INDIA'S CYBER LANDSCAPE: AN ASSESSMENT OF INDIAN EFFORTS SINCE INDEPENDENCE

Nageen Ashraf*

Abstract

India, as the world's largest digitally connected democracy, recognizes the critical importance of cyberspace in the face of evolving technological dynamics. With the second-largest global internet base, India emphasizes self-sufficiency to bolster cyber resilience and reduce dependence on foreign technology. This research explores India's historical efforts, spanning from the post-independence era to contemporary times, aimed at fortifying its cyberspace. The study delves into domestic measures such as the New Electronics Policy (NEP), IT Act 2000, and the National Cyber Security Policy, complemented by the establishment of key entities like the National Informatics Centre, CERT-In, Defence Cyber Agency, and National Task Force. The analysis extends to bilateral and multilateral collaborations, elucidating India's position as a global IT industry leader. Secondary resources of data, along with the Primary documents- including India's official policies- form the basis of this research, offering a comprehensive understanding of India's digital landscape.

Keywords: *Cyber threats, South Asia, Digital India, National Cyber Security Policy, Cyber warfare.*

Introduction

In an era where advancements are taking place at an unprecedented pace, it is not unfortunate for India to develop a strong cyberspace. Safeguarding national security encompasses a crucial aspect in the form of cybersecurity, prompting India to actively fortify its cyberspace for sustainability in the evolving global landscape. The imperative for India to cultivate a resilient cyberspace arises from various compelling reasons. First, the technologically evolving world calls for a well-protected cyberspace. Any state that does not focus on cyberspace during such

* An MPhil scholar at the School of Politics and International Relations (SPIR), Quaid-i-Azam University, Islamabad. The author can be reached at nageenashraf13@gmail.com and her areas of interest include geopolitics and security studies.

technological upheaval would surely have to bear consequences later on. Secondly, India intends to be a regional hegemon and such ambitions also demand India to have a robust cyberspace. Other than that, commonality of cyber-attacks occurrence, their ability to undermine state's security, and the enormous economic losses because of cyber-attacks are also among the reasons India should work harder on its cyber space.[1]

In order to mitigate the growing cyber threats, India has been trying to build its defensive as well as offensive cyber warfare capabilities. The South Asian security dilemma, which is taking place with respect to the great power competition between the USA and China, is a primary factor in India's pursuit of cyber warfare capabilities. China aims to become a cyber-super power with ambitions to counter the USA, and China's capabilities are causing insecurity within India. China has tried to reduce its reliance and dependency on US-based technology and has made efforts to produce its technology. The notion of "techno-nationalism" has granted China the status of one of the emerging cyber powers.[2] It has made its cyberspace strong enough for cyber-warfare against its opponents, especially the USA. China is preparing for full-fledged cyber warfare against its opponents.[3] In contrast to the USA's notion of "internet for all", China holds the view of cyber sovereignty, which is state-controlled cyberspace. And now, cyber space is considered one of the key drivers in China's pursuit of becoming a superpower.[4]

China's efforts have thus created a security dilemma within India. China has also been working on different areas, including AI and Quantum computing, to build its cyber warfare capabilities. China is expected to catch up with the USA and dominate the AI industries by 2030.[5] If China keeps working at the same pace, it will most likely to develop software that protects its systems from cyber-attacks from adversaries. Along with such defensive measures, China's pursuit of quantum computing will allow it to break well-established encryptions and get into the systems quickly. In addition, China is believed to be building a digital Silk Road, which means that China's technology and equipment are also being used in states

---

1 Sumeet Jindal, "Here's Why India Needs Strong Cyber Security Laws," *Newsroom Post,* July 20, 2021, https://newsroompost.com/opinion.

2 Adam Segal, "When China Rules the Web: Technology in Service of the State," *Foreign Affairs* 97 (2018): 10, https://cs.brown.edu/courses/csci1800/sources.

3 Jayson M. Spade, *China's Cyber Power and America's National Security*, Carlisle Barracks, PA: US Army War College, 2011, https://apps.dtic.mil/ sti/citations.

4 Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, USA, 2015.

