print, December 30, 2022, https://theprint.in/india/indias-had-its-worst-year-of-cyberattacks-but-2023-will-see-govt-firms-ramp-up-defences/1286441/.

15 "India Saw 18 Million Cyber Attacks in First Quarter of 2022: Google's Royal Hansen," Money Control, accessed January 23, 2023, https://www.moneycontrol.com/news/business/india-saw-18-million-cyber-attacks-in-first-quarter-of-2022-google-executive-royal-hansen-9084911.html.

16 Ibid.

17 Raksha Kumar, "Cyberattacks on Hospitals Thwart India's Push to Digitize Health Care," NPR, December 17, 2022, sec. Health, https://www.npr.org/sections/goatsandsoda/2022/12/17/1143396605/cyberattacks-on-hospitals-thwart-indias-push-to-digitize-health-care.

18 Outlook India, "Recent Cyber Attacks With Alleged Chinese Involvement That Targeted India's Critical Infrastructure," https://www.outlookindia.com/, December 2, 2022, https://www.outlookindia.com/national/ recent-cyber-attacks-with-alleged-chinese-involvement-that-targeted-india-s-critical-infrastructure-news-24189.

19 Abhijit Ahaskar, "India Saw the Highest Number of Cyberattacks on Govt Agencies in 2022: Report," The Mint, December 30, 2022, https://www.livemint.com/technology/tech-news/india-saw-the-highest-number-of-cyberattacks-on-govt-agencies-in-2022-report-11672389099189.html.

2022.[20] Meanwhile, the share of government-targeted cybercrime aimed at China fell to 4.5 percent in 2022, from 13.1 percent in 2021.[21] The AI-focused cyber threat prediction firm also established that, in addition to foreign powers, grassroots hacktivism also posed a considerable threat to India, particularly the Malaysia-based group Dragon Force and the Khalifa Cyber Crew. Both organisations proclaim an agenda of targeting India's cyber landscape, citing discrimination against Muslim communities in the country. Overall, hacktivism groups were found by CloudSek to be responsible for 9 percent, while ransomware groups were responsible for 6 percent of cyber-attacks perpetrated on government agencies.[22] While hard to confirm, this indicates a relatively higher degree of engagement in cyber-attacks by government-adjacent organisations both globally and in terms of cyber-attacks perpetrated against India specifically.

Banks in India are not immune from cyber-attacks, pointing to cybercrime endangering the financial infrastructure of the country as well. As the India Defence Review (IDR) put it earlier in January, "The more India is moving to reap the benefit of digitalization, the more its economy comprising all critical infrastructures, financial institutions are susceptible to cyber-attacks that are being launched constantly by India's adversaries lying inside and outside of India." The IDR goes on to enumerate that between June 2018 and March 2022 248 data breaches were successfully carried out against various Indian banks, 41 of which were against banks in the public sector.[23]

The cyber threat level faced by India is considerable and appears to continue growing, as illustrated in the above section. In addition, it has been shown that a proportionately significant amount of malicious cyber activity against India is targeted at the public sector. At a time when initiatives such as the Digital India (DI) flagship programme aim to extend the cyber sphere to all 1.4 billion Indian citizens, such threats pose considerable obstacles to the DI's vision to empower citizens to become digitally literate, as well as secure online.[24] For example, as *The Week* illustrates: "In February 2021, [...] SITA, the Geneva-based air transport data giant which serves more than 90 per cent of the world's airlines, informed Air India that hackers stole the personal data of 4.5 million passengers."[25] The very infrastructure of India faces the risk of disruption by grassroots cyber organisations pursuing political agendas, as well as by foreign powers (chiefly, China) that seek to expand their rivalry with India into the cyber domain. In short, there is much concern about the cybersecurity of Indian people. The following section provides a landscape of the various institutional outlets India has dedicated to addressing the cyber threat faced by the country.

2.2 Hacktivism: Threats by non-state initiators

In the era defined by the Internet, information hacktivism is an emerging threat that cannot be ignored. Hacktivism is loosely defined as politically, socially, or religiously motivated hacking and

---

[20] Hansika Saxena and Aastha Mittal, "Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022" (CloudSek, n.d.), 1.

[21] Saxena and Mittal, "Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022."

[22] Ahaskar, "India Saw the Highest Number of Cyberattacks on Govt Agencies in 2022."

[23] "Digital India under Cyber Attack!!," Indian Defence Review (blog), accessed January 24, 2023, http://www.indiandefencereview.com/spotlights/digital-india-under-cyber-attack/.

[24] Government of India, "Digital India," accessed January 25, 2023, https://digitalindia.gov.in/.

[25] "Inside Story of Cyber Attacks on India's Banks, Airlines, Railways… and the Fightback," The Week, accessed January 23, 2023, https://www.theweek.in/theweek/cover/2022/01/06/inside-story-of-cyber-attacks-onindia-banks-airlines-railways-and-the-fightback.html.

activism carried out on the Internet to perform cyberattacks.[26] Websites are defaced by hacktivists daily for various reasons. For example, they can spread messages or disrupt vulnerable networks. According to some scholars, hacktivism and website defacement are increasing threats in India.[27] This phenomenon is partly due to geopolitical tensions between India and Pakistan. India is focusing on enhancing its cyber offensive capabilities by collaborating more closely with the US and Israel as a result of events that have occurred in recent years.[28]

State-sponsored hacktivists tend to deface vulnerable websites, regardless of their content. Hacktivists also target government websites, aiming to make direct statements to the government.[29] One prominent theme is government accountability and transparency.[30] However, various groups have targeted government websites to raise environmental awareness. This also means that hacktivist groups targeted companies and organisations involved in environmentally harmful actions, such as pollution.

Moreover, hacktivism in India has addressed social issues, with activists leveraging digital platforms to advocate marginalised communities and address issues such as caste discrimination, gender inequality, and LGBTQ+ rights. Hacktivist actions include defacement of websites, data leaks, and other cyber operations aimed at challenging social norms and promoting inclusivity.

Since early 2020, web-based propaganda content targeting India has also emerged. This is the result of the government's decision to downgrade from 4G to 2G across the country.[31] The government stated that this was a necessary move to slow down online propaganda. However, news outlets argue that this decision worsened propaganda and did not slow it down.

As the landscape of hacktivism in India continues to evolve, it raises important questions regarding the balance between digital activism, ethical considerations, and broader implications for democracy and civil society in the country. The interplay between technology, activism, and governance remains a dynamic and complex aspect of India's sociopolitical fabric.

In India, certain hacktivist groups concentrated on using technology to fight legal fights. These advocates used their legal expertise to contest perceived injustices and supported whistleblowers in court cases as well as to promote digital rights. Hacktivism in India has raised significant concerns, but it has not been without difficulties and disputes. The indistinct boundaries between cybercrime

---

[26] SecAlliance, "The Changing Landscape of Hacktivism," April 21, 2022, accessed via https://www.secalliance.com/blog/the-changing-landscape-of-hacktivism.
[27] Marco Romagna and Niek Jan van den Hout, "Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats," conference paper presented at the 27th Virus Bulletin International Conference, October 2017, accessed via https://www.researchgate.net/profile/Niek-Jan-Van-Den-Hout/publication/320330579_Hacktivism_and_Website_Defacement_Motivations_Capabilities_and_Potential_Threats/links/5c1bc034a6fdccfc705cd71c/Hacktivism-and-Website-Defacement-Motivations-Capabilities-and-Potential-Threats.pdf.
[28] Summar Iqbal Babar, Muhammad Nadeem Mirza, and Irfan Hasnain Qaisrani, "Evaluating the Nature of Cyber Warfare between Pakistan and India," *Webology* 18, no. 6 (2021): 6973-6985, ⟨halshs-03788162⟩.
[29] Romagna and van den Hout, "Hacktivism and Website Defacement".
[30] L. Ireland, "We are all (not) Anonymous: Individual- and country-level correlates of support for and opposition to hacktivism," *New Media & Society* 0, no. 0 (2022), https://doi.org/10.1177/14614448221122252.
[31] Alik Naha, "Emerging Cyber Security Threats: India's Concerns and Options," *International Journal of Politics and Security* (IJPS) 4, no. 1 (2022): 170-200, https://doi.org/10.53451/ijps.996755; "NIC-CERT GOVT OF INDIA," accessed January 25, 2023, https://nic-cert.nic.in/.

and activism can lead to ethical dilemmas. Furthermore, hacktivist activities may have unforeseen repercussions that harm innocent people, or inadvertently harm networks and services.

2.3 India's national cyber landscape

Having illustrated the cyber threats faced by India, it is also important to enumerate the various initiatives and bodies in place to mitigate these threats. The digital world is changing rapidly. Therefore, the need for cybersecurity has never been more pressing. The Indian government has made cybersecurity one of its top priorities, with a vision to make India a "cyber-smart" nation by 2023. Steps are being taken by the government to ensure that businesses are prepared for cyber-related changes by enforcing a comprehensive plan called the National Cyber Security Strategy (NCSS).[32] The is designed to help businesses and citizens alike avoid becoming victims of cybercrime and prevent vicious attacks on their connections, including attacks from countries seeking to steal intellectual property or other sensitive information.

The NCSS has four central objectives:

1) Improving India's cyber security infrastructure

2) Supporting research on protecting against cyber threats

3) Encouraging the development of operational capabilities; and

4) Promoting awareness of cybersecurity issues among citizens

The Ministry of Electronics and Information Technology (MeitY)[33] is the nodal government body responsible for all aspects of digitalisation and cybersecurity in India, as well as for addressing issues revolving around the wider context of technological innovation (see Figure 1). It was formed as one of the Union ministries on 1 January 2017 under the MeitY designation. MeitY develops policies for technology and telecommunications, as well as for the protection of data security, privacy, and intellectual property rights.

---

[32] National Cyber Security Strategy," Drishti IAS, accessed January 25, 2023, https://www.drishtiias.com/ daily-updates/daily-news-analysis/national-cyber-security-strategy-1.

[33] "MeitY Organisations | Ministry of Electronics and Information Technology, Government of India," accessed January 25, 2023, https://www.meity.gov.in/content/meity-organisations.

