IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

India's Cyber Diplomacy: Shaping Global Alliances For A Secure And Resilient Future

RAJ GOHEL

PhD Research Scholar

School of International Studies & Diaspora, Gujarat University

Abstract:

India's increasing significance in the worldwide digital environment has emphasized the need for cyber diplomacy as a fundamental element of its international relations strategy. This article examines India's growing role in cyber diplomacy, emphasizing its efforts to form global alliances to ensure a secure and resilient cyberspace. Through an analysis of India's bilateral and multilateral activities, the article emphasizes significant projects and agreements that demonstrate India's dedication to promoting international cooperation in the field of cybersecurity. Furthermore, the study analyzes the obstacles that India encounters, such as the delicate equilibrium between national security concerns and the imperative for transparency and collaboration in the realm of cyberspace. An analysis of India's cyber dialogues with key powers including the United States, European Union, Japan, and Australia, together with its involvement in international forums such as the United Nations and the BRICS alliance, reveals how India is establishing itself as a frontrunner in influencing the global cyber governance framework. At its core, this paper contends that India's proactive cyber diplomacy is essential for tackling the intricate issues of the digital era and for constructing a secure, robust, and inclusive global cyberspace.

Keywords: Cyber Diplomacy,Digital Diplomacy, Foreign Policy, Global Cyber Alliances International Governance,India-US Relations,Multilateral Cyber Engagements

Introduction

Cyberspace has become a crucial sphere in the 21st century, exerting influence on all aspects of global security, economic stability, and diplomatic relations. In an era of growing global interconnectivity facilitated by digital networks, the imperative for strong cybersecurity protocols and international collaboration has reached critical levels. A wide range of cyber threats, including espionage, cybercrime, and state-sponsored attacks, present substantial dangers to national security, economic progress, and the operation of life-sustaining infrastructure. Within this particular framework, cyber diplomacy has emerged as a crucial element of a country's foreign policy, functioning as a forum for communication, collaboration, and the creation of standards and regulations in the realm of cybersecurity.

India's fast-expanding digital economy and large number of internet users place it at a critical juncture in influencing the global cyber environment. Given its position as a prominent IT powerhouse and a significant participant in the worldwide digital economy, India's strategy towards cyber diplomacy is of utmost

importance, not just for its own national security and economic concerns but also for the stability and security of the global digital ecosystem. The nation's overarching foreign policy goals guide its cyber diplomacy approach, encompassing the promotion of a peaceful and secure global atmosphere, the advancement of economic growth, and the equitable distribution of the advantages brought about by the digital revolution.

India's cyber diplomacy endeavors have undergone substantial development in the last ten years, mirroring its growing involvement in international cyber governance and its aspiration to assume a leadership position in influencing worldwide standards for cybersecurity. This study examines the specific aspects of India's cyber diplomacy, including its interactions with other countries, the obstacles it encounters, and the potential prospects that loom in the future. This study aims to provide a comprehensive understanding of India's efforts to establish global partnerships and create a secure and resilient cyberspace by examining its cyber dialogues with key global actors, including the United States, the European Union, Japan, and Australia, as well as its involvement in international forums such as the United Nations and BRICS.

India's proactive approach to cyber diplomacy highlights its acknowledgment of the need for cooperation in tackling the intricate issues of the digital era. In light of the ongoing evolution and increasing complexity of cyber threats, it is imperative for India to establish robust international alliances to safeguard not just its own cybersecurity but also that of global society. This study posits that India's cyber diplomacy is not solely a reaction to urgent challenges but rather a proactive approach intended to influence the trajectory of global cyber governance. India is strategically employing cyber diplomacy to establish a digital future that is both secure and resilient, while also promoting inclusivity for itself and the global community.

India’s Cyber Policy Framework

India's cyber policy framework is a comprehensive strategy aimed at tackling the complexities and possibilities presented by a swiftly changing digital environment. Given the country's growing integration into the global digital economy, the need for strong cybersecurity measures has become more pressing. India's cyber policy framework demonstrates its dedication to safeguarding its digital infrastructure, guaranteeing the security of its citizens' data, and establishing itself as a frontrunner in worldwide cyber governance.