5 Segal, 2018.

under the BRI project. The digital side of the BRI also encourages India to opt for a strengthened cyber space. These Chinese companies are also storing data of the population while also providing people with effective internet services.[6]

Such initiatives by China have challenged the US cyberspace and put China's rivals at greater risk, especially India. In 2020, India had a border stand-off with China. Other than that, the growing Chinese navy in the Indian Ocean is also a threat to India.[7] Therefore, it is beyond doubt that besides all these factors, China's cyber warfare capabilities also endanger India, considering their rivalry in multiple areas. The Sino-Indian War of 1962, the fight for regional dominance, the long-going border dispute, China's cordial relations with Pakistan and the 2020 Ladakh episode are pertinent reasons why China is perceived as a grave threat by India. Thus, India sees growing cyber capabilities across the border as a grave threat to its national security.[8] Therefore, this study aims to answer the research question, "What efforts has India taken to become one of the leading technological powers in the world?" In doing so, the paper considers major efforts by India at domestic and international levels since its independence. Some of the indicators of India's tech power include the success of Indian MNCs, and the development of technology start-ups in India. However, these indicators are not mentioned in the paper because they're out of the scope of this paper.

Efforts by India in Post-Colonial Era

Considering that India is a nuclear weapon state, cyber-nuclear nexus cannot be negated. Cyber-nuclear threats are on the rise, and the world has already witnessed the case of Stuxnet, a cyber-worm which was used to disrupt Iran's nuclear program. Being termed as the most sophisticated cyber weapon ever created, Stuxnet is an eye-opener, especially for the nuclear states all around the world. Moreover, the presence of terrorist groups in South Asia and their efforts to generate instability time and again also pose serious security challenges for India. Therefore, India has regarded cyberspace as a constituent of its national security.

Tracing back the history of India's IT sector, the influence of British policies and traditions over independent India remained for some time as far as the privacy and the IT sector of the state were concerned. Because of

---

6 Segal, 2018.

7 Joshua T. White, "After the Foundational Agreements: An Agenda for US-India Defense and Security Cooperation," *Brookings Institution* (2021), https://www.brookings.edu/wp-content/uploads/2021/01.

8 Mike Hamilton, "India: A Growing Cybersecurity Threat," Dark Reading, December 2020, https://www.darkreading.com/threat-intelligence.

strict restrictions and surveillance over its citizens during the colonial period, Indian government asserted same control over its citizens in the postcolonial period. However, when the economic condition worsened because of centralization of government, India realized that opening up economy and IT sector could help the devastating economy improve. Finally in the time period of Indira Gandhi several initiatives were taken to open up the IT market, which were then extended by her son Rajiv Gandhi. Similarly, more economic reforms were taken by Narasimha Rao to open up the market. Afterwards from time to time, different governments have tried to send their fiscal support to the IT industry including the grant of subsidies and resource allocation.[9]

National Informatics Centre 1976

The establishment of NIC was one of the milestones in India's shift towards e-governance. One of the main objectives of this initiative was to assist the government in e-governance[10], and it was successfully achieved its objective to a great extent. One of NIC's achievements was the Asian Games in 1982, which New Delhi hosted. All the clerical work in those games was computerized, and locally made software by NIC along with locally made computers were used.[11] Along with this, the center has played a decisive role in incorporating e-governance applications within India on national as well as district level.[12]

New Electronics Policy (NEP) 1984

Indian government realized the need for the state to build up its IT sector and thus slackened many restrictions on the private firms, uplifting them to become self-sufficient. One such initiative was taken in 1967, known as The Electronics Corporation India Limited, which aimed at producing computers without the help of external partners. Likewise, The New Electronics Policy was also one of the initial efforts taken towards the openness of the market. It was a landmark step taken to allow private industries to take hold of the market, unlike India's previous government centric policies. The policy also encouraged the imports of technology

---

9 Thomas Barnes. "The IT Industry and Economic Development in India: A Critical Study," *Journal of South Asian Development* 8, no. 1 (2013): 61-83. https://journals.sagepub.com/doi/abs/10.1177.

10 Vaidyeswaran Rajaraman, "History of Computing in India: 1955-2010," *IEEE Annals of the History of Computing* 37, no. 1 (2015): 24-35. https://ieeexplore.ieee.org/

11 Rajaraman, 2015, 28.

12 Shweta Ghate, and Pragyesh Kumar Agrawal, "A Literature Review on Cyber Security in Indian Context," *J. Comput. Inf. Technol* 8, no. 5 (2017): 30-36.

from the West [13] and allowed the private companies of India to manufacture telecommunications equipment.[14] It was a comprehensive policy that encompassed four major aims of technology exchange, computer imports for governmental departments, facilitate the return of expatriate Indian technicians, and the establishment of Export Processing Zones.[15]