India's institutional cyber landscape
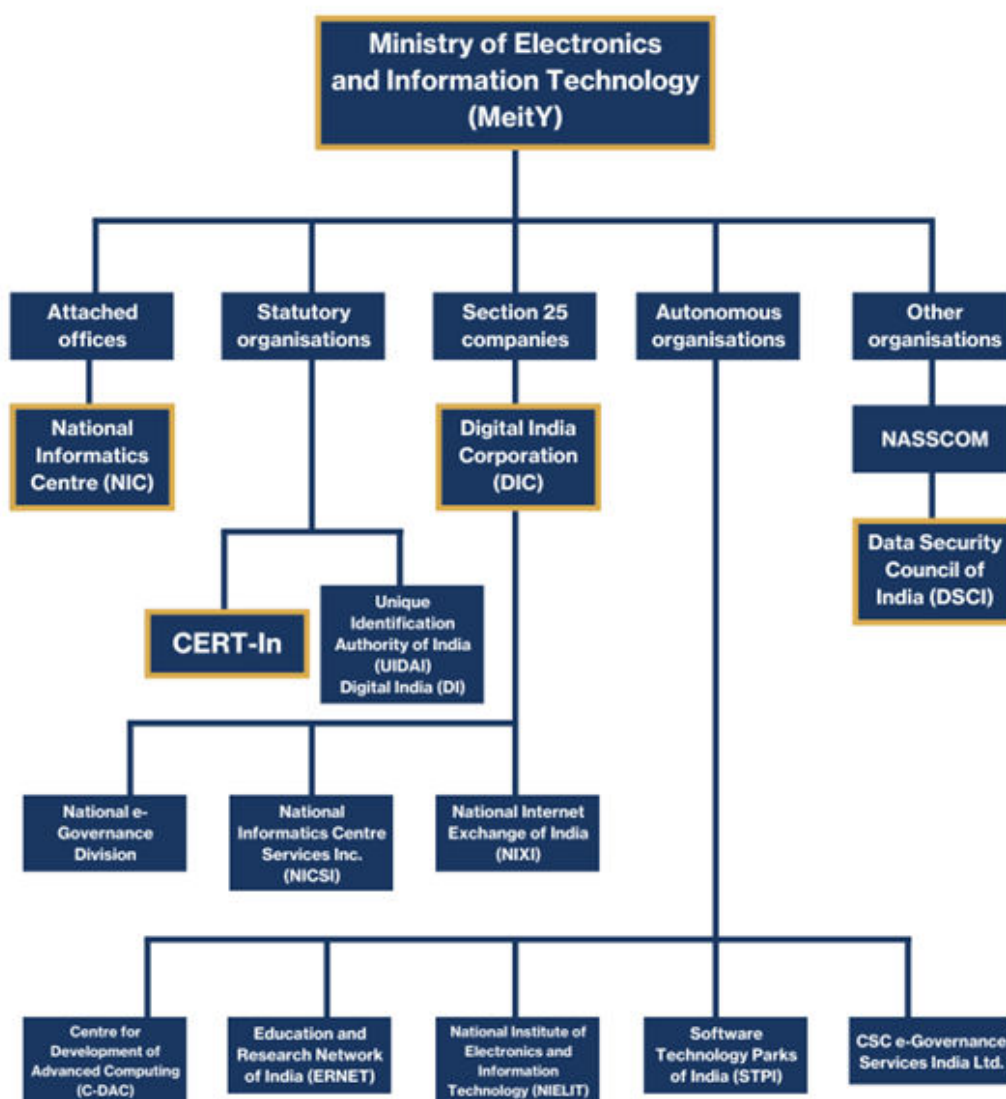
Figure 1: India's institutional cyber landscape.

The Government of India launched several initiatives under the MeitY umbrella. There are various schemes and services to improve the cybersecurity landscape in the country.[34] These initiatives aim to protect critical infrastructure and other key assets from cyber-attacks, combat cybercrime, and promote digital literacy and access to digital services. The most significant ones are listed below:

- **National Cyber Coordination Centre (NCCC):** for monitoring and responding to cyber threats
- **National Critical Information Infrastructure Protection Centre (NCIIPC)**: for protecting critical infrastructure from cyber attacks
- **Cyber Security for MSMEs scheme:** provides training and raises awareness of threats to small and medium-sized enterprises (SMEs) and their employees

---

- **Indian Computer Emergency Response Team (CERT-In)**: CERT-In[35] is India's national nodal agency for responding to cyber security threats
- **National Cyber Safety and Security Standards (NCSSS)**: for developing and implementing standards for cyber security in India
- **Digital India (DI):** for transforming India into a digitally empowered society and knowledge economy. It includes a range of initiatives to improve access to digital services and to promote digital literacy
- **India Cyber Crime Coordination Centre (I4C):** for coordinating, integrating, and strengthening the fight against cybercrime in India[36]

Indian Cyber Crime Coordination Centre (I4C)

National Cybercrime Threat Analytics Unit (TAU)	
National Cybercrime Reporting portal	
Platform for Joint Cybercrime Investigation Team	
National Cybercrime Forensic Laboratory (NCFL) Ecosystem	
National Cybercrime Training Centre	
Cybercrime Ecosystem Management Unit	
National Cyber Crime Research and Innovation Centre	

Table 1: Indian Cyber Crime Coordination Centre (I4C).

[35] "NIC-CERT GOVT OF INDIA," accessed January 25, 2023, https://nic-cert.nic.in/.
[36] "Indian Cyber Crime Coordination Centre (I4C) – A 7-Pronged Scheme to Fight Cyber Crime," accessed January 25, 2023, https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579184.

In the wake of the recent rise in cybercrime, India has launched a new initiative to combat this issue. **India Cyber Crime Coordination Centre (I4C)** is a national effort to combat cybercrime and its associated threats (see Table 1).[37] The I4C is a multi-agency centre that coordinates with other government departments and law enforcement agencies to identify and respond to new threats, as well as to help prevent them from happening in the first place.

The **Digital India (DI)** program is the flagship initiative launched by the Government of India in 2015 with the goal of transforming India into a digitally empowered society and knowledge economy.[38] The framework aims to ensure that government services are made available to citizens electronically and that citizens can access these services through a computer or mobile device. The DI program includes several subsidiary initiatives aimed at improving digital infrastructure, promoting e-governance, and increasing digital literacy. Some of the major initiatives that help citizens of India be digitally literate and more cyber-aware include the following.

- **BharatNet:** This initiative aims to connect all Gram Panchayats (village councils) in a country with high-speed internet through a fibre-optic network.
- **Digital Locker:** This initiative provides citizens with a digital locker to store important documents and certificates electronically.
- **e-Sign:** This initiative allows citizens to sign documents electronically, making it easier for them to access government services.
- **e-Governance:** The program aims to increase the use of technology in government processes to improve transparency, efficiency, and accountability.
- **Digital India Portal:** A one stop solution for all government services
- **Skill India:** The program aims to train and upskill citizens to meet the demands of the digital economy.

The DI programme has made significant progress in areas such as e-governance, digital infrastructure, and digital literacy. The Digital India budget for 2023 has been made public, and it shows that cybersecurity projects will be one of the biggest parts of the plan.[39] In its 2023 budget, DIC allocated $300 million for cybersecurity projects in 2022-2023 with an emphasis on training and education; $500 million for research into artificial intelligence and machine learning, $300 million for creation of a national data centre; and $200 million for improving internet connectivity in rural areas. The Smart City Project of Digital India benefited more than 100 cities throughout the country from to 2019-23. The number of people using 'Digi Locker' in India is expected to reach 1.2 billion by 2023.[40]

However, there are still challenges to be addressed, such as ensuring that all citizens have access to digital services and addressing the issues of data privacy and security. Even after several programs, India continues to face a significant number of cyber threats, especially following the COVID-19

[37] "Details about Indian Cybercrime Coordination Centre (I4C) Scheme | Ministry of Home Affairs," accessed January 25, 2023, https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/ Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

[38] Government of India, "Digital India," accessed January 24, 2023, https://digitalindia.gov.in/.

[39] All Statements of Budget Estimates, Notes on Demands for Grants 2022-2023 -Ministry of Electronics and Information Technology," accessed January 25, 2023, https://www.indiabudget.gov.in/.

[40] "Digital India | IBEF," India Brand Equity Foundation, accessed January 25, 2023, https://www.ibef.org/ government-schemes/digital-india.

pandemic.[41] The Indian government also recognises the need for a strong legal framework to tackle cybercrime. The Information Technology (IT) Act was enacted by the government in 2000, providing avenues for a range of legal measures to tackle cybercrime and protect personal data.

Cybersecurity is also one of the key concerns of the G20, given that increasing reliance on technology and the internet has made the world more vulnerable to cyber-attacks. India is presently holding the presidency of the G20 from 1 December 2022 to 30 November, 2023.[42] India is actively participating in the G20's efforts to improve global cybersecurity. To accomplish its goals, the G20 has created a few committees that address specific issues within their jurisdiction. These committees include one dedicated specifically to online safety issues (the "Online Safety Working Group").[43] This working group brings together experts from around the world so that they can develop strategies for protecting people against online threats like cyberbullying or cyberstalking; sharing best practices for dealing with these problems and encouraging cooperation between government agencies.[44]

Cyber resilience is a key component of any information security strategy. In India, the still developing levels of digital literacy among the population can make it difficult to address this issue from a policy perspective. The first step in addressing cyber resilience is improving awareness and education, for which the Indian government has implemented a Stay Safe Online Campaign.[45] This process can be enhanced through training programs that target specific groups. Examples include women or youth engagement, which is conducted by an information security education and awareness portal aimed at cyber capacity building through Cytrain. Similar initiatives are targeted at officers from States and Union Territories, as well as from central police organisations or the Central Armed Police Force itself. The next step is to encourage businesses to take responsibility for their own cyber defences by providing them with guidelines on how to protect themselves against threats.[46] India still appears to be taking these first steps; however, several key initiatives already show great promise. Most notably, Cyber Swachhta Kendra is a public-private partnership between the government and private sector to promote cyber hygiene. It also provides information and tools for securing systems across sectors. This centre is being operated by CERT-In under Section 70B of the Information Technology Act of 2000. Cyber Swachhta Kendra is addressed more in-depth in the following chapter.

Finally, there is still a need for investments in infrastructure to increase connectivity between organisations and access to resources, such as cloud storage. This would allow both companies and individuals to share information in real time without worrying about whether they are connecting over insecure networks or using outdated technology that cannot keep up with modern threats.

---

[41] Vishal Jain, "The Challenge and Future of Cybersecurity in 2023," The Times of India, accessed January 25, 2023, https://timesofindia.indiatimes.com/blogs/voices/the-challenge-and-future-of-cybersecurity-in-2023/.
[42] Urvin Mistry, "G- 20 India's Presidency and Cybersecurity Enterprises," CyberPeace Foundation (blog), January 17, 2023, https://www.cyberpeace.org/g-20-indias-presidency-and-cybersecurity-enterprises/.
[43] "Shri Ashwini Vaishnaw Launches 'Stay Safe Online' Campaign and 'G20 Digital Innovation Alliance' as Part of India's G20 Presidency," accessed January 25, 2023,
https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=1887114.
[44] "Ministry Of Personnel, Public Grievances and Pensions, G20 SECRETARIAT NEWSLETTER | January 2023," accessed January 25, 2023, https://darpg.gov.in/.
[45] "Stay Safe Online," SSO, accessed January 25, 2023, https://staysafeonline.in/.
[46] "India Studies in Business and Economics," Springer, accessed January 25, 2023, https://www.springer.com/series/11234.

3. Legal, strategic, and policymaking frameworks

As elaborated in the last chapter, India launched several programs and initiatives to promote digital hygiene and cyber resilience. Cyberattacks on India's critical infrastructure, such as the 2020 cyberattack on the Kudamkulam Nuclear Power Plant,[47] demonstrate that India faces a high risk of attack by its adversaries in the region. Thus, while India still has a long way to go in promoting digital literacy and capacity-building efforts, the current cyber threat landscape warrants a robust and comprehensive legal, strategic, and policy framework to detect and prevent cyberattacks and crimes in cyberspace.

