Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
July-December 2023 4(2), 2199–2203

INDIA'S CYBERSECURITY DIPLOMACY: BUILDING GLOBAL ALLIANCES

Pramod Kumar Chaudhary [1]

[1] Research Scholar, Shri Venkateshwara University

Corresponding Author

Pramod Kumar Chaudhary,
pramodchdhr7@gmail.com

DOI
10.29121/shodhkosh.v4.i2.2023.3386

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The emerging interconnection and interdependence of the world, cyberspace has become an indispensable domain that shapes national security, economic growth and stability of the world. With India now emerging as a rising global power and global digital leader, it has catapulted cybersecurity diplomacy as its centrepiece of international agendas. This paper looks at India's attempts at developing global alliances and advancing multilateralism in positioning itself to respond to cyberspace challenges. India's cybersecurity diplomacy exists at different levels. It is a convinced advocate in multilateral platforms such as the United Nations for norms governing state behavior in cyberspace and for a rules based global order. India works in regional cooperation with South Asian and ASEAN partners in regard to cyber resilience and capacity building initiatives. It has been brokering strong cybersecurity partnerships bilaterally with countries including the United States, Japan, Australia and the European Union on the basis of reciprocal threat intelligence sharing, joint exercises, technological innovation. An additional member of the Quad, India is involved in Indo-Pacific cyber security initiatives seeking to protect critical infrastructure and foster digital inclusivity. India has domain civil cybersecurity defenses and imparted the capacities to a relative through CERT–In and NCIIPC, investment in capacity building programming and public private party ties to the expansion within India's technological abilities. India maintains that the balancing of cyber sovereignty with principles of an open and secure internet should follow by respecting equitable data governance frameworks and inclusive international standards. But geopolitical tensions, advanced cyber threats, and fast-moving technology still exist. As a proactive player in India's diplomacy, its form in shaping global cyber governance plays a leading role. India is working to develop a secure digital ecosystem by creating trust, transparency and collaboration, to drive a peaceful, innovative and shared prosperity in the era of unprecedented digital transformation.

Keywords: Cybersecurity, Diplomacy, cyberspace, Global Alliances, etc

1. INTRODUCTION

Like cyberspace itself, the landscape in which we live forms a rapidly evolving global environment that has so far important repercussions on national security, economic growth and stability of the society. With nations becoming ever more interconnected in the digital revolution, international diplomacy cannot go on without cybersecurity. The subject of robust cybersecurity diplomacy has boomed for India, a growing global power seeking to help lead in technology and innovation. India, aiming to guarantee the security of its digital infrastructure and to protect its digital sovereignty, seeks to deeply engage in global cooperation to build multilateral ties and forged global alliances to enhance norms of cyber security worldwide, also to leverage India's own capabilities for a responsible future of cyberspace governance.

2. CYBERSECURITY AS A DIPLOMATIC PRIORITY: THE RISE

With digitalisation picking up pace in India starting a tryst with cybersecurity began in earnest with the country assailing initiatives like Digital India to transform India as a digitally empowered society and knowledge economy. With

the growing number of smartphones, expanding internet penetration and the government's drive to move itself to the e-governance mode, India has seen its digital footprint expand. However, it has also been an expansion that has exposed vulnerabilities because India is in now suffering a deluge of cyber-attacks on its critical infrastructure, financial institutions and other sensitive government networks. In recent years, India saw more than one million cybersecurity incidents, and hence it's imperative to adopt adequate cybersecurity norms. India recognized the inherent cross border nature of cyber threats and turned its attention to facilitating engagement with other stakeholders of the global cyberspace community to understand and solve challenges in cyberspace in common. For this reason, cybersecurity soon became a strategic priority in diplomacy as a cyber protection measure of national assets and as promoting international stability.

3. INDIA'S CYBERSECURITY POLICY FRAMEWORK

An adequate Cybersecurity policy framework has been developed by India in order to back its diplomatic efforts. Updating the National Cyber Security Policy in 2013, the government had laid down strategies to protect information infrastructure, build capabilities to prevent cyber threats and foster a culture of cybersecurity. A future version of this policy will be updated to address the fluidity of cyber threats and new technologies like artificial intelligence and the Internet of Things (IoT). India's commitment to protecting vital digital assets is evident in the creation of institutions like the National Critical Information Infrastructure Protection Centre (NCIIPC). In addition, roles have been streamlined by the creation of a National Cybersecurity Coordinator reporting to the National Security Council Secretariat.