National Task Force on IT and Software Development 1998

In 1998, the then-prime minister of India, Atal Behari Vajpayee, established a task force in order to facilitate the Indian government in becoming a global superpower in the field of information security and technology.[16]The task force was entrusted with the task of developing National Informatics Policy's draft and also aimed at facilitating the implementation of NIP and helped the government in strengthening the IT industry. Even today, India has asserted the importance of self-sufficiency in the technological domain. In an interview, India's Union Minister Ashwini Vaishnaw opined, "We aim to make India a tech export engine," with ambitions to make India lead the 6G. [17]

These steps were three of the important initial efforts to prioritize the IT sector and move towards digitalization. These initiatives helped India to attain self-sufficiency to a greater extent. In contemporary times, India has continued to be one of the leading exporters of IT at the global level. Between March 2022 and 2023, its IT exports were worth $230 billion, making around 11 % of the global computer and IT exports.[18] Initially, working on cyberspace aimed to mitigate the economic losses caused by cyber-attacks. In addition, the initiatives taken focused more towards the privacy of the citizens and did not view cyber space as a national security concern. It was not until Mumbai attacks that India

---

13 Biswajit Dhar, and Reji K. Joseph. "India's Information Technology Industry: A Tale of Two Halves," *Innovation, Economic Development, and Intellectual Property in India and China: Comparing Six Economic Sectors* (2019): 93-117.

14 Ramesh Subramanian, "Historical Consciousness of Cyber Security in India," *IEEE Annals of the History of Computing* 42, no. 4 (2020): 71-93.

15 Biswajit Dhar, and Reji K. Joseph, "India's Information Technology Industry: A Tale of Two Halves."

16 AnnaLee Saxenian, "Bangalore: The Silicon Valley of Asia?" *Center for Research on Economic Development and Policy Reform,* February, 2001, https://www.researchgate.net/profile.

17 Gulveen Aulakh and Subhash Narayan, "We Aim to make India A Tech Export Engine: Ashwini Vaishnaw," *Mint,* November 26, 2023, https://www.livemint.com/news/india.

18 "India: The World's Newest Economic Superpower," *Foreign Affairs,* September 7, 2023, https://www.foreignaffairs.com/sponsored-gmi-india.

realized that cyber space can also become a serious threat to states' physical security.[19]

Efforts by India in the 21st Century

India has broadened its cyber landscape during escalating cyber espionage incidents. It has been thinking of institutionalizing cyber warfare in order to gain superiority in the region using this asymmetric warfare.[20] India, like all other states, is concerned about economic growth as well as the risks and vulnerabilities associated with the cyberspace.[21] With time, India has managed to become one of the strongest IT industries in the world. It was labelled as a recognized IT superpower in the early 20th century [22] and continues to be the leader of IT and IT-enabled services.[23] Some have even labelled it as the "tech- super power",[24] which is also an emblem of India's resilient digital landscape. Some major efforts taken by India in the last two decades have played a major role in making India a leading cyber-power. These initiatives include the following.

The Information Technology Act, 2000

India came up with the information technology act in 2000 whose major objective was to amend and update previous acts in accordance with the changing technological environment. The act is also considered as a fundamental law that deals with e-commerce and cybercrimes[25] The Act is a detailed framework that defines cyber and computer related terms along with the crimes and their punishments. Critics argued that IT Act 2000 undermined the citizen's right to privacy in the name of regulation of space.[26] The Act was then amended in the year 2008 to address some loopholes that were present in the 2000 Act. The Act was criticized because despite being a landmark act that put spotlight on many key

---

19 Swaran Singh and Jayanna Krupakar, "Indo–US Cooperation in Countering Cyber Terrorism: Challenges and Limitations," *Strategic Analysis* 38, no. 5 (2014): 703-716.

20 Pukhraj Singh, "Battle-Ready for the Fifth Dimension: Assessing India's Cyber-Defence Preparedness," *Jindal Journal of International Affairs* 1, no. 1 (2011): 339-351, https://jgu-dev.s3.ap-south-1.amazonaws.com.

21 Sameer Patil, "India's Lead on Cyber Space Governance, " *Gateway House,* August 15, 2018, https://www.gatewayhouse.in/india-cyber-space-governance.

22 Luke Harding, "India: The New IT Superpower," *The Guardian,* 2000. http://www.theguardian.com/technol ogy/2000/

23 "India: The World's Newest Economic Superpower," 2023.

24 Ernestas Naprys, "India's on Fast Track to Tech Superpower Status," *Cybernews,* 12 December 2023, https://cybernews.com/editorial.

25 *Information Technology Act* 2000, India, http://www.mit.gov.in/ itbill.asp.