In the absence of a unified, exclusive law focused on cybersecurity, India relied on the Information Technology Act of 2000 and many other sector-specific policies and regulations to regulate and promote best practices for cybersecurity. The following sections chronologically discuss the key highlights in the country's strategic, legal, and policy journey towards regulating cyberspace and enhancing national cybersecurity (see Table 2).
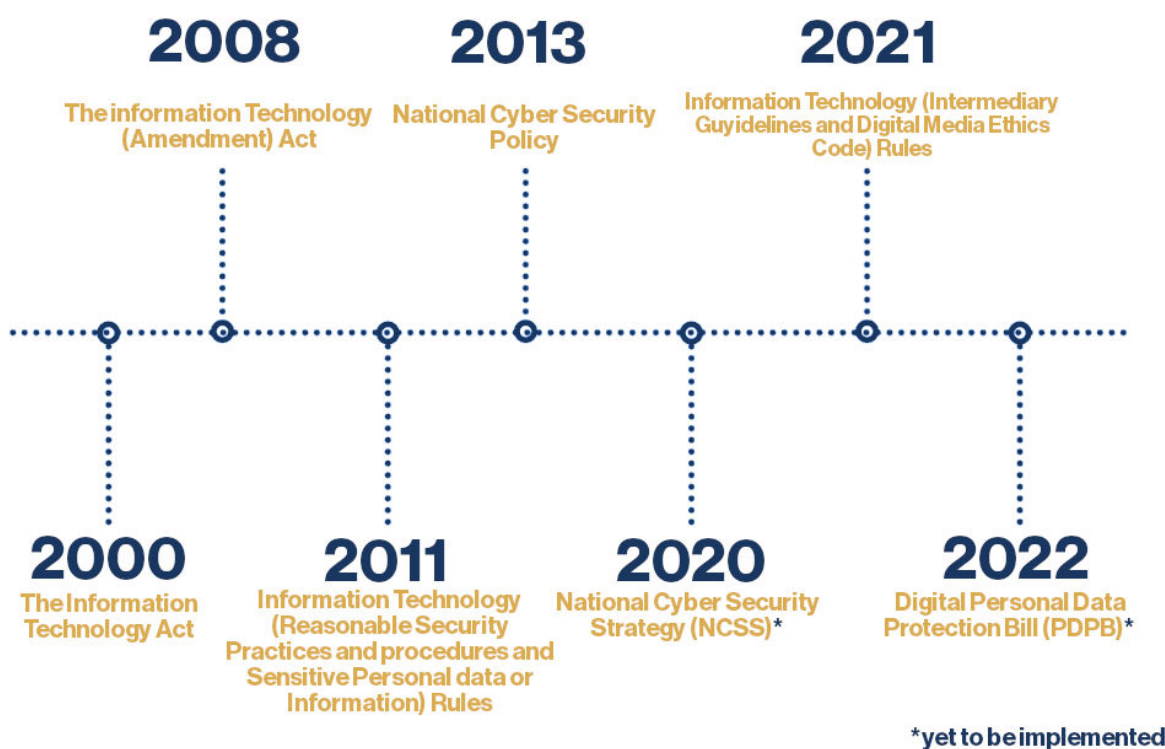

Figure 2: India's cyber legislation timeline.

---

[47] Maj Gen P K Mallick, "Cyber Attack on Kudankulam Nuclear Power Plant" (Vivekananda International Foundation, 2019), https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf.

3.1 Legal Frameworks

The foremost legal framework governing India's cyber sector is the **Information Technology Act, 2000 (IT Act).**[48] As a landmark piece of legislation drawing from the 1996 United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce,[49] the primary objectives of the IT Act were to legally recognize and regulate e-commerce processes, facilitate, and promote e-governance, and boost the IT industry. Despite the absence of the term "cybercrime" from the legislation, Chapters IX-XIIA of the IT Act provide details addressing computer-related offences and their respective procedures and punishments. While Chapter IX deals with penalties, compensation, and adjudication,[50] Chapter X elaborates on the procedures, powers, duties, and composition of an Appellate Tribunal to deal with disputes and settlements.[51] Chapter XI outlines all offences and their punishments,[52] while Chapters XII and XIIA specify cases in which intermediaries are exempt from liabilities,[53] as well as the procedures and powers of law enforcement to collect electronic evidence for cases.[54]

Further, Section 70B of the Act paves the way for the formation of the Indian Computer Emergency Response Team (CERT-In), a body that is a part of MeitY and, as discussed in other chapters, acts as the nodal agency for cybersecurity threat mitigation and defense. CERT-In has been instrumental at forecasting and disseminating information about cybersecurity issues and issuing advisories and whitepapers regarding the procedures and practices of, as well as (emergency) responses to cyber incidents[55]

The Information Technology (Amendment) Act, 2008,[56] brought about changes to the IT Act, which was hailed as a progressive and necessary step towards safeguarding the country's cyber infrastructure and its users. Most notably, the 2008 Amendment is credited with drastically expanding the scope of the IT Act for e-commerce and adding provisions for 1) recognizing and regulating electronic signatures and strengthening the legal recognition of electronically signed contracts;[57] 2) defining the role and liabilities of intermediaries; 3) adding sections to recognize and prescribe punishments for a host of cyber offences like cyber terrorism,[58] child pornography,[59] account manipulation, phishing and spam; and 4) tightening regulations on the monitoring, interception, and decryption of electronic records.[60]

---

[48] "The Information Technology Act, 2000," Pub. L. No. 21 (2000).

[49] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment, 1996 : With Additional Article 5 Bis as Adopted in 1998 (New York : United Nations, 1999., 1999), https://search.library.wisc.edu/catalog/999878764902121.

[50] The Information Technology Act, 2000. §43-47.

[51] The Information Technology Act, 2000. §48-64.

[52] The Information Technology Act, 2000. §65-78.

[53] The Information Technology Act, 2000. §79.

[54] The Information Technology Act, 2000. §79A.

[55] Ministry of Electronics and Information Technology, Government of India, "Indian Computer Emergency Response Team," accessed January 26, 2023, https://www.cert-in.org.in/.

[56] Ministry of Law and Justice, "The Information Technology (Amendment) Act, 2008," Pub. L. No. DL- (N)04/007/2003-09 (2009), https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihb gfGhdfgFHytyhRtMTk4NzY=.

[57] Ministry of Law and Justice. §10A.

[58] Ministry of Law and Justice. §66F.

[59] Ministry of Law and Justice. §67B.

[60] Ministry of Law and Justice. §69.

The most significant use of the 2008 Amendments to the IT Act in recent times was the Union Government's response to the deadly Indo-China border clash at Galwan Valley in 2020.[61] The Union Government enacted Section 69A of the IT Act, which gives it the "power to issue directions for blocking public access to any information via any computer source."[62]

> The following are the detailed clauses (quoted verbatim) of Section 69A of the IT Act, 2000:
>
> "Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resources.
>
> The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.
>
> The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine."

The above clauses impose comprehensive limitations on the operations of Chinese technology companies in the country, including popular services such as TikTok, CamScanner, and the UC Browser. By implementing provisions of the IT Act, India has set an adept example of how to attain an assertive strategic posture in the cyber domain to ensure national security for the contingency of interstate conflicts.[63]

However, there is room for significant improvements that have yet to be made to the IT Act in this decade, especially owing to the rapidly changing nature of the cyber landscape. For example, the IT Act needs to address crimes committed on mobile phones and include a comprehensive framework of safety checks to protect individual and institutional privacy, especially given that Section 66A penalises sending "offensive messages" on online channels but is extremely vague in how it defines such content. In 2015,[64] The Supreme Court of India struck down Section 66A of the IT Act, reiterating that citizens cannot not be prosecuted under its ambit and emphasizing the "cardinal" importance of the freedoms of thought and expression.[65] The IT Act is also direly lacking any specific definitions and safeguards to transnational cyberwar as an offence and has been criticised by some for decreasing penalties for existing listed offences.

---

[61] Nandagopal Rajan, "Explained: How Ban of TikTok and Other Chinese Apps Will Be Enforced; the Impact for Indian Users," The Indian Express, 2020, https://indianexpress.com/article/explained/india-bans-chineseapps-impact-explained-6482150/; Chauncey Jung, "India Shows the World How to Use 'Cyberspace Sovereignty' Against China," The Diplomat, 2020, https://thediplomat.com/2020/07/india-shows-the-worldhow-to-use-cyberspace-sovereignty-against-china/.

[62] The Information Technology Act, 2000. §69A.

[63] Dia Rekhi, "India Set an Important Precedent by Banning TikTok: FCC Commissioner Brendan Carr," The Economic Times, January 2, 2023, https://economictimes.indiatimes.com/tech/technology/india-has-set-animportant-precedent-in-banning-tiktok-us-official/articleshow/96666862.cms?from=mdr.

[64] The Information Technology Act, 2000. §66A.

[65] Bhadra Sinha, "Don't Try Anyone under Invalid Sec 66A of IT Act, SC Raps Centre, States; Scraps Ongoing Cases," ThePrint (blog), October 12, 2022, https://theprint.in/judiciary/dont-try-anyone-under-invalid-sec66a-of-it-act-sc-raps-centre-states-scraps-ongoing-cases/1164801/.

In 2021, MeitY also amended a secondary legislation stemming from Section 87 of the IT Act, namely the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** (hereafter, IT Rules).[66] Overriding a similar set of IT guidelines (i.e. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011), the new IT Rules expand on the due diligence requirements of intermediaries - who are entities that transmit and store user-generated data on behalf of other parties - including social media platforms, online marketplaces, search engines, and internet and telecom service providers.[67] The IT Rules require intermediaries to inform users about privacy policies, user agreements, and content restrictions and ensure that users adhere to the above. The Rules also require intermediary organisations to designate a Grievance Officer to address content violation complaints and liaise with a Grievance Appellate Committee in the Union Government.[68] Complaints regarding the removal of objectionable or prohibited content must also be addressed within 72 hours.[69] The 2021 IT Rules are necessary to ensure that intermediaries do not arbitrarily self-regulate content published on their platforms. At the same time, the Rules have been critiqued for, going beyond the powers of the parent IT Act 2000 and for failing to provide definitions of important terms in its content restriction and traceability obligations that could cause ambiguity and possibly impede on the freedom of speech and privacy of users.[70]

The most recent cybersecurity draft legislation, which has been a prominent topic of discussion, is the **Digital Personal Data Protection Bill 2022 (PDPB).**[71] The draft PDPB seeks to create a horizontal framework across sectors that establishes the rights and duties of users in conjunction with the duties and obligations of data fiduciaries to lawfully process user data. The Bill has been welcomed as an important initiative at a crucial time when India is strengthening its role as a global leader through its G20 Presidency and multiple bilateral and regional trade agreements.