National Cyber Security Policy (NCSP) 2013

The National Cyber Security Policy (NCSP) 2013 is a fundamental pillar of India's cybersecurity policy plan. The National Cybersecurity Strategy Program (NCSP), initiated by the Ministry of Electronics and Information Technology (MeitY), seeks to establish a secure and robust online environment for individuals, enterprises, and the government. The initiative delineates the imperative of safeguarding critical information infrastructure (CII) from cyber threats, augmenting the capacity to avert and address cyber incidents, and cultivating a cybersecurity-oriented culture through consciousness and education.

The National Cybersecurity Strategy (NCSP) promotes the establishment of public-private partnerships and cooperation across diverse forces such as academia, industry, and civil society to strengthen India's cybersecurity ecosystem. Furthermore, the strategy underscores the need for research and development in cybersecurity technology and promotes the creation of a strong legal and regulatory structure to tackle developing cyber risks.

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)

Established in 2017, the Cyber Swachhta Kendra, also referred to as the Botnet Cleaning and Malware Analysis Centre, is a project within the Ministry of Information and Technology (MeitY) with the objective of offering tools and resources to counteract botnets and malware. This part of India's wider endeavor to safeguard its cyberspace, this programme provides free tools for identifying and eliminating malware from personal computers and mobile devices.

The Cyber Swachhta Kendra partners with internet service providers (ISPs), antivirus firms, and other relevant parties to guarantee the efficacy and broad availability of the solutions offered. This effort serves the dual purpose of safeguarding the digital assets of individuals and companies, while also making a significant contribution to the general mitigation of cyber risks within the nation.

National Critical Information Infrastructure Protection Centre (NCIIPC)

Established under the Information Technology Act, 2000, as modified in 2008, the National Critical Information Infrastructure Protection Centre (NCIIPC) is responsible for protecting critical information infrastructure (CII) in India. Critical Infrastructure Infrastructure (CII) encompasses the fundamental assets and systems necessary for the operation of the economy and national security, including those associated with banking, communications, energy, and defense industries.

The mission of NCIIPC is to identify Critical Infrastructure Infrastructure (CII) assets, evaluate their susceptibility to cyber threats, and collaborate with stakeholders to establish preventative measures. An essential function of the center is to guarantee the resilience of India's key infrastructure against cyberattacks, which can have grave implications for the country's security and economy.

Indian Computer Emergency Response Team (CERT-In)

In India, CERT-In serves as the primary agency responsible for addressing cybersecurity events. This entity functions under the Ministry of Information and Technology (MeitY) and has the responsibility of providing alerts and advisories, coordinating responses to cyber incidents, and conducting cybersecurity drills and simulations. Furthermore, CERT-In collaborates with global computer emergency response teams (CERTs) to exchange knowledge and exemplary cybersecurity methods.

CERT-In's essential role is to help organizations improve their cybersecurity stance by offering advice on installing security measures and addressing attacks. The agency's involvement in incident management and its proactive stance towards cybersecurity establish it as an essential element of India's cyber policy framework.

Information Technology Act, 2000

The Information Technology Act, 2000 establishes the legally binding basis for India's approach to cybersecurity and electronic governance. Electronic records and digital signatures have legal validity and enforceability according to the legislation. The legislation also includes measures to address cybercrime, control the management of sensitive personal data, and guarantee the security of digital information.

The IT Act has undergone modifications over time to adapt to the evolving nature of cyber risks and comply with international norms. The revisions have enhanced the legal structure for cybersecurity in India, equipping law enforcement agencies with the essential capacity to effectively address cybercrime.