26 Subramanian, 2020.

issues, the act failed to address the preventive measures needed to be taken to make cyber-attacks unsuccessful. The government mostly tried to retain supremacy over the internet and cyber space by citing the external cyber security threats.[27] Critics also argued that the 2000 IT Act paid no attention towards the cyber-crimes and was more inclined towards issues related to e-commerce, but the loopholes were somehow covered in the amended IT Act of 2008.

CERT-IN- 2004

At the organizational level, the Indian Computer Emergency Response Team (CERT-In)- established in 2004- remains one of the most dominant institutions as it is a major national agency which is responsible for the collection, monitoring, coordination, analysis, and dissemination of information.[28] The IT Act did not address the prevention of cyber breaches, and dealt only with the consequences of a digital breach. In this regard, the Response Team was assigned the task of blocking malicious websites as a preventive measure as an attempt to address the insufficiency of the IT Act.[29] The team is also responsible for helping out citizens with regard to technical assistance as well as the recovery of their systems from the cyber-attacks. It has also played a role in raising awareness among people as far as cyber security is concerned.[30]

National Cyber Security Policy 2013

Even though the inclination towards digitalization in India began in the era of Rajiv Gandhi, but 2013 was the year of major achievements for India in the cyber domain.[31] The first ever cyber security policy in India was formulated in 2013. The main objective of this policy was to create a safe and secure cyber environment in the state and to protect the state from cyber-attacks and cyber espionage. The policy puts forward the guidelines as well as strategies for securing cyber space and creating an

---

27 Subramanian, 2020.

28 E. Dilipraj, and Ramnath Reghunadhan, "Organisational Governance of Cyber Space in India," *Journal of Air Power and Space Studies* 13, no. 1 (2018): 115-134. https://capsindia.org/wp-content/uploads/

29 Subramanian, 2020.

30 M. Tariq Banday, and Farooq Ahmad Mir, "A Study of Indian Approach towards Cyber Security," In *2012 1st International Conference on Emerging Technology Trends in Electronics, Communication & Networking*, 1-6. IEEE, 2012. https://ieeexplore.ieee.org/abstract/document/6470114/.

31 E Dilipraj, "India's Cyber Security 2013: A Review," *Centre for Air Power Studies* 97, no. 14 (2013): 1-4, https://capsindia.org/wp-content/uploads.

invulnerable cyber ecosystem.[32] Along with this policy, other achievements for India included being labeled as an "Authorizing state" when previously it was a consumer state.

The national cyber security policy was a landmark step taken by the Indian government to protect cyberspace, but many loopholes still that need to be addressed. There is a need to update the 2013 national cyber security policy keeping in view the inevitability of cyber warfare and the technological advancements that have taken place over time.[33] Other than the problem of implementation of policy nationwide, one of the major issues is that the policy does not look at cyberspace as a form of warfare; rather it focuses on securing the data of individuals and organizations.[34] Another problem is that the policy does not consider cyber security as an important element of nuclear security.[35] Being the first ever such policy, the policy was abstract but it nonetheless guided the creation of different institutions like National Critical Information Infrastructure Protection Centre which makes up the digital landscape of India.

National Cyber Security Policy- 2020

In 2020, India updated the national cyber security strategy to broaden the cyber landscape and to address the growing vulnerabilities. The three goals- as mentioned in the National Cyber Security Policy 2020- are to secure, strengthen, and synergize the digital landscape of India.[36] This will be done by ensuring the security of public services, supply chains, critical infrastructures, small businesses, and digital payments. Moreover, the policy also aims to ensure the preparedness of different sectors in cyber domain in order to secure cyber space at national level. At the same time, it lays down options to deal with the digital transformations.[37] As far as the pillar of strength is concerned, the policy lays down an ambition to strengthen institutions, structure, governance, research, innovation, capability, assurance, audit, crisis management, and data security. Thirdly, the policy also aims to synergize human and institutional resources in

---

32 Pulkit Mohan, "*Ensuring Cyber Security in India's Nuclear Systems*," Observer Research Foundation, 2020, https://www.orfonline.org/wp-content/uploads/2020/10/ORF.

33 Arun Sukumar, and R. K. Sharma, "The Cyber Command: Upgrading India's National Security Architecture," ORF Special Report 9 (2016). https://orfonline.org/wp-content/uploads/2016/03.

34 Sukumar and Sharma, 2016.

35 Pulkit Mohan, *Ensuring Cyber Security in India's Nuclear Systems.*

36 Data Security Council of India, *"National Cyber Security Strategy 2020,"* https://www.dsci.in/files/content/knowledge-centre/2023.