A salient feature of the proposed bill is its vague approach to cross-border data transfers in the interest of its digital sovereignty. This approach was included in previous versions of the bill and received criticism from industry experts, who were concerned about the lack of data localisation measures in the draft bill. The PDPB addresses the release and transfer of sensitive personal data from Indian citizens to foreign countries via fiduciary obligations. However, in its current form, the bill does not distinguish between countries that have secure data protection frameworks and those that do not. As Sudhansu Nayak from the Observer Research Foundation notes, this is the largest

[66] Ministry of Electronics and Information Technology, Government of India, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021," Pub. L. No. G.S.R. 139(E) (2021), https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20 Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

[67] Ministry of Electronics and Information Technology, Government of India, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021," Pub. L. No. G.S.R. 139(E) (2021), https:// mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20 Ethics%20Code%29%20Rules%2C%202021%20English.pdf. §3(1).

[68] Ministry of Electronics and Information Technology, Government of India. §3(1)(a).

[69] Ministry of Electronics and Information Technology, Government of India. §3(2).

[70] "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021," PRS Legislative Research, February 25, 2021, https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021.

[71] Ministry of Electronics and Information Technology, Government of India, "The Digital Personal Data Protection Bill, 2022" (2022), https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20 Data%20Potection%20Bill%2C%202022_0.pdf.

"elephant in the room"[72] with respect to the PDPB. This provision can be beneficial and has great potential to allow large volumes of data to build sophisticated artificial intelligence and machine learning capabilities but is missing crucial safeguards and legal recourse should these partner states act irrationally or be de-notified later.

Another major amendment needed for PDPB is the definition of the term "sensitive personal data" and increased obligations from data fiduciaries to safeguard individual privacy. The lack of such safeguards in the current form of the Bill have been highlighted by organisations like the Human Rights Watch, who have critiqued the draft Bill for prioritising the enablement of "unchecked state surveillance" over the privacy of citizens, particularly children.[73]

3.2 Strategic and policy frameworks

On the policy front, India made significant moves with the introduction of the country's first-ever **National Cyber Security Policy (NCSP) in 2013**.[74] Touted as an "evolving task" catering to the entire spectrum of ICT providers and users, the NSCP was created as an "umbrella framework" to guide all sectors—government and non-government entities and small, medium, and large enterprises (SMEs)—with designing relevant and appropriate internal cybersecurity strategies.[75] The policy outlines effective strategies to protect networks, information, and information systems. For example, test infrastructure, malware monitoring and cleaning facilities, and the introduction of a 24/7 National Critical Information Infrastructure Protection Centre (NCIIPC) to tackle cybersecurity threats in strategic areas like space, nuclear, and air control.[76] It also lays emphasis on fiscally incentivizing businesses to adopt best practices in cyber resilience infrastructure building, and on developing indigenous technology solutions by supporting the creation of a trained workforce of around 500,000 cybersecurity professionals.[77]

The NSCP aimed to reach its objectives using the following strategies: a) creating a secure cyber ecosystem; b) creating an assurance framework; c) encouraging open standards; d) strengthening the regulatory framework; e) creating mechanisms for security threat early warning, vulnerability management and response to security threats; f) securing e-governance services; g) protection and resilience of critical Information Infrastructure; h) promotion of research & development in cybersecurity; i) reducing supply chain risks; j) human resource development; k) creating cybersecurity awareness; l) developing effective public-private partnerships; and m) information sharing and cooperation.[78]

However, to tackle some of the gaps in the NCSP, the government announced its intention to introduce a new national cybersecurity strategy. The Data Security Council of India (DSCI) prepared

---

[72] Sudhansu Nayak, "Digital Personal Data Protection Bill 2022: Reservations and Recommendations," ORF, November 29, 2022, https://www.orfonline.org/expert-speak/digital-personal-data-protection-bill-2022/.

[73] Human Rights Watch, "India: Data Protection Bill Fosters State Surveillance," Human Rights Watch (blog), December 22, 2022, https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance.

[74] Ministry of Communication and Information Technology and Department of Electronics and Information Technology, "National Cyber Security Policy - 2013," Pub. L. No. 2(35)/2011-CERT-In (2013), https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf.

[75] Ministry of Communication and Information Technology and Department of Electronics and Information Technology.

[76] Ibid.

[77] Ibid.

[78] Ibid.

and submitted a comprehensive draft **National Cyber Security Strategy (NCSS)** to the Union Government in 2020,[79] and the Prime Minister's Office (PMO) has announced that it is currently reviewing the proposed strategy for implementation.[80]

The proposed NCSS for India includes three sets of actions: part 1 deals with securing India's cyberspace, part 2 deals with strengthening cyber capabilities, and part 3 deals with cyberspace synergies. It details 21 key areas to "ensure a safe, secure, trusted, resilient, and vibrant cyberspace for India's prosperity."[81] This includes a renewed focus on robustly enhancing and building resilience infrastructure in the wake of new cybersecurity and cyber warfare threats by transnational actors and doubling down on strengthening threat detection and responses to new technologies, such as Advanced Persistent Threat Vectors.

According to the draft NCSS, there is a need for Critical Information Infrastructure Protection, Small and Medium Businesses security, and Sectoral Preparedness. As the Union Government emphasises doubling down on its crucial 'Make in India' and 'Digital India' efforts, it is expanding its digital footprint thanks to the large-scale digitisation of public services. Over the past few years, and in the wake of the pandemic, India has pushed for the rapid digitisation of critical industries, social spaces, payments, and transactions. Consequently, the risk of threat exposure in cyberspace has increased. For example, a November 2022 cyber-attack against the AIIMS compromised the sensitive data of 30-40 million patients, reigniting public debate about building adequate cyber resilience and response infrastructure in the nation.[82]

The proposed NCSS asserts that national cybersecurity efforts would be insufficient unless state-level (quasi-federal) efforts were undertaken. Additionally, the draft strategy calls for the union to strengthen its cyber security structure, institutions, and governance, as well as separate budgetary allocations for cybersecurity. To strengthen India's strategic and commercial interests, the draft strategy suggests that the end products of cyber security research, innovation, and technology development should be commercialised. Moreover, it has reiterated the importance of developing cyber security capabilities and skills to serve India's digital well-being. To systematise data security, the proposed NCSS recommends strengthening audit and assurance functions, reinforcing Incident/Crisis Management, and improving data governance in India owing to the scale, pace, and complexity of cyber security.

Further, NCSS is categorical about the positive use of advanced technologies such as 5G, wireless, cloud, mobility, IoT, AI/ML, robotics, AR/VR, hardware/semiconductor, HPC and Quantum Computing, DLT, UAV, SDI, and material science, stating that these advancements will play a significant role in shaping India's cyber security in the long run. Finally, the proposed strategy calls for the synergy of India's internet infrastructure, technical standards, cyber insurance, cyber diplomacy, digital forensic technologies, methods, and legal procedures to advance India's interests

[79] Data Security Council of India, "National Cyber Security Strategy 2020" (DSCI - A NASSCOM Initiative, 2020).
[80] Devesh K. Pandey, "Draft Cybersecurity Strategy Has Been Formulated: Centre," The Hindu, December 14, 2022, sec. India, https://www.thehindu.com/news/national/national-security-council-secretariat-formulated-draft-national-cyber-security-strategy-centre/article66262515.ece.
[81] Data Security Council of India, "National Cyber Security Strategy 2020".
[82] Express News Service, "AIIMS Server Hack: Seek Interpol Help for IP Address Details, Delhi Police Ask CBI," The Indian Express, December 18, 2022, https://indianexpress.com/article/cities/delhi/aiims-server-hackdelhi-police-cbi-interpol-help-ip-address-details-8331538/.

in safe, secure, and open cyberspace. It also aims to position and brand India as a leading global cyber security force on both domestic and global platforms.

It is worth noting that in addition to the legal, policy, and strategic frameworks elucidated above, the Government of India has formed ancillary bodies such as NCIIPC, NCCC, and the Online Cyber Crime Portal to streamline cyber threat detection, coordination, and communication efforts. To support the work done by these bodies, the following initiatives have also been established:

1. **Cyber Surakshit Bharat Initiative.**[83] The Cyber Surakshit Bharat Initiative was created to spread awareness about cybercrimes and build capacity among frontline IT officials and Chief Information Security Officers in government departments to adequately defend digital and technological infrastructures and tackle potential cyberattacks.[84]

2. **Cyber Swachhta Kendra.**[85] The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is an initiative set up by MeitY under NCPS and operated by CERT-In.[86] Its main goal is to detect botnet infections in the country, and to inform and enable the cleaning and securing of end-user systems to prevent the spread and development of further infections.

3.3 Lessons from India's cybersecurity frameworks

As discussed above, India has made significant strides in passing laws and creating policies towards its goals of creating a Digital India with resilient and secure cyberspace for its citizens. However, improvements can still be made, particularly with respect to the resilience infrastructure, response capabilities, user surveillance, data protection, and privacy. Defence expert Lt. Col. Sanjiv Tomar, has expressed a need for the creation of a cyber command as a "parallel hierarchical structure […] prudent to address the jurisdiction issues right at the beginning of policy implementation."[87] The implementation of existing public-private partnerships also needs to be strengthened to ensure that SMEs and organisations can be protected from potential attacks. Several experts have pointed out the need to strengthen the National Cyber Coordination Centre (NCCC) and redraft the policy to account for and recognize the complexity of cyber incidents and rapidly evolving technological innovations.

At the end of the day, India suffers from the same problem as the US, EU, and every other state or regional actor trying to create regulations in cyberspace - no one can accurately predict the scale and speed at which new viruses, malware, and other threat technologies emerge and evolve. Consequently, lawmakers, defense experts, and cyber professionals in the country are working to constantly and consistently revise existing frameworks to ensure that systems and users can protect themselves from malicious actors in cyberspace.

---

[83] Ministry of Electronics and Information Technology, Government of India, "Cyber Surakshit Bharat Physical Training Programme," 2022, https://www.meity.gov.in/writereaddata/files/Cyber%20Surakshit%20Brochure_.pdf.
[84] Translation: Cyber Secure India Initiative.
[85] CERT-In, "Cyber Swachhta Kendra Botnet Cleaning and Malware Analysis Centre," accessed January 26, 2023, https://www.csk.gov.in/.
[86] Translation: Cyber Cleanliness Centre.
[87] Sanjiv Tomar, "National Cyber Security Policy 2013: An Assessment," Manohar Parrikar Institute for Defence Studies and Analyses (blog), August 26, 2013.

4. Indian defensive and offensive cyber capabilities

Having outlined both India's cyber landscape and the various institutional frameworks around it, the present chapter's aspiration is to assess what defensive and offensive cyber capabilities these translate into. After all, it is by illuminating what India can and cannot do in exact terms that a clear evaluation of India's cyber resilience may be put forth. Cyberspace has become a staging ground for state-sponsored conflicts, often rising to levels of national security concerns. Some prime examples include the 2007 Estonia cyber-attack, the 2008 Georgia cyber-attack, the 2010 Stuxnet attack on Iran, and the 2015 NitroZeus operation, among others.[88] However, more recently, the alleged 2016 Russian cyber interference in US presidential elections, the 2017 Ukraine Power Grid Cyber Attack, the 2017 NotPetya Malware Attack, led to a ripple of concern across the globe about the possibility of hostile militaries inflicting significant damage to other states by targeting their cyberspace.[89] The 2020 cyber-attack on the Kudamkulam Nuclear Power Plant and other cyber-attacks on India by its adversaries in the region demonstrate that there is a high likelihood that as modern warfare evolves, disputes between states will always include attacks on critical infrastructure connected to cyberspace.[90] To that end, before addressing Indian cyber capabilities in detail, the wider nebula of cyber capabilities in general terms must be disentangled.