The Digital Personal Data Protection Bill, 2023

India's Digital Personal Data Protection Bill, 2023 is an important milestone in developing a comprehensive legal framework for data protection. The legislation establishes a Data Protection Authority to supervise the handling of personal data and ensure compliance with data protection standards. Furthermore, it implements safeguards to ensure people's privacy rights, including the requirement of obtaining consent for data processing and granting individuals the ability to access and rectify their data.

We created the legislation to align with international data protection norms like the General Data Protection Regulation (GDPR) in the European Union, while taking into account the unique challenges and needs of

India's digital environment. Upon its implementation, this Act will have a pivotal function in protecting personal data and bolstering confidence in India's digital environment.

National Cyber Coordination Centre (NCCC)

The establishment of the National Cyber Coordination Centre (NCCC) aimed to provide real-time monitoring of cyber threats and facilitate the coordination of government response activities. In order to provide situational awareness of the cyber threat landscape, the NCCC functions as a fusion center, collecting and evaluating data from several sources. It is critical in managing national cybersecurity incidents, facilitating prompt and synchronized operations in response to intrusions.

By improving India's capacity to identify and counter cyber attacks, the NCCC enhances the general security and robustness of the nation's digital infrastructure.

Digital India Programme and Cyber Surakshit Bharat Initiative

The Digital India Programme is a comprehensive government initiative aimed at transforming India into a society and economy empowered by digital technology and knowledge. This effort places considerable emphasis on guaranteeing cybersecurity for citizens, corporations, and government operations. The initiative facilitates the development of secure digital infrastructure and services, ensuring the integration of cybersecurity into India's comprehensive digital transformation framework.

The Cyber Surakshit Bharat Initiative, which was launched as part of the Digital India Programme, directly targets the enhancement of cybersecurity measures within government institutions. It offers training, professional development, and awareness initiatives for government professionals, promoting the implementation of optimal cybersecurity measures in different government institutions.

India’s Bilateral Cyber Dialogues

The bilateral cyber talks with important global partners have a vital role in shaping India's approach to cybersecurity and its larger cyber diplomacy. The dialogues serve as forums for collaboration on many aspects of cybersecurity, including the exchange of information and enhancement of capabilities, as well as the establishment of cyberspace norms and standards. The twofold goals of strengthening its own cybersecurity capabilities and contributing positively to global cyber stability motivate India's bilateral contacts.

1. India-U.S. Cyber Dialogue

The India-United States relationship. This cyber partnership is highly significant in India's bilateral cyber interactions. The India-U.S. initiative was launched in 2011. In recent years, Cyber Dialogue has evolved into a robust venue for collaborative efforts on cybersecurity matters. The discourse centers around numerous crucial domains, such as safeguarding vital infrastructure, combating cybercrime, advancing cybersecurity research and development, and establishing global standards in the realm of cyberspace.

The Joint Declaration on Enhancing Cybersecurity Cooperation, which both countries signed in 2016, is an outstanding outcome of this discussion. This declaration officially established the intention of both countries to collaborate on cybersecurity. Given its sophisticated cybersecurity infrastructure and skills, the United States offers a crucial alliance for India, which aims to strengthen its own cyber defenses and infrastructure. Additionally, the partnership has expanded to include collaboration in the areas of cyber incident management, capacity building, and exchange of best practices.

2. India-European Union Cyber Dialogue

The Cyber Dialogue between India and the European Union (EU) is a vital bilateral interaction that underscores India's dedication to strengthening global collaboration in the field of cyberspace. Commenced in 2016, this discourse centers on several cybersecurity concerns, such as cybercrime, data security, and the

development of worldwide cyber standards. The European Union, with its rigorous data protection rules and sophisticated cybersecurity architecture, presents a significant alliance for India as it formulates its own data protection and cybersecurity policies.

This dialogue has facilitated collaboration between India and the EU on several projects, including promoting responsible state conduct in cyberspace and strengthening resilience against cyber attacks. Furthermore, the partnership encompasses capacity-building initiatives, whereby the European Union offers technical support and specialized knowledge to assist India in enhancing its cybersecurity infrastructure.