37 National Cyber Security Strategy 2020*,* 2020.

order to mitigate cyber threats and to achieve overall objectives of a regulated and well-governed cyber space.[38]

Digital India 2015

Reports show that internet penetration and the use of smartphones grew exponentially in the past decade and are still expected to rise the same way.[39] Because India's reliance on the internet has been increasing rapidly, the government of India took the initiative of approving the national e-governance plan in 2006. Later on, the authorities decided to transform Indian society digitally and came up with a plan for "Digital India" in 2015.[40] The landmark step taken by the government of India is aimed at allowing citizens to have access to high-speed internet, safe and secure cyberspace, as well as digital literacy.[41]

Under the umbrella of Digital India, another initiative was taken known as Cyber Swachhta Kendra. It is a Botnet cleaning and malware analysis center which aims at the detection of botnet infections, notifying users about them and guiding users to secure their systems.[42] Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA) is another program launched in 2017 under Digital India and it aims to have at least one digitally literate individual in every household in order to have skills reuired to compete in the growing digital ecosystem.[43] The major aim of this initiative was to bridge the gap between urban and rural areas by making individuals learn how to run devices like PC, cellphones, and tablets so they can in turn help in the nation-building of the state.[44] Through this program and its implementation, India has become one of the leading states in the world to use technology for the improvement of socio-economic conditions of its citizens.[45]

---

38 National Cyber Security Strategy 2020, 17.

39 Aditya Bharadwaj, "Assessing India's Preparedness, *Wild Blue Yonder*, 2020, https://media.defense.gov/2020/Jul/21/2002460417/.

40 Sumanta Bhattacharya, and Bhavneet Kaur Sachdev, "Can India be Successful in Achieving a Digital Economy and its Vision of Digital India: A Case Study," *International Journal of Innovative Research in Science, Engineering, Technology IJIRSET*, Vol 10: 11 (2021), https://www.researchgate.net/profile.

41 Digital India, July 2, 2023, https://digitalindia.gov.in/.

42 Cyber Swachhta Kendra, June 20, 2023, https://www.csk.gov.in/.

43 Aanandita Gahlot, and Shubhankar Gahlot, "Changing the State of Literacy in the Digital Age in India," *EPIC Series in Education Science* 3 (2020): 98-107, https://d1wqtxts1xzle7.cloudfront.net.

44 Gahlot, 2020.

45 Sumanpreet Kaur, and Sajad Ahmad Mir, "Digital India: An Analysis of its Impact on Economic, Social, and Environmental Sectors," *Neuroquantology* 20, no. 22 (2022): 2551-2561, https://www.researchgate.net/profile.

Defense Cyber Agency (DCA)- 2018

Previously, there have been agencies and bodies that used to deal with civilian cyber security concerns. But, in 2018, India initiated the establishment of a specialized body focused on addressing the military aspects of cybersecurity. This initiative aimed to safeguard India's digital infrastructure from foreign hackers, fostering collaboration among the navy, military, and air force. The creation of the DCA aimed to enhance collective efforts in countering cyber threats, with a particular focus on adversaries such as Pakistan and China.[46] Other than that, the agency was also expected to work towards the formulation of a cyber-warfare doctrine.[47] It was a major step because it indicates India's seriousness towards the weaponization of cyberspace as a major tool for 5th generation warfare.[48]

India's Cooperation in Cyber Domain

As an effort to boost up its cyber capacity in the times of increasing relevance of cyber space in international relations, India has signed different bilateral agreements with Russia, USA, and Israel as well as multilateral agreements with regional organizations like EU and ASEAN.[49] In the years between 2000 and 2017, India signed almost 100 cyber-agreements that were either directly related to cyber- security or indirectly aimed at cyber-security.[50] It has also participated in different sessions of UN-GGE where it encouraged that states should cooperate with each other in this new realm of warfare in order to mitigate the growing cyber threats. UN Group of Governmental Experts (UN-GGE) was an international platform created to develop a framework for global cyber governance. The efforts started in 2004 but so far had not been able to bear fruit because of disagreement of major powers over the control and regulation of cyber space and the applicability of International humanitarian Law.[51] However, in the 6th session of 2021, major powers

---

46 ANI, India Set To Get Defence Cyber Agency to Fight Pak, Chinese Hackers, *NDTV*, (April 30, 2019), https://www.ndtv.com/india-news/.

47 Gunjan Chawla, "India's New Defence Cyber Agency—II: Balancing Constitutional Constraints And Covert Ops?" *Medianama,* https://www.medianama.com/2019/10/.

