Cyber-Diplomacy: A Crucial Step Forward in the International Relations of India

Dr Preethi Amaresh[@]

Abstract

As the world is undergoing a drastic technological shift in the 21st Century, emerging technologies have occupied a prominent position in international relations as well. Due to this, 'Cyber Diplomacy' (CD) in this regard has come to play a crucial role between nation-states and is still in a developmental stage in public diplomacy and is hence called 'Public Diplomacy 2.0'. Cyberspace is further becoming increasingly post-liberal due to the gradual shift in the global order. CD has likewise taken over much of the global political system over the last several years and has become an essential segment in today's world as many countries have acknowledged the importance of engaging with other countries including India. Several countries' foreign ministries have also appointed 'Cyber Diplomats' due to the advancement of technology in geopolitics and the increasing politicisation of cyberspace. CD is indeed paramount for maintaining the long-term resilience of cyberspace in the facade of increasing threats from nation-states.

Introduction

The world is moving at a brisk pace with the 'Fourth Industrial Revolution' acting as a catalyst, heading to a 'Great Technological Transformation'. Cyber Diplomacy (CD) is considered the zenith of foreign policy in the 21st Century, beneficial for

[@] **Dr Preethi Amaresh** is a Political Scientist, author of four books and graduated with a Doctorate from Geneva, Switzerland. Presently, Dr. Amaresh works as a Lead (Tech Policy, Law, Internet Governance and Diplomacy) at the CyberPeace Foundation- United Service Institution of India, Headquarters (New Delhi, India). She is also a columnist of several articles published at national and international platforms. Her interests include Geopolitics, Soft Power and Artificial Intelligence.

Journal of the United Service Institution of India, Vol. CLIV, No. 635, January-March 2024.

countries in a competitive geopolitical backdrop. As the international borders have become blurred to a point in the era of globalisation, countries are employing it for their advancement, which has impacted international relations of the world in an incredible way. Today, diplomacy has grown to include unexplored domains of policies related to cyber security. As countries have increased their presence in digital aspects, cyber security has paved its pathway to become paramount in their foreign and security policies. CD is the art, the science, and the means by which nations, groups, or individuals conduct their affairs in cyberspace to safeguard their interests and promote their political, economic, cultural or scientific relations, while maintaining peaceful relationships according to European Union (EU) CD toolbox.[1]

Currently, CD is still in a developmental stage in public diplomacy and is hence called 'Public Diplomacy 2.0'. It is also called virtual diplomacy, digital diplomacy, or more typically comprehended as e-diplomacy. The emergence of the following domain began as several foreign ministers have set up offices exclusively devoted to cyber-space and have assigned 'Cyber Diplomats' in the former years due to the increasing politicisation of cyber-space and more comprehensive techno-geopolitical dynamics. The foremost government document to focus on the global facets of cyber threats was the journal of the 'United States (US) International Strategy for Cyberspace' which brought out the onset of CD. The following strategy delineates several areas such as law enforcement, military etc., and further relies on three pillars consisting of Defence, Diplomacy and Development. CD has taken over much of the global political system over the last several years and has become an essential segment in today's world as many countries have acknowledged the importance of engaging in it with other countries.[2] But, the feasible consequences of this differ considerably depending on the country involved as to whether they are engaged in offensive or defensive strategies.[3] Japan, the US, Singapore, and South Korea believe it would enable world peace via cooperation.[4] In addition to traditional methods of diplomacy, CD thoroughly affects international relations by delivering an alternative communication medium for governments.[5] Nonetheless, cyber diplomats do not enjoy the same level of trust as compared to traditional diplomatic channels.[6] On the contrary, CD can also negatively impact international relations if a country discovers that another country has been trying to spy.[7] The 1983 movie 'War Games' and 1993 publication 'Cyber War is Coming' by Arquilla and Ronfeldt accentuated the role of cyber warfare as a looming danger.[8] In the present scenario, several major powers want to shape cyberspace as per their national interest and overpower the area of digital realm.[9]

CD and Global Order

Cyberspace is further becoming increasingly post-liberal due to the gradual shift in the global order in the hot off the press digital age. While the liberal global order (western dominated institutions) facilitated the expansion of cyberspace, the shift towards a post-liberal order has witnessed the 'Dawn of CD' in the present era. Several countries' foreign ministries have also appointed 'Cyber Diplomats' due to the advancement of technology in geopolitics and the increasing politicisation of cyberspace. It is used to thwart cyber attacks through persistent dialogue in a world where more countries are acquiring offensive cyber capabilities. The basic components in the CD toolbox are confidence-building efforts, cyber capacity building and the evolution of cyber standards. Cyberspace is both complicated and constantly evolving compared to traditional extents of land, sea and air where diplomacy set the firm foundation of the state's normative exchange. Also, the partnership in this domain has been fractured and off-the-cuff. Diplomatic strategies towards cyberspace are further fraught with convoluted challenges.