3. India-Japan Cyber Dialogue

Established in 2012, the India-Japan Cyber Dialogue is a crucial element of the strategic alliance between the two nations. Japan, renowned for its advanced technology industry and strong cybersecurity framework, plays a crucial role as a partner for India in its efforts to establish a secure digital economy. The discourse centers around several crucial domains, such as safeguarding vital infrastructure, fostering cybersecurity collaboration in the Indo-Pacific region, and establishing global standards for cyberspace.

India and Japan have collaborated on cybersecurity research and development, acknowledging the critical role of innovation in effectively tackling developing cyber risks. Collaborative exercises and capacity-building programs have reinforced the alliance, aiming to enhance the cybersecurity capabilities of both countries.

4. India-Australia Cyber Dialogue

In recent years, the India-Australia Cyber Dialogue has become an integral component of a wider strategic engagement. Established in 2014, the discussion aims to strengthen collaboration in the fields of cybersecurity, cybercrime prevention, and the formulation of global cyber standards. This relationship is especially pertinent given the shared concerns of both nations over cyber threats in the Indo-Pacific area.

The India-Australia Cyber Dialogue has facilitated collaborative endeavors in areas such as cyber threat intelligence sharing, capacity building, and joint exercises. An analysis of Australia's sophisticated cybersecurity system and its proactive approach to cyber governance offers India significant insights and assistance in enhancing its own cybersecurity infrastructure.

5. India-Israel Cyber Dialogue

The cyber alliance between India and Israel is characterized by a strategic emphasis on advancing cybersecurity and fostering technical cooperation. Established in 2014, the India-Israel Cyber Dialogue has resulted in substantial collaboration in domains including cyber defense, cybercrime prevention, and cybersecurity research and development. Israel, renowned for its cutting-edge cybersecurity technologies and emerging companies, presents a crucial alliance for India to strengthen its information security capabilities.

In the realm of cybersecurity, India and Israel engage in collaborative endeavors encompassing cooperative research projects, technology transfers, and the exchange of exemplary methodologies. The specific goal of this collaboration is to protect critical infrastructure and develop advanced cybersecurity solutions that can effectively address the complex cyber risks faced by both countries.

6. India-Russia Cyber Dialogue

An integral component of the wider strategic alliance between India and Russia, the India-Russia Cyber Dialogue aims to strengthen collaboration in the fields of cybersecurity and information security. The discussion encompasses several topics, such as cybercrime, cyberdefense, and the establishment of global standards for cyberspace. Russia's cyber defense expertise and strategic implementation of information security provide India with unique perspectives as it formulates its own cybersecurity policies.

This discourse has facilitated collaboration between India and Russia in areas such as joint exercises, capacity building, and the sharing of cyber threat intelligence. The agreement further underscores the need for multilateral collaboration in tackling worldwide cyber issues.

7. India-France Cyber Dialogue

India's cyber collaboration with France, established through the India-France Cyber Dialogue, centers on domains including cyber defense, safeguarding vital infrastructure, and advancing global cyber standards. Given its significant focus on cybersecurity and digital sovereignty, France presents a highly beneficial alliance for India in its endeavors to strengthen its cybersecurity capacities.

In the realms of cybersecurity research and development, capacity building, and the exchange of best practices, the India-France Cyber Dialogue has resulted in constructive collaboration. The collaborative effort also aims to advance a cyberspace that is free, open, and secure, in accordance with the common principles of both nations.

India's Multilateral Cyber Engagements

Asserting its commitment to creating global cybersecurity norms, fostering international collaboration, and guaranteeing an open, safe, and resilient cyberspace, India's participation in multilateral forums is a crucial element of its cyber diplomacy. India aims to tackle the global nature of cyber threats by actively participating in several multilateral forums and promoting fair and comprehensive governance frameworks in the Internet domain. These interactions enable India to cooperate with other countries, thereby contributing to the advancement of worldwide cyber standards and strengthening its own cybersecurity stance.

