IJAER/ March-April 2024/Volume-13/Issue-2 ISSN: 2278-9677
International Journal of Arts & Education Research
(Peer-Reviewed, Open Access, Fully Refereed International Journal) Impact Factor:7.06

Creating International Partnerships for a Safe and Robust Future: India's Cyber Diplomacy

Fathimath Suhara Kadakkadan

Research Scholar, Glocal School of Art and Social Science,

The Glocal University, Mirzapur Pole, Saharanpur (U.P).

Dr. Waseem Ahmad

Research Supervisor, Glocal School of Art and Social Science

The Glocal University, Mirzapur Pole, Saharanpur (U.P).

ABSTRACT:

India's rising prominence in the global digital landscape has underscored the importance of cyber diplomacy as a key component of its international relations strategy. This article explores India's expanding role in cyber diplomacy, highlighting its initiatives to forge international partnerships aimed at ensuring a secure and resilient cyberspace. By examining India's bilateral and multilateral engagements, the article showcases notable projects and agreements that reflect India's commitment to fostering international collaboration in cybersecurity. Additionally, the study addresses the challenges India faces, including the delicate balance between national security interests and the necessity for transparency and cooperation in cyberspace. An evaluation of India's cyber dialogues with major powers such as the United States, the European Union, Japan, and Australia, along with its participation in global forums like the United Nations and the BRICS coalition, illustrates how India is positioning itself as a leader in shaping the global cyber governance landscape. Ultimately, this paper argues that India's proactive approach to cyber diplomacy is crucial for addressing the complex challenges of the digital age and for building a secure, resilient, and inclusive global cyberspace.

Keywords: Digital Diplomacy, Foreign Policy, Global Cyber Alliances,Cyber Diplomacy

INTRODUCTION-:

Cyberspace has emerged as a vital domain in the 21st century, impacting various facets of global security, economic resilience, and diplomatic interactions. As digital networks foster increasing global interconnectivity, the need for robust cybersecurity measures and international cooperation has become paramount. A diverse array of cyber threats, such as espionage, cybercrime, and state-sponsored attacks, poses significant risks to national security, economic development, and the functioning of essential infrastructure. In this context, cyber diplomacy has become an integral component of a nation's foreign policy, serving as a platform for dialogue, collaboration, and the establishment of standards and regulations in the field of cybersecurity.

India's rapidly growing digital economy and substantial internet user base position the country at a pivotal point in shaping the global cyber landscape. As a leading IT hub and a key player in the international digital economy, India's approach to cyber diplomacy is crucial not only for its national security and economic interests but also for the overall stability and security of the global digital environment. The nation's broader foreign policy objectives inform its cyber diplomacy strategy, which includes fostering a peaceful and secure global climate, promoting economic development, and ensuring an equitable distribution of the benefits arising from the digital revolution.

India's cyber diplomacy initiatives have seen significant progress over the past decade, reflecting its increasing engagement in global cyber governance and its ambition to take on a leadership role in shaping international cybersecurity standards. This analysis delves into the various dimensions of India's cyber diplomacy, focusing on its relationships with other nations, the challenges it faces, and the future opportunities that may arise. The objective of this study is to offer a thorough insight into India's endeavors to forge global alliances and foster a secure and resilient cyberspace by exploring its cyber discussions with major global players, including the United States, the European Union, Japan, and Australia, as well as its participation in international platforms such as the United Nations and BRICS.

India's proactive stance on cyber diplomacy underscores its recognition of the necessity for collaboration in addressing the complex challenges of the digital age. Given the continuous evolution and growing intricacy of cyber threats, it is crucial for India to forge strong international partnerships to protect not only its own cybersecurity but also that of the global community. This analysis suggests that India's cyber diplomacy is not merely a response to immediate threats but a forward-thinking strategy aimed at shaping the future of global cyber governance. By strategically leveraging cyber diplomacy, India seeks to create a digital landscape that is secure, resilient, and inclusive for both itself and the international community.

India's Cybersecurity Policy Framework

India's cyber policy framework represents a thorough approach to addressing the challenges and opportunities arising from a rapidly evolving digital landscape. As the nation increasingly integrates into the global digital economy, the urgency for robust cybersecurity protocols has intensified. This framework reflects India's commitment to protecting its digital infrastructure, ensuring the safety of citizens' data, and positioning itself as a leader in international cyber governance.