4.1 Defining Cyber capabilities and the roles they play

Capabilities are generally defined as the ability to affect a desired outcome. In the context of cyber operations, having a capability means possessing the resources, skills, knowledge, operational concepts and procedures to be able to reach a desired effect in cyberspace.[91] Capabilities constitute the building blocks and foundation of operations in cyberspace. Thus, any policy instrument that can manifest a desired effect in cyberspace may be considered a cyber capability. Such capabilities may be defensive or offensive in nature.

Offensive cyber operations are characterised by US and UK military doctrines as effects (i.e. capabilities) that seek to project power through the application of force in or through cyberspace to achieve (military) objectives. These operations may have a direct real-world impact on the physical and social layers as they seek to disrupt, manipulate, and deny opponents.[92] Defensive capabilities, on the other hand, are passive or active measures seeking to preserve the ability to use cyberspace to enable one's own freedom of action. These may include vulnerability assessment and risk

[88] M.K. Sharma, "India's Cyber Warfare Strategy in Next Decade," July 16, 2013; Matthias Schulze, "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations," in 2020 12th International Conference on Cyber Conflict (CyCon) (2020 12th International Conference on Cyber Conflict (CyCon), Estonia: IEEE, 2020), 183–97, https://doi.org/10.23919/CyCon49761.2020.9131733.

[89] Adam Badawy, Emilio Ferrara, and Kristina Lerman, "Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign," 2018, https://doi.org/10.48550/ARXIV.1802.04291.

[90] Mallick, "Cyber Attack on Kudankulam Nuclear Power Plant".

[91] Tom Uren Hanson Bart Hogeveen, Fergus, "Defining Offensive Cyber Capabilities," accessed January 11, 2023, http://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

[92] "AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)," n.d.; "Cyber Primer 3rd Edition," n.d.

management as well as possible responsive measures in line with operational needs. Essentially, they prevent or mitigate the effectiveness of the offensive cyber operations conducted by potential adversaries. Naturally, certain capabilities may play both offensive and defensive roles. For instance, a credible deterrent, albeit offensive in nature (by virtue of being a guaranteed counter-attack), is used primarily for defensive purposes to deter adversaries through punishment.

4.2 Assessing India's cyber capabilities – the Cyber Arms Watch

Label	Declared Capabilities Rating (DCR)	Perceived Capabilities Rating (PCR)
Level 0	No Official Indications of Offensive Cyber Capability	No aspirations to obtain offensive cyber capabilities
Level 1	Stated Aspiration for Offensive Cyber Capability	Perceived to have obtained or used spyware capabilities.
Level 2	Sanctioned media reporting on offensive cyber details and/or operations by an official (capabilities likely to exist but unconfirmed by official resources, the extent of which being unknown)	Perceived to be working on obtaining offensive cyber capabilities
Level 3	National strategy or related official document mentioning existing offensive cyber capabilities	Perceived to have either launched or obtained the ability to launch some forms of cyber effect operation
Level 4	Defence cyber strategy or similar with details on offensive cyber command structures (general order of battle) and missions, conditions of employment and overall principles of operation	Perceived to have integrated offensive cyber capabilities into their military structure and use it (either literally or as a deterrent) to achieve strategic objectives.
Level 5	Defence cyber strategy or similar where offensive cyber capabilities are detailed, including available definitions of different types of cyber effects, detailed order of battle (units, manpower, budget), as well as specific and general TTPs.	Viewed as having launched several successful offensive cyber effect operations, with the proven capability to denigrate and destroy enemy systems or infrastructure.

Table 2: The six-tiered labelling system for the Cyber Arms Watch.

The HCSS Cyber Arms Watch seeks to create a cyber transparency index that offers a comparison between the stated and perceived cyber capabilities of countries. In rating countries' capabilities with a six-tiered system, the delta between the Declared Capabilities Rating (DCR) and the Perceived Capabilities Rating (PCR) forms the basis for a country's cyber transparency, which is measured by the Cyber Transparency Index (CTI).

In the latest (May 2022) edition of the HCSS Cyber Arms Watch, India is rated with a DCR of level 1 and PCR of level 3 (cf. Table 2), resulting in an untransparent cyber transparency rating.[93] Officially, while cyberspace and offensive cyber capabilities are identified and mentioned in doctrinal documents on information warfare, there is a lack of clarity in the available data. As such, the nature and extent of India's cyber capabilities cannot be determined reliably. India's Defense Cyber Agency (DCyA) has reportedly become operational in August 2021, indicating that the Indian government intends to develop cyber capabilities further. Beyond this, however, it is difficult to differentiate aspirational cyber capabilities from capabilities that are already (being) established in India due to a lack of reliable and transparent information, particularly from government and interconnected circles.[94]

The perceived rating of India's cyber capabilities, on the other hand, is much higher at Level 3. Nonetheless, there remains a discrepancy among different observers and experts, while most are hopeful of India's potential to develop cyber capabilities, there remains much scepticism about the effectiveness of India's current and near-future capabilities. Equally, there are many doubts about

---

[93] HCSS, "Cyber Arms Watch," HCSS, 87–88, accessed January 9, 2023, https://hcss.nl/cyber-arms-watch/.
[94] Louk Faesen et al., "Uncovering the Stated & Perceived Offensive Cyber Capabilities of States," n.d.

the actual level of commitment of the Indian government towards cyber as a strategic domain and towards constructing and expanding its cyber capabilities. As such, many institutes tend to rank India conservatively: the Belfer Center's *National Cyber Power Index* (2020) ranks India as the 21st most comprehensive cyber power, and its offensive capabilities 28th out of 30.[95] The Institute for Strategic Studies (IISS), on the other hand, ranks cyber powers in a 3-tiered system based on relative strength of countries across 7 categories:[96]

- Strategy and doctrine
- Governance, command, and control
- Core cyber intelligence capability
- Cyber empowerment and dependence
- Cyber security and resilience
- Global leadership in cyberspace affairs
- Offensive cyber capabilities

Tier 1 Cyber Powers (currently only the US) possess world-leading strengths in all categories, Tier 2 Cyber Powers possess world-leading strengths in some categories, and Tier 3 Cyber Powers have (potential) strengths in certain categories, while possessing significant weaknesses in others. The IISS considers India a Tier 3 Cyber Power, identifying the potential of India's strong digital economy, strong start-up and private sector initiative, as well as India's visibility in cyber diplomacy.[97] Nonetheless the above studies remark only modest progress in the spheres of policy and doctrine. Through leveraging its digital infrastructure and industry and adopting a whole-of-society approach, India could transition from a solid regional power into a comparably strong global player.[98]

While India enjoys a good deal of cooperation with the US on cybersecurity,[99] expanding its capabilities will prove instrumental in solidifying India's position in the regional and global balances of power. A lack of clear vision of cyber space and building India's cyber capabilities is deemed a major impeding factor in India's progress as an upand-coming cyber power. While developments and progress are in work across the Indian political sphere (cf., Chapter 3 - Legal, strategic, and policymaking frameworks), India's cybersecurity responses are somewhat lacking, indicating a potentially low ability or resolve to respond to cyber threats. India fares quite well against Pakistan, where it has been conducting low-medium intensity offensive cyber operations (both attacks and counterattacks) for several years now.[100] Against the looming cyber threat of China, however, India seems to be either unwilling or unable to respond in kind. The People's Liberation Army (PLA) has made significant reforms and has successfully integrated the whole spectrum of electronic and information warfare, including cyber space; the Indian army and defense agencies are quite

---

[95] Julia Voo et al., "National Cyber Power Index 2020," 2020.

[96] "Cyber Capabilities and National Power: A Net Assessment," IISS, accessed January 18, 2023, https://www. iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[97] "Cyber Power - Tier Three," IISS, accessed January 9, 2023, https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three.

[98] Hannes Ebert, "Hacked IT Superpower: How India Secures Its Cyberspace as a Rising Digital Democracy," India Review 19, no. 4 (August 7, 2020): 376–413, https://doi.org/10.1080/14736489.2020.1797317; "Cyber Power - Tier Three".

[99] Joshua T White, "After the Foundational Agreements: An Agenda for US-India Defense and Security Cooperation," n.d.

[100] "The Cyber Threat Facing Pakistan," accessed January 18, 2023, https://thediplomat.com/2020/06/ the-cyber-threat-facing-pakistan/; "Indian Cyber-Espionage Activity Rising amid Growing Rivalry with China, Pakistan," The Daily Swig | Cybersecurity news and views, February 25, 2021, https://portswigger.net/ daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan.

behind.[101] After repeated breaches gathering sensitive data and some disruptive attacks between 2010-2018, India only mustered a limited response, primarily in trying to reduce its vulnerabilities. And yet, India's effort to prevent Chinese technological domination, through banning apps and the 'Make in India' campaign was only marginally effective.[102] While restraint is prudent given the difficulty of attributability and certainty in cyber-attacks, defensive capabilities in cyberspace will always remain less efficient and flawed given that there are always unknown vulnerabilities in digital systems. In essence, defence is always failing, necessitating offensive countermeasures to edify deterrence and make it credible.[103]

Nevertheless, one should be careful when employing offensive cyber capabilities, even if one can accurately identify the hostile target for retribution, offensive manoeuvres can have a high potential for collateral damage, along with an opportunity for further escalation.[104] And if one is unsure as to which actors are responsible for attacks on India's cyber infrastructure, employing purely offensive means is outright dangerous. With the pervasiveness of proxies and botnets, the odds are that without clearly being able to attribute the attack to a (known) hostile actor, the wrong entity may be targeted.[105] Thus, simply building up offensive cyber capabilities, while useful, is not optimal. A whole-of-society effort is needed, encompassing both preparedness and vigilance from the civilian sector, as well as cyber diplomacy to determine a clear set of norms and rules of engagement.[106] India has many factors that can leverage to secure a leading role in this transformative process, not only its start-up culture and digital-industrial potential, but also its global position vis-à-vis the other great powers. Through strategy, India could endeavour to connect other cyber powers and form a network of international cyber cooperation or, at the very least, a framework of understanding.

---

[101] Ibid.

[102] "India's Response to China's Cyber Attacks," accessed January 9, 2023, https://thediplomat.com/2019/07/ indias-response-to-chinas-cyber-attacks/.

[103] Institute of South Asian Studies, "Going On The Offensive: India's Cyber Capabilities – Analysis," Eurasia Review (blog), December 30, 2022, https://www.eurasiareview.com/31122022-going-on-the-offensive-indias-cyber-capabilities-analysis/; Bommakanti, "Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army".