4. INDIA'S MULTILATERAL ENGAGEMENT IN CYBERSECURITY

India has made substantial progress in positively helping to promote multilateral strategies to bolster cybersecurity collaboration and norms development. As a member state of the United Nations, India has played an active role in advocating for international rules regarding ways in which states act in cyberspace. For India, having cornered initiatives such as the United Nations Group of Governmental Experts (UNGGE) and the Open Ended Working Group (OEWG), an important point has been underscored that a rules based order on the earth is necessary for peace, security and stability in cyberspace. India's key declaration at the UN has been to promote universally agreed norms for responsible state behavior in cyberspace - the applicability of international law in cyberspace, protection of critical infrastructure and cooperation for combating cyber crime and cyber terrorism. This bears India's weight and forms part of its generally espoused stance towards multilateralism, that calls for the ladder between developed and developing nations in their engagement around cybersecurity. India has also been an active participant to the Global Conference on Cyber Space (GCCS), organised in New Delhi in 2017. The conference brought together stakeholders around the world to discuss cyber norms and capacity building, and bring about a secure and inclusive cyberspace.

5. CYBERSECURITY REGIONAL COOPERATION

And at the regional level, it has been trying to strengthen its cybersecurity collaboration with India's neighbours and strategic partners. While combating geopolitical challenges, India has inked bilateral contracts with nations such as Bangladesh, Bhutan, Nepal and Sri Lanka to engage in information share, joint cyber exercises and joint research. The efforts are toward creating collective defense against cyber threats beyond national borders. In recent years, the India-ASEAN Cyber Dialogue launched provides a platform to enhance the exercise of cybersecurity and discuss potential areas of cooperation in this area. Besides, India also continues to participate in the ARF workshops on the cybersecurity, which are contributing to the confidence building measures and cooperative mechanisms.

6. ENHANCING STRATEGIC PARTNERSHIP

In its pursuit of India's above average capabilities in cybersecurity, India's cybersecurity diplomacy stretches to its strategic partnerships with the major global powers such as United States, the European Union, Japan, Australia and Russia. Such partnerships are anchored in the common concerns of cyber threats and their common interest in a secure and open cyber space. Under the rubric of India-us Cyber Framework Agreement signed in 2016 India and the United States have a robust India-US Cyber Partnership. This includes sharing information on cyber threats; the carrying out of joint exercises and, cooperation on capacity building activities. The two countries have also teamed up to forge greater

resilience in critical infrastructure and suppress cyber enabled terrorism. As part of that dialogue, the US and India hold regular dialogues like the US-India Cyber Dialogue and this ongoing cooperation and alignment on the policy approach is enabled. India's cybersecurity collabation with the European Union also encompasses policy dialogue, knowledge sharing and the development of norms of good behavior on the part of the states. Research and innovation on cybersecurity technologies has been jointly funded by collaborative projects under the EU's Horizon 2020 program. The 2020 India-Japan Cybersecurity Agreement made it explicit of their commitment to increase capacities building, research and development and protection of critical infrastructure.

India has emphasised its commitment to work jointly with Australia in stemming cybercrime and in ensuring safe use of new technologies in the two countries' respective regions. India Australia Framework Arrangement on Cyber and Cyber Enabled Critical Technology Cooperation and Cybercrime prevention, capacity building, international cyber policy development sector involved . At the same time, cybersecurity is part of India's longstanding relationship with Russia. It has been dialogues by the two countries to discuss cyber threats and to examine means of cooperative efforts to provide a secure cyberspace.