National Cyber Security Policy (NCSP) 2013

The National Cyber Security Policy (NCSP) 2013 serves as a cornerstone of India's approach to cybersecurity. Launched by the Ministry of Electronics and Information Technology (MeitY), the National Cybersecurity Strategy Program aims to create a secure and resilient digital landscape for individuals, businesses, and government entities. This initiative emphasizes the necessity of protecting critical information infrastructure (CII) from cyber threats, enhancing capabilities to prevent and respond to cyber incidents, and fostering a culture of cybersecurity awareness and education.The National Cybersecurity Strategy (NCSP) advocates for the formation of public-private partnerships and collaboration among various sectors, including academia, industry, and civil society, to bolster India's cybersecurity framework. Additionally, the strategy highlights the importance of research and development in cybersecurity technologies and supports the establishment of a robust legal and regulatory framework to address emerging cyber threats.

Cyber Hygiene Center (Botnet Removal and Malware Assessment Facility).

Established in 2017, the Cyber Swachhta Kendra, known as the Botnet Cleaning and Malware Analysis Centre, operates under the Ministry of Information and Technology (MeitY). Its primary aim is to provide tools and resources to combat botnets and malware. This initiative is part of India's broader strategy to enhance cybersecurity, offering complimentary tools for detecting and removing malware from both personal computers and mobile devices.The Cyber Swachhta Kendra collaborates with internet service providers (ISPs), antivirus companies, and other stakeholders to ensure the effectiveness and widespread accessibility of its solutions. This initiative not only protects the digital assets of individuals and businesses but also plays a crucial role in reducing overall cyber threats across the country.

National Critical Information Infrastructure Protection Centre (NCIIPC)

The National Critical Information Infrastructure Protection Centre (NCIIPC) was established under the Information Technology Act of 2000, with amendments made in 2008. Its primary role is to safeguard critical information infrastructure (CII) in India. CII includes vital assets and systems that are essential for the functioning of the economy and national security, covering sectors such as banking, communications, energy, and defense.NCIIPC's mission involves identifying CII assets, assessing their vulnerability to cyber threats, and working with various stakeholders to implement preventive strategies. A key responsibility of the center is to ensure the resilience of India's critical infrastructure against cyberattacks, which could pose serious risks to the nation's security and economic stability.

Indian Computer Emergency Response Team (CERT-In)

In India, the primary agency tasked with managing cybersecurity incidents is CERT-In. Operating under the Ministry of Electronics and Information Technology (MeitY), this organization is responsible for issuing alerts and advisories, coordinating responses to cyber incidents, and conducting cybersecurity drills and simulations. Additionally, CERT-In works in collaboration with international computer emergency response teams (CERTs) to share knowledge and best practices in cybersecurity. CERT-In plays a crucial role in enhancing the cybersecurity posture of organizations by providing guidance on implementing security measures and responding to attacks. Its active participation in incident management and commitment to proactive cybersecurity initiatives position it as a vital component of India's cyber policy framework.

Information Technology Act, 2000

The Information Technology Act of 2000 provides the foundational legal framework for India's strategy regarding cybersecurity and electronic governance. This legislation grants legal recognition and enforceability to electronic records and digital signatures. Additionally, it incorporates provisions aimed at combating cybercrime, regulating the handling of sensitive personal data, and ensuring the protection of digital information. Over the years, the IT Act has been amended to keep pace with the changing landscape of cyber threats and to align with global standards. These updates have strengthened the legal framework for cybersecurity in India, empowering law enforcement agencies with the necessary tools to effectively tackle cybercrime.

The Alphanumeric Individual Data Defense Bill, 2023

India's Alphanumeric Individual Data Defense, 2023 marks a significant advancement in establishing a robust legal framework for data protection. This legislation introduces a Data Protection Authority tasked with overseeing the management of personal data and ensuring adherence to data protection regulations. It also incorporates measures to uphold individuals' privacy rights, such as mandating consent for data processing and empowering individuals to access and correct their personal information. The legislation has been designed to align with global data protection standards, including the General Data Protection Regulation (GDPR) of the European Union, while addressing the specific challenges and requirements of India's digital landscape. Once enacted, this Act will play a crucial role in safeguarding personal data and enhancing trust in India's digital ecosystem.