1.The United Nations (UN)

India has actively contributed to the United Nations' efforts to establish a framework for states' responsible conduct in cyberspace. Indian participation in the UN Group of Governmental Experts (GGE) on Advancing Responsible State Behavior in Cyberspace and the Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security has been instrumental in influencing cybersecurity debates.

India promotes the relevance of current international law to the realm of cyberspace and endorses the establishment of voluntary standards for responsible conduct of states in cyberspace. The paper underscores the need for enhancing capabilities, implementing confidence-building strategies, and fostering international collaboration to effectively tackle the issues presented by cyber threats. Moreover, India has pushed for greater inclusivity in global cyber governance, ensuring that the perspectives and needs of developing countries are adequately considered in international discussions.

2.The BRICS

With its membership in BRICS (Brazil, Russia, India, China, and South Africa), India actively participates in international cyber discussions aimed at strengthening cybersecurity collaboration among the five developing economies. Indian participation in BRICS facilitates collaboration with other member governments on matters such as cybercrime, data protection, and cyber rules formulation.

The Working Group on Information and Communication Technologies (ICTs) Cooperation under the BRICS countries focuses on several facets of cybersecurity, such as safeguarding critical infrastructure, enhancing cyber resilience, and fostering capacity development. India has utilized this forum to promote a coordinated strategy towards cybersecurity that takes into account the economic and developmental requirements of member states while also addressing security issues.

3. Shanghai Cooperation Organization (SCO)

India's participation in the Shanghai Cooperation Organization (SCO) highlights its commitment to regional collaboration in the field of cybersecurity. India has been an active participant in the initiatives of the Shanghai Cooperation Organization (SCO) to strengthen cybersecurity, combat cybercrime, and advance information security since 2017.

The SCO's emphasis on regional stability and security aligns with India's regional strategic goals. India collaborates with member states through the SCO's Regional Anti-Terrorist Structure (RATS) to combat the use of cyberspace for terrorist operations and strengthen collective efforts to combat cybercrime. Furthermore, India's participation in the SCO includes efforts to foster a shared understanding of cyber risks and the need for collaborative measures to tackle them.

4. Commonwealth of Nation

India's inclusion in the Commonwealth Cyber Declaration, 2018 highlights its commitment to fostering international collaboration in cybersecurity within the Commonwealth of Nations. The declaration underscores the need for collaborative efforts to address cyber threats, safeguard vital infrastructure, and guarantee the safe and unrestricted transmission of information on the internet.

India has actively participated in capacity-building activities within the Commonwealth's cybersecurity initiatives, sharing its specialist knowledge and exemplary methods with other member states. India's participation in the Commonwealth also presents an opportunity for cooperation in the advancement of international cyber standards and global cybersecurity resilience.

5. G20

India's participation in the G20 has been critical in facilitating the resolution of global cybersecurity issues within the framework of the digital economy. During the G20's deliberations on the digital economy, India has stressed the need for implementing measures that foster digital inclusiveness, safeguard against cyber risks, and guarantee the security of digital infrastructure.

India has made significant contributions to the cybersecurity agenda of the G20 by providing funding to projects that prioritize the improvement of critical infrastructure security, foster cyber resilience, and tackle the challenges presented by emerging technologies like artificial intelligence (AI) and the Internet of Things (IoT). India's participation in the G20 demonstrates its dedication to influencing global policies that effectively manage the interplay between economic development and cybersecurity concerns.

6. ASEAN Regional Forum (ARF)

India uses the ASEAN Regional Forum (ARF) as a significant forum to actively participate in dialogues with Southeast Asian countries about cybersecurity issues. India, as a participant in the ARF, engages in collaborative efforts with ASEAN member states and other partners to strengthen regional cybersecurity cooperation and effectively tackle shared cyber risks.

India's involvement in the ARF includes active participation in deliberations on strategies to enhance trust in cyberspace, the exchange of exemplary cybersecurity methods, and contributions to capacity-building initiatives at the regional level. India's participation in the ARF also underscores its wider strategic goals in the Indo-Pacific region, where cybersecurity is progressively acknowledged as a crucial element of regional security.