[104] Tom Uren Hanson Bart Hogeveen, Fergus, "Defining Offensive Cyber Capabilities," accessed January 11, 2023, http://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

[105] James Coker, "Offensive Cyber-Capabilities: How and When Should They Be Used?," Infosecurity Magazine, March 2, 2021, https://www.infosecurity-magazine.com/magazine-features/offensive-cybercapabilities-be-used/.

[106] Faesen et al., "Uncovering the Stated & Perceived Offensive Cyber Capabilities of States"; "India's Cyber Security: A Look at the Approach and the Preparedness - Indian Council of World Affairs.

5. Results of the National Cyber Resilience Game

5.1 The National Cyber Resilience Game (NCRG)

As part of the IDCSS22, students took part in the India NCRG, incorporating all the issues highlighted in the previous chapters. This serious game, developed by the HCSS, is a gamified analytical tool that facilitates group discourse on various strategically relevant subjects. The results of these game sessions lend strategic and analytical insights into the capabilities that the participants deem the most important. The aim of the NCRG was to diagnose and illuminate gaps in Indian cyber resilience, with participants having been provided with background information about India's cyber landscape and strategic objectives. Considering the large number of participants in the NCRG during the 2022 school, the game's resulting data may prove useful for Indian policymakers.

5.2 Categorising capabilities between strategic sectors and strategic functions

	Protection & Prevention	Threat Reduction (Mitigation)	Response	Deterrence
Diplomacy				
Military				
(Counter)Intelligence				
Economic				
Law Enforcement				
Public-Private Partnerships (PPP)				

Table 3: An overview of the strategic sectors and functions used in the National Cyber Resilience Game.

Compared to the defensive-offensive dichotomy outlined in the previous chapter, a more complex and nuanced categorization of cyber capabilities was used for the National Cyber Resilience Game of 2022 (see Table 3).

The 47 capability cards of the India NCRG could be linked to their strategic function(s) (protection, mitigation, etc.), as well as their respective sectors of impact. Capabilities may be assigned to one or more places on the board. For instance, the capability to identify and reduce military vulnerabilities while building the capacity to attack malicious actors to prevent cyber threats should be placed in the military sector, which may influence all four strategic functions. Identifying and reducing vulnerabilities will reduce the damage to incoming threats; as a result, not being an easy target may outright prevent future attacks. Likewise, the ability to attack malicious actors (be it pre-emptively or in response to hostile action) can be both a deterrent and a potential punitive response for adversaries.[107] In another example, para-cyber or trans-cyber capabilities (i.e. capabilities whose nature is technically beyond the realm of cyberspace) such as implementing economic sanctions against malicious actors, can have broad-reaching effects in cyberspace.[108] Prima facie, economic sanctions are an economic and diplomatic response to hostile action by other powers, but economic sanctions may also pre-emptively reduce technological connectivity and dependency on strategic competitors or rivals (meaning fewer potential backdoors and vulnerabilities for them to exploit).[109] Leveraging cyber diplomacy and economic connectivity, a power could equally use the threat of sanction to their advantage, not only as a deterrent, but to compel other powers to be aligned with India's international cyber policy.[110] As such, the capability of adopting and enforcing economic sanctions fulfils the function of protection, response, and deterrence in the economic sector, as well as the functions of threat reduction, response and potentially deterrence in the diplomatic sector.

5.3 The results of the game

During the IDCSS22, over 300 students participated in the India NCRG, placing cards on the strategy board a total of 836 times. The present section enumerates the statistical results of these 836 card placements.

The card placed most often (32 times) was *an assistant private actor in detecting attacks*. This card denotes "[t]he ability to assist private actors in reducing vulnerabilities and detecting attacks in order to reduce their risk of being attacked." Within the top five most placed capability cards it was followed by *Identify and reduce military vulnerabilities*, *Adopt and enforce economic sanctions*, *Implement protection measures*, and *Prosecute actors breaching international law*, which were placed 29, 28, 25, and 23 times respectively. Overall, there were eight cards that were placed 20 or more times, also including *Promote cyber hygiene*, *Raise awareness on vulnerabilities in vital sectors*, and *Invest in R&D*, which were placed 22, 21, and 20 times respectively. Figure 3 presents how often each card was placed.

---

[107] "AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)".

[108] Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?," in 2018 10th International Conference on Cyber Conflict (CyCon) (2018 10th International Conference on Cyber Conflict (CyCon), Tallinn: IEEE, 2018), 55–72, https://doi.org/10.23919/CYCON.2018.8405010.

[109] "India's Cyber Security Capabilities," accessed January 12, 2023, https://edukemy.com/daily-current-affairs/ gazette/2021-07-27/indias-cyber-security-capabilities.

[110] Seden Akcinaroglu and Elizabeth Radziszewski, "Web of Links: Rival Connections and Strategic Accommodation in Response to Threats," Journal of Global Security Studies 2, no. 3 (July 2017): 237–52, https://doi.org/10.1093/jogss/ogx009.
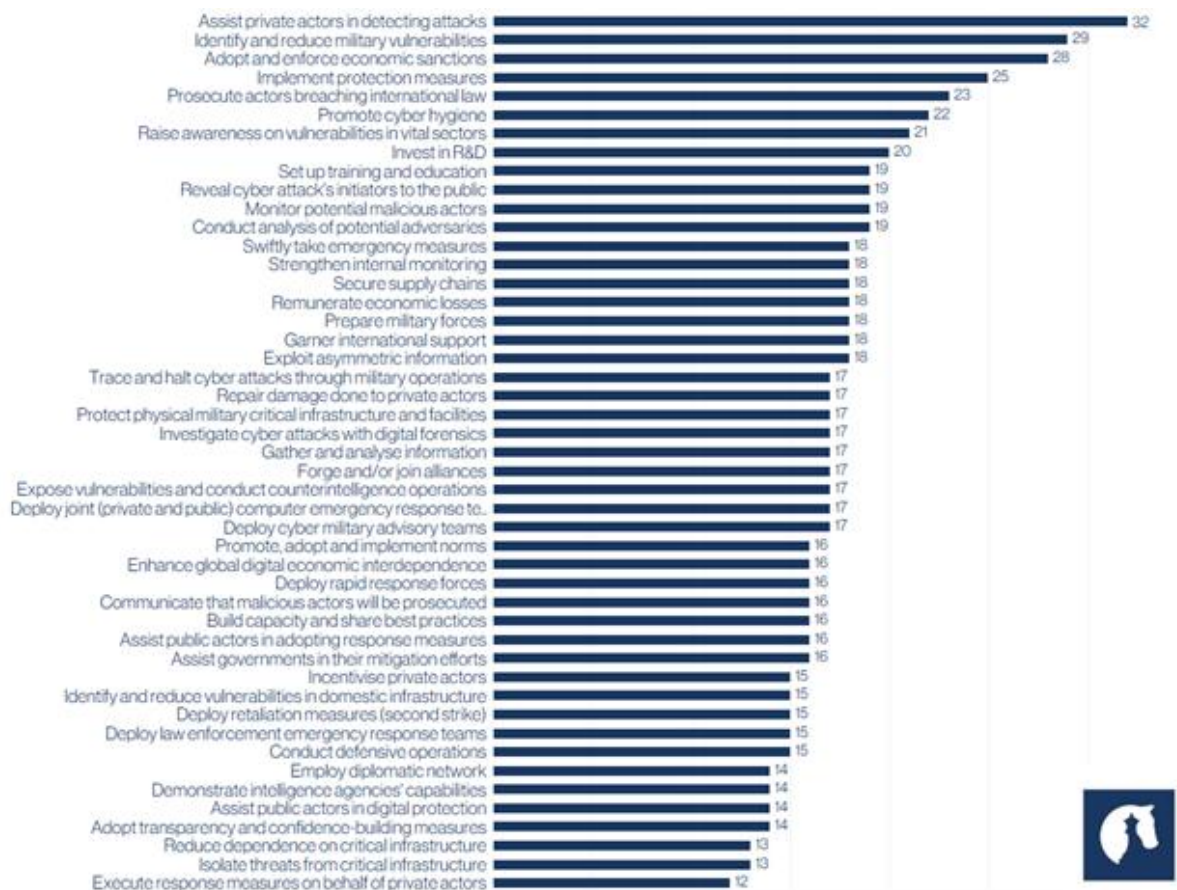
Figure 3: List of the India NCRG capability cards with frequency of placement.

The allocation of capability cards above denotes certain priorities among the participants. Raising awareness and promoting general digital literacy are seen by the participants as an underlying requisite and enhancement of India's cyber resilience at large. Conversely, various broad-stroke capabilities, such as the identification and reduction of military vulnerabilities to cyber threats, or the reliance on economic capabilities in deterring foreign actors from targeting India with cyber-attacks, are also seen by the participants as vital. This suggests that a resilient Indian posture when it comes to national cyber resilience consists both of educational initiatives aimed at the public, as well as high-level executive action.

The least frequented capability card was *Execute response measures on behalf of private actors*, which was placed by participants only 12 times throughout the duration of the NCRG. This suggests an overarching sentiment among participants regarding government involvement in the cybersecurity of private actors. While providing assistance to private actors in defending against cyber threats is seen as a strategically crucial objective by the participants (so much so that the most-placed card denotes the capability to do just that), active government involvement in striking back is of low priority.

Two more capability cards were placed by the participants 13 times each. These were *reduced dependence on critical infrastructure* and *isolated threats from critical infrastructure*. The lack of reliance on these capabilities may indicate a few underlying sentiments among participants. On the one hand, the explanation seems apparent that there may be insufficient levels of awareness as to what makes a specific infrastructure critical. Thus, the reliance of such a critical infrastructure on the

cyber domain may also fall short of sufficient recognition. On the other hand, the revamping of critical infrastructure with cyber resilience in mind may prove to be a disruption to such institutions' day-to-day conduct, and participants may see such disruptions to be too high to pay for the mitigation of potential cyberattacks in the future.

The participants relied on the remaining 36 capability cards consistently, but with some degree of restraint, placing them between 14 and 29 times. The low arbitrage in the popularity of these cards suggests that they are viewed as important enough to be placed consistently by most active participants but not as strategically vital at the national level to enjoy a degree of prominence comparable to the five most placed capabilities. The distribution of capability cards across strategic sectors and functions, however, somewhat nuances this picture (see Table 4).