National Cyber Coordination Centre (NCCC)

The National Cyber Coordination Centre (NCCC) was created to enable real-time surveillance of cyber threats and to streamline the government's response efforts. Acting as a fusion center, the NCCC gathers and analyzes information from various sources to enhance situational awareness of the cyber threat environment. It plays a vital role in managing national cybersecurity incidents, ensuring timely and coordinated actions against intrusions. By bolstering India's ability to detect and respond to cyber attacks, the NCCC significantly strengthens the overall security and resilience of the country's digital infrastructure.

Digital India Programme and Cyber Surakshit Bharat Initiative

The Digital India Programme represents a holistic government initiative designed to convert India into a society and economy that is driven by digital technology and knowledge. A significant focus of this initiative is on ensuring cybersecurity for individuals, businesses, and governmental functions. It supports the establishment of a secure digital infrastructure and services, embedding cybersecurity within the broader framework of India's digital transformation.

As a key component of the Digital India Programme, the Cyber Surakshit Bharat Initiative specifically aims to bolster cybersecurity protocols within government entities. It provides training, skill enhancement, and awareness programs for government personnel, fostering the adoption of best practices in cybersecurity across various governmental organizations.

India’s Bilateral Cyber Dialogues

Bilateral cyber discussions with key global partners play a crucial role in defining India's strategy for cybersecurity and its broader cyber diplomacy efforts. These dialogues act as platforms for collaboration on various facets of cybersecurity, such as information sharing, capability enhancement, and the development of norms and standards for cyberspace. India's engagement in these bilateral relationships is driven by the dual objectives of bolstering its own cybersecurity capabilities and fostering global cyber stability.

1. India-U.S. Cyber Dialogue

The relationship between India and the United States is marked by a significant cyber partnership that plays a crucial role in India's bilateral cyber engagements. Initiated in 2011, the India-U.S. initiative has seen the Cyber Dialogue transform into a vital platform for joint efforts in cybersecurity. The discussions encompass several key areas, including the protection of critical infrastructure, the fight against cybercrime, the promotion of cybersecurity research and development, and the establishment of international standards in cyberspace.A notable achievement of this dialogue is the Joint Declaration on Enhancing Cybersecurity Cooperation, signed by both nations in 2016, which formalized their commitment to work together on cybersecurity issues. The United States, with its advanced cybersecurity capabilities and expertise, serves as an essential partner for India, which seeks to bolster its own cyber defenses and infrastructure. Furthermore, the partnership has broadened to include cooperation in cyber incident management, capacity building, and the sharing of best practices.

2. India-European Union Cyber Dialogue

The Cyber Dialogue between India and the European Union (EU) represents a crucial bilateral engagement that highlights India's commitment to enhancing global cooperation in cyberspace. Initiated in 2016, this dialogue addresses various cybersecurity issues, including cybercrime, data protection, and the establishment of international cyber standards. The EU, known for its stringent data protection regulations and advanced cybersecurity framework, serves as a key partner for India as it develops its own data protection and cybersecurity strategies.

This dialogue has enabled joint efforts between India and the EU on multiple initiatives, such as advocating for responsible state behavior in cyberspace and bolstering defenses against cyber threats. Additionally, the partnership includes capacity-building programs, where the European Union provides technical assistance and expertise to support India in improving its cybersecurity capabilities.

3. India-Japan Cyber Dialogue

Established in 2012, the India-Japan Cyber Dialogue serves as a vital component of the strategic partnership between the two countries. Japan, recognized for its cutting-edge technology sector and robust cybersecurity measures, is an essential ally for India in its pursuit of a secure digital economy. The discussions focus on several key areas, including the protection of critical infrastructure, promoting cybersecurity cooperation in the Indo-Pacific region, and setting international standards for cyberspace. India and Japan have engaged in joint research and development initiatives in cybersecurity, understanding the importance of innovation in addressing emerging cyber threats. Collaborative exercises and capacity-building initiatives have strengthened their partnership, with the goal of enhancing the cybersecurity capabilities of both nations.

4. India-Australia Cyber Dialogue

In recent years, the India-Australia Cyber Dialogue has emerged as a crucial element of broader strategic cooperation. Initiated in 2014, this dialogue focuses on enhancing collaboration in cybersecurity, preventing cybercrime, and developing global cyber standards. The partnership is particularly relevant due to the mutual concerns both countries share regarding cyber threats in the Indo-Pacific region.The India-Australia Cyber Dialogue has enabled joint efforts in areas such as sharing cyber threat intelligence, building capacity, and conducting collaborative exercises. A review of Australia's advanced cybersecurity framework and its proactive stance on cyber governance provides India with valuable insights and support to bolster its own cybersecurity capabilities.