48 Nidhi Singh, India's New Defence Cyber Agency.

49 Sameer Patil, India's Lead on Cyber Space Governance.

50 Hannes Ebert,"Hacked IT Superpower: How India Secures its Cyberspace as a Rising Digital Democracy," *India Review* 19, no. 4 (2020): 376-413. https://www.tandfonline.com/doi/full/10.1080.

51 Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace," *Just Security* (2021), https://centaur.reading.ac.uk/98699.

came to the same page to tackle this growing cyber threat all over the world.

In contemporary times, India has bilateral strategic cyber dialogues with over 10 countries. Moreover, it has signed myriad cyber MoUs, agreements and joint statements with a further 40-odd countries.[52] These cyber collaborations have helped India build its offensive cyber warfare capabilities.[53] Even though the collaboration in cyber space is not necessarily aimed at offensive capabilities, the collaboration has helped India improve its offensive cyber capabilities because of access to advanced technology, exchange of technical expertise, and enhancement of skills and training programs. Along with these agreements, India's Land Warfare Doctrine of 2018 also mentioned the readiness of the Indian Army in the cyber landscape. The doctrine asserts, "The Indian Army will enhance capabilities to address the challenges of non-contact domains of conflict viz cyber, space and information as a component of our National strategy for non- contact warfare to cause unaffordable losses to potential adversaries."[54] With regards to building offensive cyber capabilities, the doctrine acknowledges that cyber warfare has become another domain of competition, which is why India will make efforts to strengthen its cyber deterrence along with capabilities of eliminating cyber threats from the adversaries.[55]

India-USA India and USA have been the defense partners for a very long time and security is an integral part of Indo-US bilateral ties.[56] The Indo-US cooperation in the technological field dates back to as early as 1980s when both the states signed a memorandum of understanding mainly aimed at the exchange and transfer of technology.[57] 9/11 attack and the Mumbai attacks brought US and India on the same page for their fight against terrorism. Both the attacks also highlighted the vulnerabilities of cybercyber space and its exploitation by terrorist groups. Therefore, it was believed that cyber cooperation between both the states

---

52 Cherian Samuel, and Munish Sharma, *India's Strategic Options in a Changing Cyberspace*, New Delhi: Pentagon Press LLP, 2019, https://idsa.in/system/files/book/

53 Ammad Farooq, and Ahmad Ali, "India's Growing Cyber Partnerships and Challenges for Pakistan," *Margalla Papers 26* (2): 49-61. (2022), https://doi.org/10.54690/margallapapers.26.2.121.

54 Indian Army, "*Land Warfare Doctrine- 2018,*" *SSRI*, https://www.ssri-j.com/MediaReport/Document/

55 "*Land Warfare Doctrine- 2018,*" 10.

56 Cara Abercrombie, "Realizing the Potential," *Asia Policy* 14, no. 1 (2019): 119-144, https://www.jstor.org/stable/26642266.

57 Steven R. Weisman, "U.S.-India Technology Accord Gains," *The New York Times* . (May 4, 1985), https://www.nytimes.com/1985/05/04/world.

would be fruitful; however, before 9/11 took place, initiatives had already begun that focused on cyber security. India and USA established India–US Cyber Security Forum Initiative in 2001 which fostered the exchange of expertise in the specific domain. Under the forum, India improved its cyber capabilities to a good extent. In fact, the development of CERT-In, (one of the first steps taken by Indian govt. to secure cyber space) was also a fruitful result of US-India cyber cooperation. With the passage of time, the forum also helped CERT-In to work on variety of areas, covering different issues like detection of malware, cyber forensics, and cyber terrorism.[58]

While India possesses commendable cyber-intelligence capabilities, its comprehensive understanding often leans on collaboration with the United States. The initiation of cyber security cooperation in the early 2000s faced a setback when an incident revealed that certain individuals from India were involved with US intelligence, leading to a decline in trust between the two nations and hindering further collaboration.[59] But then, finally, in 2011, a memorandum of understanding was signed, which again boosted the technological and information exchange.[60] Indo-US cooperation in the field of defense and security will be beneficial for both US and India. In 2018, a Memorandum of Understanding[61] was also signed in the cyber domain, which was similar to the MoU signed between both in 2011.[62]

India-EU

The European Union and India have some converging interests. Keeping in view the fact that India is working towards digitalization of the state under its program "Digital India", and EU is working on the "Digital Single Market", there is a lot of room for cyber cooperation between both the states. When both the states set the EU-India agenda for Action 2020,

---

58 Swaran Singh and Jayanna Krupakar, "Indo–US Cooperation in Countering Cyber Terrorism: Challenges and Limitations."

59 Srijith K. Nair, "The Case for an India-US Partnership in Cybersecurity," *Takshashila Institution, Inde* 14 (2010) https://takshashila.org.in/s/India-US-cybersecurity.pdf.