	Protection & Prevention	Threat Reduction (Mitigation)	Response	Deterrence
Diplomacy	19 43 5 29 26 / 11 38 24 14 1 / 30 3 41 2 18 7 / 47 33 32	29 43 30 38 5 / 19 9 1 11 31 7 / 47	30 5 19 15 1 13 / 8 29 43 41 18 / 38	38 19 43 1 5 30 / 9 41 18 26 35 / 25 3 7 8 29
Military	4 17 41 8 3 10 / 40 18 12 7 24 / 14 32	4 41 17 28 8 6 / 47 24 40	8 32 25 41 4 15 / 34 36 37	41 6 25 12 8 17
(Counter)Intelligence	40 10 7 3 12 33 / 21 17 47 14 6 4 / 2 1 16 19 8 24 / 26 36 11	6 10 24 12 3 40 / 16 28 45 36 7 / 17 42 47 19 21 4 / 15 2 14 13	15 25 36 7 34 / 12 35 16 37 3 17 / 21 8 23 29 6 24 / 13	35 12 34 3 6 25 / 39 4 13 1 7 8
Economic	1 33 47 22 14 11 / 2 3 13 27 24 40 / 9 10 20 44 45	14 11 2 27 28 47 / 32 20 7 45 21 9 / 13	22 15 1 9 14 29 / 46	9 1 29 26 22 23 / 38 14 29 45
Law Enforcement	3 1 14 27 18 5 / 13 22 10 47 24 / 19	6 46 3 5 18 47 / 2 33 19	46 42 37 5 18 3 / 15 13 34 24 32 / 10	5 18 3 13 40 26 / 42 22 46 25 24
Public-Private Partnerships (PPP)	2 27 33 26 11 / 39 20 47 13 16 / 31 14 24 19 12 / 40 7 3 21 29 1 / 6 8 10 44	2 31 16 14 44 / 28 21 47 20 6 / 29 33 7 19 45 / 36 27 15 11 32 8 / 10 3 41	44 23 15 16 2 / 38 42 34 19 20 / 7 33 46 6 8 32 / 39 37	20 1 47 8 16 27 / 37

Table 4: Distribution of capability cards.

In summary, the Public-Private Partnerships (PPP) strategic sector saw the most capability card placements, whereas the military strategic sector saw the least. In contrast, the Protection and Prevention strategic function saw the most capability card placements by participants, with the most frequented sector being PPP within the function. When both strategic functions and strategic sectors were factored in, it was the Military Deterrence field in which participants placed the fewest cards.

The lessons of the NCRG seem to be multifaceted. Firstly, it could be observed that participants wanted the Indian government to assume a more prominent role in assisting private actors in defending against cyber-attacks, while outright retaliation on behalf of private actors was not seen as a priority at all. Second, passive resilience being outsourced to the population is considered a high priority. Broad action related to the promotion of digital hygiene and awareness-raising was seen as a high priority by participants points at this conclusion. Third, gaps in military cyber defense are also

seen as a top priority by participants, despite the relatively low prominence of military and deterrent capabilities in the end data. Fourth, the criticality of infrastructure and related vulnerabilities is seen either as less relevant than other areas or as too costly to address. Fifth, it can also be concluded that participants wanted the Indian government to continue developing broad-stroke domestic and foreign policies in fields such as investment in R&D or the issuing of economic sanctions against malicious actors in the cyber domain.

6. Conclusions and recommendations

6.1 Observations

The present report showcases the position of India within the cyber domain. The severity of the threats faced by India in the cybersphere is illustrated in the first two chapters. Comprehensive overviews are provided in subsequent chapters on India's cyber landscape; the legal, policy, and strategic frameworks in place; and the defensive and offensive cyber capabilities of India in subsequent chapters. Finally, HCSS's largest Serious Game as of January 2023 has yielded significant insights into popular sentiments revolving around the cyber domain. The lessons and observations obtained from the analyses are presented in this section.

From the findings of open-source desk research, it is clear that India has been and is still developing formidable cyber capabilities. This means that significant institutional frameworks are in place to build national cyber resilience, and that considerable entrepreneurial and innovation ecosystems exist within India to power that process. That said, in many ways, India's resilient posture within the cyber domain falls short of meeting the challenges of the time, illustrated by the sheer volume of malicious foreign activity targeted at the Indian cyber infrastructure by state and non-state actors. To meet these challenges, various measures must be undertaken in the future, especially with respect to capacity building to respond to cyber-attacks, the protection of infrastructure, and making the military cyber resilient. Additionally, the results of the NCRG uncovered representative popular sentiments as to how the fine-tuning of effort allocation should be conducted within the developmental schemes aimed at making India more cyber-resilient.

The foremost takeaway from these findings is two-fold. First, India's capacity to respond to cyber-attacks, while considerable, lags behind the requirements of the challenges it faces. This is especially true when it comes to defending private actors, strategic sectors of infrastructure, and military vulnerabilities. Second, India's efforts to cultivate digital hygiene and awareness of cybersecurity among its population are the most welcome and show promising frameworks for building cyber-resilient India.

6.2 Recommendations

Based on the conclusions, the authors shortlisted several recommendations for Indian policymakers with respect to what actions across the various strategic sectors would contribute to India's cyber resilience:

1. **Expanding existing legislation pertaining to the cyber domain.** The development of norms and good conduct within the cybersphere is of paramount importance in building a cyber-resilient India. Amending the IT Act to meet the challenges of the 2020s, facilitating the implementation of the National Cyber Security Strategy (NCSS), or expanding the Personal Data Protection Bill (PDPB) could all serve this purpose. Further regulation of data usage and privacy protection would safeguard the population more comprehensively from bad faith by foreign and domestic actors. Conversely, communicating about new cyber legislation to the public cultivates the objectives of digital hygiene and cyber awareness, sought both by the Indian government and the participants of the NCRG. There is a need for grassroots capacity building in both urban and rural areas, localised, and translated into different languages.

2. **Develop the ability to respond to cyberattacks on a large scale.** Expanding CERT-In's capacity to handle a larger volume of cases would allow for more extensive crackdowns on and responses to cyber-attacks. Both private actors and critical sectors of the infrastructure, such as healthcare and finance, depend on cybersecurity in their day-to-day conduct. As such, CERT-In should manage to handle a larger proportion of cyber-attacks targeted at various Indian entities would enhance this efficiency. Moreover, a lower success rate of cyber breaches would deter grassroots organisations from attempting these in the first place.

3. **Conduct cybersecurity assessments of vulnerabilities in the Indian military.** The mitigation of these vulnerabilities not only enhances operational effectiveness in the contingency of high-intensity warfare but also forms the primary line of securing military assets in peacetime. Such assessments also enable the safer deployment of cyber capabilities when it comes to deterrence and response options. Furthermore, vulnerability assessments will empower India to reform its cyber doctrine; such a development could precipitate in a clear vision and framework for operations in wartime, as well as resilience in peacetime.

Bibliography

"About DSCI- Data Protection, Thought Leadership, Policy Advocacy." Accessed January 25, 2023. https://www.dsci.in/content/about-us#about_section.admin.

Ahaskar, Abhijit. "India Saw the Highest Number of Cyberattacks on Govt Agencies in 2022: Report." The Mint, December 30, 2022. https://www.livemint.com/technology/tech-news/india-saw-the-highest-number-of-cyberattacks-on-govt-agencies-in-2022-report-11672389099189.html.

"AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)," n.d.

Akcinaroglu, Seden, and Elizabeth Radziszewski. "Web of Links: Rival Connections and Strategic Accommodation in Response to Threats." *Journal of Global Security Studies* 2, no. 3 (July 2017): 237–52. https://doi.org/10.1093/jogss/ogx009.

"All Statements of Budget Estimates, Notes on Demands for Grants 2022-2023 -Ministry of Electronics and Information Technology." Accessed January 25, 2023. https://www.indiabudget.gov.in/.

Badawy, Adam, Emilio Ferrara, and Kristina Lerman. "Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign," 2018. https://doi.org/10.48550/ARXIV.1802.04291.

Bommakanti, Kartik. "Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army," n.d.

CERT-In. "Cyber Swachhta Kendra Botnet Cleaning and Malware Analysis Centre." Accessed January 26, 2023. https://www.csk.gov.in/.

Chatterjee, Anupriya. "India's Had Its Worst Year of Cyberattacks, but 2023 Will See Govt & Firms Ramp up Defences." *The Print*, December 30, 2022. https://theprint.in/india/indias-had-its-worst-year-of-cyberattacks-but-2023-will-see-govt-firms-ramp-up-defences/1286441/.

Coker, James. "Offensive Cyber-Capabilities: How and When Should They Be Used?" Infosecurity Magazine, March 2, 2021. https://www.infosecurity-magazine.com/magazine-features/offensive-cybercapabilities-be-used/.

Computer Security Division, Information Technology Laboratory. "CSRC Topic: Advanced Persistent Threats | CSRC." CSRC | NIST, February 25, 2020. https://csrc.nist.gov/Topics/Security-and-Privacy/risk-management/threats/advanced-persistent-threats.

"Cyber Primer 3rd Edition," n.d.

"Data Protection in the EU". European Commission. Accessed February 10, 2023. https://commission.europa. eu/law/law-topic/data-protection/data-protection-eu_en.

Data Security Council of India. "National Cyber Security Strategy 2020." DSCI - A NASSCOM Initiative, 2020.

"Details about Indian Cybercrime Coordination Centre (I4C) Scheme | Ministry of Home Affairs." Accessed January 25, 2023. https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme.

Digital Guardian. "What Is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More." Text. Accessed February 1, 2023. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more.

"Digital India." Accessed January 24, 2023. https://digitalindia.gov.in/.

Drishti IAS. "National Cyber Security Strategy." Accessed January 25, 2023. https://www.drishtiias.com/daily-updates/daily-news-analysis/national-cyber-security-strategy-1.

Ebert, Hannes. "Hacked IT Superpower: How India Secures Its Cyberspace as a Rising Digital Democracy." *India Review* 19, no. 4 (August 7, 2020): 376–413. https://doi.org/10.1080/14736489.2020.1797317.

Express News Service. "AIIMS Server Hack: Seek Interpol Help for IP Address Details, Delhi Police Ask CBI." *The Indian Express*, December 18, 2022. https://indianexpress.com/article/cities/delhi/aiims-server-hack-delhi-police-cbi-interpol-help-ip-address-details-8331538/.

Faesen, Louk, Alexander Klimburg, Simon van Hoeve, Raffaele Minicozzi, Salome Petit

Siemens, and Giulia Tesauro. "Uncovering the Stated & Perceived Offensive Cyber Capabilities of States," n.d.

Government of India. "Digital India." Accessed January 25, 2023. https://digitalindia.gov.in/.

Hanson, Tom Uren, Bart Hogeveen, Fergus. "Defining Offensive Cyber Capabilities." Accessed January 11, 2023. http://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

———. "Defining Offensive Cyber Capabilities." Accessed January 11, 2023. http://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

HCSS. "Cyber Arms Watch." HCSS. Accessed January 9, 2023. https://hcss.nl/cyber-arms-watch/.

"HCSS Strategic Game." Accessed January 12, 2023. https://idcss22.strategicgame.nl/info.

HCSS, "The Indo-Dutch Cyber Security School", accessed June 06, 2024 https://hcss.nl/indo-dutch-cyber-security-school/#:~:text=HCSS%20is%20proud%20to%20announce,October%20to%2010th%20of%20November.

IISS. "Cyber Capabilities and National Power: A Net Assessment." Accessed January 18, 2023. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

IISS. "Cyber Power - Tier Three." Accessed January 9, 2023. https://www.iiss.org/blogs/researchpaper/2021/06/cyber-power---tier-three .

India Brand Equity Foundation. "Digital India | IBEF." Accessed January 25, 2023. https://www.ibef.org/government-schemes/digital-india.

"Indian Cyber Crime Coordination Centre (I4C) – A 7-Pronged Scheme to Fight Cyber Crime." Accessed January 25, 2023. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579184.