5. India-Israel Cyber Dialogue

The partnership between India and Israel in the field of cybersecurity is marked by a strategic focus on enhancing cybersecurity measures and promoting technical collaboration. Initiated in 2014, the India-Israel Cyber Dialogue has led to significant joint efforts in areas such as cyber defense, the prevention of cybercrime, and research and development in cybersecurity. Israel, known for its innovative cybersecurity technologies and burgeoning startups, serves as a vital ally for India in bolstering its information security capabilities.In the cybersecurity domain, India and Israel work together on various initiatives, including joint research projects, technology transfers, and the sharing of best practices. The primary objective of this partnership is to safeguard critical infrastructure and create sophisticated cybersecurity solutions that can effectively tackle the intricate cyber threats encountered by both nations.

6. India-Russia Cyber Dialogue

A key element of the broader strategic partnership between India and Russia, the India-Russia Cyber Dialogue seeks to enhance cooperation in cybersecurity and information security. The dialogue covers various subjects, including cybercrime, cyber defense, and the development of international standards for cyberspace. Russia's proficiency in cyber defense and its strategic approach to information security offer India valuable insights as it develops its own cybersecurity strategies.This discourse has facilitated collaboration between India and Russia in areas such as joint exercises, capacitybuilding, 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 participatingin 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 AdvancingResponsible 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 internationalcollaboration to effectively tackle the issues presented by cyber threats. Moreover, India has pushed for greaterinclusivity 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 matterssuch as cybercrime, data protection, and cyber rules formulation. The Working Group on Information and Communication Technologies (ICTs) Cooperation under the BRICScountries 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'sparticipation 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 effectivelymanage 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 withSoutheast 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 incyberspace, 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 ofthe 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 advancementof 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 promotinginternational cooperation.

Conclusion

India's commitment to fostering international cooperation, bolstering global cybersecurity, and promoting a safe and resilient digital future is exemplified by its cyber diplomacy, which is an essential component of its broader foreign policy and national security strategy. India has become a major player in establishing global cyber standards, fostering collaborative frameworks, and addressing the complex problems of the cyberspace by actively engaging in bilateral and international debates.India's aggressive approach on cybersecurity is highlighted by the bilateral cyber discussions it conducts with a number of countries. India's international cooperation enhances its cybersecurity posture and fortifies the collective endeavor to safeguard digital infrastructure and lower cyber threats. These kinds of partnerships make it easier to share the best practices, work together to develop technological solutions, and develop mutual trust all of which are essential for addressing the global nature of cyber threats.At the multilateral level, India's involvement in international fora like the ASEAN Regional Forum, the G20, the BRICS, and the UN highlights its strategic approach to global cyber governance. India's strong participation in these forums promotes inclusive governance frameworks, encourages states to act responsibly, and helps to shape international cyber norms. By promoting the inclusion of diverse viewpoints and funding initiatives that increase global cybersecurity resilience, India helps to create a fair and efficient global cybersecurity architecture.Furthermore, India's involvement in international cybersecurity initiatives, such as technical assistance and capacity building, shows its commitment to advancing global cyber capabilities. By sharing its expertise and helping to build cybersecurity infrastructure in poorer countries, India demonstrates its commitment to fostering international collaboration and creating a secure and resilient digital environment. In the end, India's cyber diplomacy is proof of its strategic vision and commitment to preserving cyber stability worldwide. The evolution of global cyber governance is significantly impacted by India's involvement in bilateral and international collaborations. Given how quickly the digital landscape is changing, India must continue to engage in international cyber diplomacy in order to effectively combat emerging cyberthreats, create a safe and resilient cyberspace, and ensure that everyone has access to the benefits of digital technologies.

References:

1.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.

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

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

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

5.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.

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

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

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

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

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

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

12. 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.

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

14. 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.

15. Ministry of Law and Justice, Government of India. The Information Technology Act, 2000 . Governmentof 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 CoordinationCentre (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 BharatInitiative." MeitY , 2018, www.cybersurakshitbharat.in.

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

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

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

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

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

25. UNODA. United Nations Office for Disarmament Affairs: Cybersecurity in the Context of InternationalSecurity. UNODA, 2020