7. INDO-PACIFIC CYBERSECURITY INITIATIVES AND THE QUAD

It has become a strategic grouping of four members: India, the United States, Japan and Australia—that has emerged as a key platform on addressing cyber security challenges of the Indo-Pacific region. The Quad's agenda is centered on cybersecurity: the region is vulnerable to cyberattacks and protecting digital connectivity has taken on strategic significance. In its Quad commitments, India has taken initiatives to bolster regional cyber resilience, share intelligence on cyber threat, and develop frameworks for the foundation of trust in the digital infrastructure. The members of the Quad have also talked about steps to stop economic spying via the cyber domain and to make sure the supply chains for critical technologies are verifiable. Recently in meetings, followers of the Quad Cybersecurity Partnership were announced which aims to coordinate security efforts to secure critical infrastructure and implement the best practices over the region. India's work to promote the Indo-Pacific Cyber Capacity Building Framework (to which ICC'11 in Bangalore 2019 will apply) reinforces India's strong leadership in the Indo-Pacific. As part of this initiative the team is providing their technical assistance, training, and resources to the countries in this region to help them in strengthening their cybersecurity defenses and protect their digital economies.

8. CYBER SOVEREIGNTY AND OPEN INTERNET PRINCIPLES

The focus of India's cybersecurity diplomacy lies in balancing proclamations for cyber sovereignty with support for the open and secure and inclusive internet. India understands the value of state control over digital assets and data, and national interest in transnational cyber threats but also believes that it should rely on global cooperation. The balancing act was evidenced in India's approach to data localization and cross border data flows. India's commitment to protecting citizens' data, while fostering a digital economy is reflected by the proposed Personal Data Protection Bill. It is a local data push by India since India considers the matter of privacy, security and national interest. But India too has been trying to also engage with global stakeholders to address fears of an economic hit for such policies.

With India participating in discussions on digital trade, digital data governance and cross border data flow frameworks, this shows that India wants to find some common ground. India works with partners to develop international standards and best practices so that its domestic priorities can be reconciled with those of the world. The multi stakeholderism in internet governance captures the Indian approach to strike a balance between state interests and private and civil society interests.

9. GLOBAL ENGAGEMENT BY DOMESTIC CAPACITY

India has spent heavily in constructing its cybersecurity infrastructure – as a step towards which the Defence Cyber Agency (DCA) was brought into being to handle cyber warfare and security threats faced by the military. India has also launched push to increase cyber literacy, train cybersecurity personnel and encourage research and development in advanced public technologies. Through the Cyber Surakshit Bharat programme, the cybersecurity ecosystem is being strengthened by training government officials and making people aware about best practices. Fostering innovation and skill development, its goal is to create Centre's of Excellence in cybersecurity across academic institutions. Indian tech

companies and startups have been at the forefront of developing cutting edge solutions for domestic security, and export potential. They allow public to share resources with private sector and knowledge exchange, thereby improving India's overall cyber readiness. India's showcasing of its expertise and resources places it as the leader in forming the global cybersecurity agenda. In the evolving world of cyber threats, India sees the need to couple cyber capabilities with its defense. But the handling of cyber threats and offensive operations falls to the Defence Cyber Agency, which is part of the Integrated Defence Staff. The development of cyber warfare as an integral part of India's military doctrine stipulates the requirement of readiness for defensive and offensive cyber operations along with cyber defense for the cyber protection of critical defense infrastructure and networks against espionage and sabotage.

10. CYBERCRIME AND CYBERTERRORISM

Due to growing number of targets, unlike China, India faces considerable threats from cyber criminals and cyber terror travels as non-state actors are using cyberspace for unlawful operations. The measures aimed at countering such threats include the improvement of legal measures, development of enforcement as well as cooperation with other governments. India is a signatory to many an international treaty and protocol which deals with issues of cybercrime including the Budapest Convention on Cybercrime. Despite, India being a non-signatory country it diplomat with states and international organizations in a bid to adjust its domestic laws and policies to the global norms. National laws including Information Technology Act, 2000 has been further revised concerning the cyber- crimes and to enforce the forces. Besides, cooperation with other organizations that have operational control over the regional security, such as Interpol, and equal cooperation agreements with other states allow exchanging the information about the criminals and providing the joint actions against the cybercriminals. The two visions are not contradictory; rather the Indian government actively participates in the anti-terrorism international forums especially on financing of this menace and radicalization.