Indian Defence Review. "Digital India under Cyber Attack!!" Accessed January 24, 2023. http://www.indiandefencereview.com/spotlights/digital-india-under-cyber-attack/.

"Indian Cyber-Espionage Activity Rising amid Growing Rivalry with China, Pakistan," February 25, 2021. https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan .

"India's Cyber Security: A Look at the Approach and the Preparedness - Indian Council of World Affairs (Government of India)." Accessed January 18, 2023. https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=6172&lid=4236.

"India's Cyber Security Capabilities." Accessed January 12, 2023. https://edukemy.com/daily-current-affairs/gazette/2021-07-27/indias-cyber-security-capabilities.

"India's Response to China's Cyber Attacks." Accessed January 9, 2023. https://thediplomat.com/2019/07/indias-response-to-chinas-cyber-attacks/.

Iqbal Babar, Summar, Muhammad Nadeem Mirza, and Irfan Hasnain Qaisrani. "Evaluating the Nature of Cyber Warfare between Pakistan and India." *Webology* 18, no. 6 (2021): 6973-6985. ⟨halshs-03788162⟩.

Ireland, L. (2022). We are all (not) Anonymous: Individual- and country-level correlates of support for and opposition to hacktivism. New Media & Society, 0(0). https://doi.org/10.1177/14614448221122252The Daily Swig | Cybersecurity news and views.

Jain, Vishal. "The Challenge and Future of Cybersecurity in 2023." *The Times of India*. Accessed January 25, 2023. https://timesofindia.indiatimes.com/blogs/voices/the-challenge-and-future-of-cybersecurity-in-2023/.

Jung, Chauncey . "India Shows the World How to Use 'Cyberspace Sovereignty' Against China," The Diplomat, 2020, https://thediplomat.com/2020/07/india-shows-the-worldhow-to-use-cyberspace-sovereignty-against-china/

Kumar, Raksha. "Cyberattacks on Hospitals Thwart India's Push to Digitize Health Care." *NPR*, December 17, 2022, sec. Health. https://www.npr.org/sections/goatsandsoda/2022/12/17/1143396605/cyberattacks-on-hospitals-thwart-indias-push-to-digitize-health-care.

Mallick, Maj Gen P K. "Cyber Attack on Kudankulam Nuclear Power Plant." Vivekananda International Foundation, 2019. https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf.

"MeitY Organisations | Ministry of Electronics and Information Technology, Government of India." Accessed January 25, 2023. https://www.meity.gov.in/content/meity-organisations.

Ministry of Communication and Information Technology, and Department of Electronics and Information Technology. National Cyber Security Policy - 2013, Pub. L. No. 2(35)/2011-CERT-In (2013). https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf

Ministry of Electronics and Information Technology, Government of India, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021," Pub. L. No. G.S.R. 139(E) (2021), https:// mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20 Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

Ministry of Electronics and Information Technology, Government of India. "Cyber Surakshit Bharat Physical Training Programme," 2022. https://www.meity.gov.in/writereaddata/files/Cyber%20Surakshit%20Brochure_.pdf.

Ministry of Electronics and Information Technology, Government of India, "The Digital Personal Data Protection Bill, 2022" (2022), https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20 Data%20Potection%20Bill%2C%202022_0.pdf.

Ministry of Electronics and Information Technology, Government of India, "Indian Computer Emergency Response Team," accessed January 26, 2023, https://www.cert-in.org.in/

Ministry of Law and Justice. The Information Technology (Amendment) Act, 2008, Pub. L. No. DL-(N)04/007/2003-09 (2009). https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbu bubjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=.

"Ministry Of Personnel, Public Grievances and Pensions, G20 SECRETARIAT NEWSLETTER | January 2023." Accessed January 25, 2023. https://darpg.gov.in/.

Mistry, Urvin. "G- 20 India's Presidency and Cybersecurity Enterprises." *CyberPeace Foundation* (blog), January 17, 2023. https://www.cyberpeace.org/g-20-indias-presidency-and-cybersecurity-enterprises/.

Money Control. "India Saw 18 Million Cyber Attacks in First Quarter of 2022: Google's Royal Hansen." Accessed January 23, 2023. https://www.moneycontrol.com/news/business/india-saw-18-million-cyber-attacks-in-first-quarter-of-2022-google-executive-royal-hansen-9084911.html.

Naha, Alik. "Emerging Cyber Security Threats: India's Concerns and Options". International Journal of Politics and Security (IJPS), Vol. 4, No. 1, 2022, pp. 170-200, DOI: 10.53451/ijps.996755. All intellectual property righ "NIC-CERT GOVT OF INDIA." Accessed January 25, 2023. https://nic-cert.nic.in/.

National Cyber Security Centre, "Quantum-safe cryptography", NCSC: Whitepaper. 2020. Accessed February 10 2023. https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography

Nayak, Sudhansu. "Digital Personal Data Protection Bill 2022: Reservations and Recommendations," ORF, November 29, 2022, https://www.orfonline.org/expert-speak/digital-personal-data-protection-bill-2022/.

Outlook India. "Recent Cyber Attacks With Alleged Chinese Involvement That Targeted India's Critical Infrastructure." https://www.outlookindia.com/, December 2, 2022. https://www.outlookindia.com/national/recent-cyber-attacks-with-alleged-chinese-involvement-that-targeted-india-s-critical-infrastructure-news-241897.

Pandey, Devesh K. "Draft Cybersecurity Strategy Has Been Formulated: Centre." *The Hindu*, December 14, 2022, sec. India. https://www.thehindu.com/news/national/national-security-council-secretariat-formulated-draft-national-cyber-security-strategy-centre/article66262515.ece.

Rajan, Nandagopal. "Explained: How Ban of TikTok and Other Chinese Apps Will Be Enforced; the Impact for Indian Users," The Indian Express, 2020, https://indianexpress.com/article/explained/india-bans-chineseapps-impact-explained-6482150/

Rekhi, Dia. "India Set an Important Precedent by Banning TikTok: FCC Commissioner Brendan Carr," The Economic Times, January 2, 2023, https://economictimes.indiatimes.com/tech/technology/india-has-set-animportant-precedent-in-banning-tiktok-us-official/articleshow/96666862.cms?from=mdr

Rights Watch. "India: Data Protection Bill Fosters State Surveillance." *Human Rights*

Watch (blog), December 22, 2022. https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance.

Romagna, Marco & van den Hout, Niek Jan. (2017). Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats. Conference Paper, 27th Virus Bulletin International Conference, October 2017. Accessed via https://www.researchgate.net/profile/Niek-Jan-Van-Den-Hout/publication/320330579_Hacktivism_and_Website_Defacement_Motivations_Capabilities_and_Potential_Threats/links/5c1bc034a6fdccfc705cd71c/Hacktivism-and-Website-Defacement-Motivations-Capabilities-and-Potential-Threats.pdf

Saxena, Hansika, and Aastha Mittal. "Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022." CloudSek, n.d.

Schaefer, Kendra. "China's Corporate Social Credit System: Context, Competition, Technology and Geopolitics". U.S.-China Economic and Security Review Commission: Trivium China. 2020. Accessed February 10, 2023. https://www.uscc.gov/research/chinas-corporate-social-credit-system-context-competition-technology-and-geopolitics

Schulze, Matthias. "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations." In *2020 12th International Conference on Cyber Conflict (CyCon)*, 183–97. Estonia: IEEE, 2020. https://doi.org/10.23919/CyCon49761.2020.9131733.

SecAlliance (April 21, 2022). The Changing Landscape of Hacktivism. Accessed via https://www.secalliance.com/blog/the-changing-landscape-of-hacktivism.

Sharma, M.K. "India's Cyber Warfare Strategy in Next Decade," July 16, 2013.
    "Shri Ashwini Vaishnaw Launches 'Stay Safe Online' Campaign and 'G20 Digital Innovation Alliance' as Part of India's G20 Presidency." Accessed January 25, 2023. https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=1887114.

Sinha, Bhadra. "Don't Try Anyone under Invalid Sec 66A of IT Act, SC Raps Centre, States; Scraps Ongoing Cases," ThePrint (blog), October 12, 2022, https://theprint.in/judiciary/dont-try-anyone-under-invalid-sec66a-of-it-act-sc-raps-centre-states-scraps-ongoing-cases/1164801/.

Smeets, Max, and Herbert S. Lin. "Offensive Cyber Capabilities: To What Ends?" In *2018 10th International Conference on Cyber Conflict (CyCon)*, 55–72. Tallinn: IEEE, 2018. https://doi.org/10.23919/CYCON.2018.8405010.

Springer. "India Studies in Business and Economics." Accessed January 25, 2023. https://www.springer.com/series/11234.

SSO. "Stay Safe Online." Accessed January 25, 2023. https://staysafeonline.in/.

"Stop Ransomware | CISA." Accessed February 1, 2023. https://www.cisa.gov/stopransomware.

Studies, Institute of South Asian. "Going On The Offensive: India's Cyber Capabilities – Analysis." *Eurasia Review* (blog), December 30, 2022. https://www.eurasiareview.com/31122022-going-on-the-offensive-indias-cyber-capabilities-analysis/ .

"The Cyber Threat Facing Pakistan." Accessed January 18, 2023. https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/.

The Information Technology Act, 2000. Act No. 21 of 2000. New Delhi: Government of India, 2000. https://www.indiacode.nic.in/handle/123456789/1999#:~:text=An%20Act%20to%20provide%20legal,storage%20of%20information%2C%20to%20facilitate

The Week. "Inside Story of Cyber Attacks on India's Banks, Airlines, Railways… and the Fightback." Accessed January 23, 2023. https://www.theweek.in/theweek/cover/2022/01/06/inside-story-of-cyber-attacks-on-india-banks-airlines-railways-and-the-fightback.html.

Tomar, Sanjiv. "National Cyber Security Policy 2013: An Assessment." *Manohar Parrikar Institute for Defence Studies and Analyses* (blog), August 26, 2013.

Tribune News Service. "Cyber Attacks in India Triple in Last Three Years, but Security Funds Underutilised." *Tribune India News Service*. Accessed January 23, 2023. https://www.tribuneindia.com/news/nation/cyber-attacks-in-india-triple-in-last-three-years-but-security-funds-underutilised-457692.

United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment, 1996 : With Additional Article 5 Bis as Adopted in 1998 (New York : United Nations, 1999., 1999), https://search.library.wisc.edu/catalog/999878764902121.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina
Schwarzenbach. "National Cyber Power Index 2020," 2020.

"Wat is een botnet?" Accessed February 1, 2023. https://www.politie.nl/informatie/wat-is-een-botnet.html.

"What Is a Network Proxy? | Security Encyclopedia." Accessed February 1, 2023.
https://www.hypr.com/security-encyclopedia/proxy.

"What Is Cybersecurity? | CISA." Accessed February 1, 2023.
https://www.cisa.gov/uscert/ncas/tips/ST04-001.

"What Is E-Governance | IGI Global." Accessed February 1, 2023.
https://www.igi-global.com/dictionary/cyber-capability-framework/8702.

White, Joshua T. "After the Foundational Agreements: An Agenda for US-India Defense and Security
Cooperation," n.d.