60 Mahrukh Khan, "Growing India-US Strategic Cooperation," *Strategic Studies* 37, no. 4 (2017): 97-117. https://www.jstor.org/.

61 A MoU (Memorandum of Understanding) is a nonbinding agreement between two or more states outlining the terms and details of an understanding, including each party's requirements and responsibility; it is often the first stage in the formation of a formal contract.

62 "India And US Sign Memorandum Of Understanding To Continue Cooperation In Cyber Security," *First Post,* January 12, 2017, https://www.firstpost.com/tech/news-analysis/.

cyber security was one of the key areas that were given importance. Along with that, both states also encouraged the exchange of technology and expertise in the domain of cyber security.[63] EU published its cyber security strategy in 2020 which highlights the importance of cyber collaboration with other states. In this regard, India is an essential partner. The European Union also conducted its sixth cyber dialogue with Delhi prior to releasing its cyber security strategy. In the dialogue, both the parties agreed to enhance cyber cooperation and capacity building measures.[64]

India-New Zealand

According to the Ministry of External Affairs, the first dialogue between India and New Zealand was held in 2017 in which both the states focused on deepening their ties in the cyber domain.[65] Both sides encouraged that cyberspace should be made free and secure and more economical and innovation should be brought in the domain. Similarly, after 2017, various talks were held between India and New Zealand, and cyber security remained an important element of the discussions. In May 2021, a virtual meeting was also held in which both sides agreed to enhance depth in the sectors of security, defense, climate change, cyber security and counterterrorism.[66] Other than these states, India has also been collaborating with Israel, Japan, Russia, UK, and Australia in the cyber domain. Additionally, India's membership in minilateral groupings like QUAD and BRICS has also enabled it to fortify its cybercyber space.

India's Digital Terrain: An Evaluation

The overall position of India in cyber space remains contested. Because of the initiatives taken to strengthen its cyber space, India was ranked 10th in Global Cyber Security Index in 2020 as per a report by International Telecommunication Union (ITU).[67] It is a landmark

---

63 Patryk Pawlak, "EU-India Cooperation on Cyber Issues: Towards Pragmatic Idealism?" *Gateway House,* (2016) https://www.gatewayhouse.in/wp-content/uploads.

64 Ministry of External Affairs, 6th India-EU Cyber Dialogue (New Delhi: Press Release, 2020), https://www.mea.gov.in/ press-releases.htm?dtl/33308/

65 Ministry of External Affairs, India-New Zealand Cyber Dialogue, New Delhi (November 27, 2017) https://www.mea.gov.in/press-releases.htm?dtl/ 29140/

66 India, New Zealand decide to enhance depth of engagement in key areas, (2021), *The Economic Times.* https://economictimes.indiatimes.com/news/ defence/india-new-zealand.

67 International Telecommunication Union "*Global Cybersecurity Index 2020,"* https://www.itu.int/dms_pub/itu-d/opb/str/

achievement for India because in 2018, India was ranked 47th in the list.[68] According to research conducted by a UK think tank (International Institute for Strategic Studies), there are seven factors[69] that determine the cyber capabilities of a state. Assessment of these factors indicates that India lies in the third tier of states having cyber power capabilities,[70]which means that there are some factors that still need improvement and some factors that show India's potential strength.[71] In contrast, according to the National Cyber Power Index of 2022, India is not among the cyber powers of 2020 as well as 2022.[72] In fact, India is not even among the top 10 cyber powers of 2020 and 2022, making India's position and capabilities contested in cyber space.

Despite various efforts, India remains the most vulnerable states to cyber-attacks. The Stuxnet, which is mainly associated with Iran, also affected around 10,000 Indian computers and targeted some critical infrastructure computers as well. Had the virus activated itself on those systems, the oil and power sectors of the state would have been crippled.[73] Analyzing the reports from 2019, almost 70% companies in India had to face serious consequences of the cyber-attacks. Most of these attacks were significant enough to create grave economic losses to the state. But again, this does not signify that India has a weak cyber space because the more digitalized a state is, the more vulnerable it becomes. Data suggests that from 2006 to 2020, India was the 3rd state in the world with most cyber-

---

68 Sandhya Sharma, "India Breaks into Top 10 Countries on UN's Index Measuring Commitment to Cybersecurity, *The Economic Times. June 29, 2021, https*://economictimes.indiatimes.com/news/defence/.