11. ISSUES ENCOUNTERED AND THE FUTURE STRATEGIES

The challenges that India is experiencing as regards to cybersecurity diplomacy. These challenges include geopolitical rivalry in South Asia, increasing threats from fifth generation cyber threats and the absence of a broad international cyberspace framework. Moreover, convincing people to trust AI is challenging also due to the constantly growing speed of technological development manifested in innovations like Artificial Intelligence and Quantum Computing. A similar issue can be identified within India where the digital divide becomes another weakness which can be amplified due to differing uses of technology and understanding. It is for this reason that efforts aimed at eliminating these disparities are central to the formulation of strategies to develop sound national cybersecurity frameworks. India simply cannot afford to rest on its laurels while China continues to build ever stronger and more intricate webs of alliances, negotiates new international and regional arrangements in various forums, and increases investment in cutting-edge technology and applications. Building up the cooperation with other departments and industries, especially focusing on the cooperation with academies and reconstruction of partnership with industrial field will also be conducive to regulating the competitive edge in cybersecurity domain. It's important for India to help support the formation of international standards and legal structure that is favorable for the developing nations. In this way, India can take an active part in defining the principles of the new world cyber-governance and make the tendencies of the global cyber-governance not only acceptable, but also fair for other states.

12. STRATEGIC SUGGESTIONS FOR THE STRENGTHEN OF CYBERSECURITY DIPLOMACY

- Incorporating contemporary issues and dynamics in the Draft National Cyber Security Policy, will offer a blueprint for domestic and international dynamics.
- Financial allocation to education and training to build a professional population in cybersecurity profession will enhance capabilities to support diplomacy in India.
- Mainly, such a structure will promote the involvement of the private sector, academic institutions, and civil society in the policy-making process, as well as guarantee that new and heterogenic ideas will be applied.
- Harmonisation of Indian laws with international standards and strengthening mechanisms will boost India's performance in combating cybercrime and partnering internationally.

- Engagement in the process of constructing International Cyber norms might enable India to have a formidable influence on the policies as per his interest and values.
- Focusing on research and development in AI, quantum computing, and other emerging fields will position India as a leader in next-generation cybersecurity solutions.

13. CONCLUSION

These efforts reflect a nascent but clear India's cybersecurity diplomacy aims at protecting the country's internet sovereignty and at the same time promoting global cyber security. Through multilateral diplomacy, India is establishing itself in the framework of the management of the cyber universe. Pursuing the challenges and opportunities opened by digitalisation, India's active participation in the sphere of cybersecurity diplomacy will play significant role in building the effective, protective, and inclusive digital world order. However, the interpretation of national interests and global duties enable India to contribute effectively to the defining of rules governing the use of cyber space for peace and stability of the world. Indeed, India understands that cyberspace is complex and cybersecurity is not just an endogenous techno-navigational problem, it is governance and geopolitics; cyber is also a diplomacy, economics, and social dynamic. This before us calls for continual engagement, teamwork and outlook for new frontiers in the information superhighway. India's actions and intentions of cybersecurity diplomacy are not only about the future of becoming a global power, but about the purpose of making technology about positivism, not pessimism and building a safer stronger world.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Basu, A. (2019, November 7). India's role in global cyber policy formulation. Lawfare. Retrieved from https://www.lawfaremedia.org/article/indias-role-global-cyber-policy-formulation

Callanan, C., Chandola, B., Ebert, H., Heinl, C., & Sarma, A. (2022, October 19). Enhancing global cybersecurity cooperation: European and Indian perspectives. Observer Research Foundation. Retrieved from https://www.orfonline.org/research/enhancing-global-cybersecurity-cooperation

Jindal, D., & Soliman, M. (2023, July 6). Understanding the growing Indo-Israeli strategic cyber partnership. Middle East Institute. Retrieved from https://www.mei.edu/publications/understanding-growing-indo-israeli-strategic-cyber-partnership

Manzoor, P. T. (2023, June 28). Bridging the digital divide: India's role in global cyber diplomacy. Youth Ki Awaaz. Retrieved from https://www.youthkiawaaz.com/2023/06/bridging-the-digital-divide-indias-role-in-global-cyber-diplomacy/

Mukerji, A. (2018, April 4). International cooperation on cyber space: India's role. Ministry of External Affairs, Government of India. Retrieved from https://www.mea.gov.in/distinguished-lectures-detail.htm?743

Patil, S. (2023). India's cyber diplomacy comes of age. Observer Research Foundation. Retrieved from https://www.orfonline.org/expert-speak/indias-cyber-diplomacy-comes-of-age

Tikk, E., & Kerttunen, M. (Eds.). (2020). Routledge handbook of international cybersecurity. Routledge.