7. International Telecommunication Union (ITU)

India's membership in the International Telecommunication Union (ITU) demonstrates its dedication to actively contributing to the advancement of worldwide cyber governance frameworks. India, as a member of the ITU, actively participates in deliberations focused on the involvement of telecommunications in cybersecurity, safeguarding vital information infrastructure, and advancing global cyber standards.

India has provided support to ITU efforts aimed at improving worldwide cybersecurity collaboration, including the establishment of capacity-building programs for developing member countries. India actively promotes an open, secure, and accessible internet that facilitates sustainable development and global connection through its participation in the ITU.

8. Global Forum on Cyber Expertise (GFCE)

India's participation in the Global Forum on Cyber Expertise (GFCE) underscores its commitment to enhancing capabilities and fostering international collaboration in the field of cybersecurity. The primary objective of the GFCE is to facilitate the exchange of knowledge, best practices, and resources in order to enhance global cyber capabilities.

India's participation in the Global Forum on Cybersecurity (GFCE) includes contributions to the advancement of cybersecurity training programs, knowledge sharing in domains such as cybercrime prevention, and engagement in worldwide efforts focused on strengthening cybersecurity resilience. Through its participation in the GFCE, India demonstrates its dedication to enhancing global cybersecurity capabilities and promoting international cooperation.

Conclusion

The cyber diplomacy of India plays a vital role in its overall foreign policy and national security strategy, demonstrating its dedication to facilitating international collaboration, strengthening global cybersecurity, and advancing a secure and robust digital future. By actively participating in bilateral and multilateral discussions, India has established itself as a significant influencer in determining worldwide cyber standards, promoting cooperative structures, and tackling the intricate issues of the cyber realm.

The bilateral cyber discussions between India and several nations emphasize India's proactive stance on cybersecurity. India's collaboration with countries around the world not only improves its own cybersecurity stance, but it also strengthens the joint effort to protect digital infrastructure and reduce cyber risks. Partnerships of this kind facilitate the sharing of most effective methods, the collaborative creation of technology solutions, and the building of mutual confidence, all of which are crucial for tackling the global character of cyber threats.

At the multilateral level, India's participation in international forums such as the United Nations, BRICS, the G20, and the ASEAN Regional Forum underscores its strategic stance towards global cyber governance. India's active engagement in these forums contributes to the formation of global cyber standards, supports the promotion of responsible conduct by states, and advances inclusive governance frameworks. India contributes to the establishment of a balanced and effective global cybersecurity architecture by supporting projects that enhance global cybersecurity resilience and advocating for the representation of diverse perspectives.

Moreover, India's participation in global cybersecurity efforts, including capacity building and technical support, demonstrates its dedication to enhancing global cyber capabilities. In order to promote international cooperation and establish a safe and resilient digital environment, India showcases its commitment by sharing its knowledge and assisting in the construction of cybersecurity infrastructure in developing nations.

Ultimately, India's cyber diplomacy serves as evidence of its strategic foresight and dedication to maintaining global cyber stability. India's participation in bilateral and multilateral partnerships has a significant impact on the development of global cyber governance. The continuous evolution of the digital landscape necessitates India's continued involvement in global cyber diplomacy to effectively tackle growing cyber threats, foster a secure and resilient cyberspace, and guarantee universal access and security to the advantages offered by digital technologies.

References:

1. Chouhan, Vivek. "India’s Approach to Cyber Diplomacy." International Studies , vol. 55, no. 3, 2018, pp. 237-253. doi:10.1177/0020881718791316.

2. Ministry of External Affairs, Government of India. "India’s Cyber Diplomacy: Strengthening Global Cooperation for a Secure Cyberspace." MEA , 2021, www.mea.gov.in/cyber-diplomacy.htm.