69 The assessment measures a country's cyber abilities on seven parameters — strategy, governance and control of cyber capabilities, core cyber-intelligence capability, cyber empowerment and dependence, cyber security and resilience, global leadership in cyberspace affairs, and offensive cyber capability.

70 "*Cyber Capabilities and National Power: A Net Assessment,*" International Institute for Strategic Studies, June 28, 2021, https://www.iiss.org/en/research-paper/2021/06/cyber-power---tier-three/

71 Regina Mihindukulasuriya, "India's Offensive Cyber Capability More Focused on Pakistan than China, UK Think Tank Says," *The Print,* June 28, 2021, https://theprint.in/india/indias.

72 Julia Voo, Irfan Hemani, and Daniel Cassidy, "Nationl Cyber Power Index 2022," *BELFER Centre for Science and International Affairs,* September 2022, https://www.belfercenter.org/sites/default/files/files/publication/.

73 E Dilipraj, "India's Cyber Security 2013: A Review."

attacks aimed at government agencies.[74] Additionally, India had to suffer a loss of Rs. 1.25 trillion in 2019 and a loss of $6 trillion during the pandemic year 2020 because of cyber threats.[75] In the initial months of 2022, India saw a tremendous increase in its cyber security incidents, with 674,000 incidents taking place.[76] From 2021 to September 2023, India witnessed an increase of 278% in cyber-attacks sponsored by state actors alone.[77] This highlights that despite many efforts, Indian cyber space and government organizations are still vulnerable to cyber-attacks and more efforts are needed in order to lower the occurrence of such incidents.

Overall, India's cyberspace is not as strong as it should be. India behind in its cyber security compared to other cyber powers, even though it has a massive population of internet users. Even though the rise in the internet has been slow in India compared to other states, India has been paying less attention to its cyberspace. But since offensive capabilities in cyberspace are more effective than one's defensive capabilities, no matter how defensive a system gets, it will always be vulnerable to foreign attacks because defensive primacy cannot be applied to even the strongest nations like the US, China and Russia.[78]

One can argue that just because India has been trying to strengthen its cyberspace, does not mean it possesses cyber warfare capabilities since it comprises intense attacks and operations. But, looking at the definition of cyber warfare provided by Clarke and Knake, cyber warfare means the "actions by a nation-state to penetrate another nation's computers or networks to cause damage or disruption."[79] From this perspective, it is clear that since India can enter the adversaries' information systems and disrupt them, it also has cyber warfare

---

74 Carmen Ang, "The Most Significant Cyber Attacks from 2006-2020, by Country," *Visual Capitalist* 4 (2021), https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/s.

75 N. Singal, "Increasing cyber-attacks show why stringent cyber-security laws are need of the hour, *Business Today,*" (2021) https://www.businesstoday.in/technology/news/

76 Muqbil Ahmar, "Cybersecurity: How does India Perform at the Global Stage?" Economic Times, April 20, 2023, https://cio.economictimes.indiatimes.com/news/digital-security/

77 The Wire Staff, "State-Sponsored Cyber Attacks Against India Went Up by 278% Between 2021 and September 2023: Report," *The Wire,* 6th November, 2023, https://thewire.in/tech/

78 Kartik Bommakanti, "India's Cyber Defence Capabilities: Their Role in Net-Centric Warfare," In *The Routledge Handbook of Indian Defence Policy*, 367-377, Routledge India, 2020.

79 Richard A. Clarke. and Robert Knake, "Cyber War: The Next Threat to National Security and What To Do About It," Ecco, 2011.

capabilities. India is in its initial phases, but the state has enough human and technological resources to become one of the major cyber actors worldwide in a few years.[80]

Conclusion

As an emerging tech giant, India has greatly improved its cyber capabilities in the past few decades. The initial efforts to boost the state's cyber security and IT sector started back in the time period of Rajiv Gandhi. After that, successive governments tried to keep up with the state's IT sector. Many steps have been taken, and various policies have been developed to make India self-reliant regarding technological equipment. This has helped India become one of the leading IT industries in the world and encouraged India to expedite its national cyber security efforts in defensive and offensive domains. In this regard, its collaboration with other second-tier cyber powers, including the USA and Israel, has allowed it to develop resilient cyberspace by incorporating offensive cyber capabilities. At the same time, despite all these efforts, the facts and figures presented in the paper justify that India remains one of the most vulnerable states in the world in terms of cyber-attacks, leaving room for further efforts towards a resilient cyberspace.

[80] John Leyden, "Indian Cyber-Espionage Activity Rising Amid Growing Rivalry With China, Pakistan," *The Daily Swig,* Feb 25, 2021, https://portswigger.net/daily-swig.