3. Singh, Shyam. "India’s Role in Global Cybersecurity Governance: Prospects and Challenges." Strategic Analysis , vol. 44, no. 4, 2020, pp. 313-328. doi:10.1080/09700161.2020.1779575.

4. Kumar, Rajesh, and Vikas Arora. "Cybersecurity Challenges in India: A Comprehensive Review." Journal of Information Security and Applications , vol. 46, 2019, pp. 100-112. doi:10.1016/j.jisa.2019.03.006.

5. Jain, Rohan. "India’s Emerging Role in Global Cyber Governance." Indian Journal of International Affairs , vol. 43, no. 2, 2017, pp. 201-218.

6. Bhat, Praveen, and Tanvi Shahi. "India's Cyber Diplomacy in the Indo-Pacific: Challenges and Opportunities." Journal of Strategic Affairs , vol. 12, no. 1, 2021, pp. 101-120.

7. International Institute for Strategic Studies (IISS). "India’s Cyber Diplomacy: Building Global Cyber Norms." IISS , 2020, www.iiss.org/blogs/analysis/2020/12/india-cyber-diplomacy.

8. Tikk, Eneken, and Mika Kerttunen. "The Emergence of International Cyber Diplomacy." Journal of International Affairs , vol. 72, no. 1, 2018, pp. 15-29.

9. Department of Electronics and Information Technology, Government of India. "India’s National Cyber Security Policy." DeitY , 2022, www.deity.gov.in/national-cyber-security-policy.

10. Sachdeva, Gauri. "India-EU Cyber Dialogue: A New Dimension in Bilateral Relations." European Foreign Affairs Review , vol. 24, no. 3, 2019, pp. 375-393.

11. Ministry of Electronics and Information Technology, Government of India. "National Cyber Security Policy (NCSP) 2013." MeitY , 2013, www.meity.gov.in/national-cyber-security-policy-2013.

12. Ministry of Electronics and Information Technology, Government of India. "Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)." MeitY , 2017, www.cyberswachhtakendra.gov.in.

13. Ministry of Electronics and Information Technology, Government of India. "National Critical Information Infrastructure Protection Centre (NCIIPC)." MeitY , www.nciipc.gov.in.

14. Ministry of Electronics and Information Technology, Government of India. "Indian Computer Emergency Response Team (CERT-In)." MeitY , www.cert-in.org.in.

15. Ministry of Law and Justice, Government of India. The Information Technology Act, 2000 . Government of India, 2000, www.indiacode.nic.in/handle/123456789/1999.

16. Ministry of Electronics and Information Technology, Government of India. "Data Protection Bill (Draft)." MeitY , 2019, www.meity.gov.in/data-protection-framework.

17. Ministry of Electronics and Information Technology, Government of India. "National Cyber Coordination Centre (NCCC)." MeitY , www.meity.gov.in/nccc.

18. Ministry of Electronics and Information Technology, Government of India. "Digital India Programme." MeitY , 2015, www.digitalindia.gov.in.

19. Ministry of Electronics and Information Technology, Government of India. "Cyber Surakshit Bharat Initiative." MeitY , 2018, www.cybersurakshitbharat.in.
Here are the references in MLA style:

20. BRICS. "BRICS Leaders' Xiamen Declaration." Xiamen, China, 2017.

21. Buchanan, Ben. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. Hurst, 2017.

22.Embassy of India, Tokyo. "India-Japan Cyber Dialogue." Embassy of India, Tokyo , 2017.

23.European Commission. "EU-India Relations: A Partnership for Sustainable Development." European Commission , 2017.

24.Ranganathan, S. "Cyber Governance in the Age of Digital Sovereignty." Observer Research Foundation , 2021.

25. SCO RATS. "SCO Regional Anti-Terrorist Structure." SCO RATS , 2017.

26.UNIDIR. The Role of the United Nations in Advancing International Cybersecurity. UNIDIR, 2020.

27. UNODA. United Nations Office for Disarmament Affairs: Cybersecurity in the Context of International Security. UNODA, 2020.