In the cut-off-the edge era, CD may enhance global amicability, whereas if cyberpunks acquire key to top government or secret military programs, this could direct to ruinous outcomes. Importantly, countries that do not utilise it are more potentially prone to get into confrontations or warfare, being unaware of the rival threats. Therefore, it is indeed paramount for maintaining the long-term resilience of cyberspace in the facade of increasing threats from nation-states. Some of the major types of cyber threats include click jacking, spyware, man-in-middle attacks, ransom ware, zero-day, denial of service attacks etc.

CD is to cyberspace what diplomacy is to international relations.[10] The net of it is dilating and heightening swiftly, creating a cyber-international society. However, its role is much less evident in the media today than the cyber-attack incidents. Collaboration in cyberspace is consequently a ‘Choice’. In the present geopolitical scenario, its future poses a path of enigma and dilemma that comprises both challenges and opportunities and countries must focus on it as a way to build the future of international relations in the ‘Age of Technological Revolution’.

CD contains measures to facilitate global standards, norms, and regulations in cyberspace, foster collaboration and avert cyber conflicts among countries to tackle cyber perils.[11] It is an inescapable instrument for less-capable countries in the contemporary epoch. Cyber operations are further not curbed by geographical frontiers and collaboration is vital to address increasingly complicated hazards. It is also an integral instrument for less-capable countries to showcase ‘Soft Power’ by shaping the foreign policy discretions of other countries through values, culture and approaches instead of coercion or sanctions. Though CD is crucial for countries, it has myriad challenges such as diverse stances among countries, lack of enforcement tools, gap in cyber security capacity, and difficulty in determining the basis of cyber attacks. International organisations like the United Nations (UN) and structures such as the Freedom Online Coalition[12] play a momentous part in it. Likewise, it is essential to incorporate non-state actors (civil society, private sector and academia).[13] The UN norms for accountable state behaviour in cyberspace are a substantial international initiative to take the edge off cyber threats and conflicts.[14]

The Role of India in CD Domain

CD is nonetheless considered a new notion for countries. India has adequately proved itself as a nation with a reliable technology ground and is vigorously assuming its role in digital and cyber-related matters at multilateral platforms and global level.[15] The CD Division of the Ministry of External Affairs (MEA) is a specialised branch dealing with global cyber governance matters, further engaged in several international forums besides the UN.[16] India has also had cyber dialogues with different countries, such as Germany, Australia, Japan, and the US etc., and has been vocal in the global forums about diving into dangers posed by cyber terrorism/crimes.[17] Furthermore, India and Israel have ventured on a shared task to improve their bilateral strategic cyber partnership.[18] The Indo-Israeli cyber partnership has steadily heightened through private-sector cooperation and investment.[19] Some of the examples of the collaborations include Cymulate, Coralogix and Think Cyber India.[20] In West Asia, India is seeking to expand technical cooperation with the United Arab Emirates in cyberspace in both public and private sectors.[21] India and EU in 2023, discussed cyber cooperation and mechanism in multilateral and regional discussions.[22] India and Netherlands held the second cyber dialogue in New Delhi.[23] The Fifth Japan and India Cyber Dialogue was held in 2023 virtually to discuss cyber security strategies.[24] The G20 nations have further aimed at protecting against global cyber threats.[25] Similarly, India and Australia are taking their bilateral ties to an exceptional deck by collaborating in bilateral trade, cyber security and Artificial Intelligence (AI).[26] India and the United Kingdom have also pushed forth to boost partnership in the cyber realm.[27]

Collaboration on cyber matters is also known to be a critical element of the bilateral relationship between India and the US.[28] Both countries have developed a wide-ranging strategic coalition that echoes their common values, democratic practices, national security and economic interests, and shared vision and regulations for cyberspace. Therefore, as part of CD, India should forge ahead further through 'Techno-Diplomatic Countries' to bolster its diplomatic collaborations that could help in addressing the rising cross-border cyber hazards securing international cyberspace. India has also been lately engaging in activities with the civil society, private sector and academia to design strategies for cyber policy and has further set up the centres of excellence and institutes of technology in several countries.

CD, thus, plays a monumental role in shaping the international ties of India. Much of the emphasis has been on shoring up domestic cyber security soundness and increasing capacity, which has been the priority of the diplomatic contributions overseas for India. The MEA and Ministry of Electronics and Information Technology have focused on cyber security through four initiatives such as the creation of cyber norms, managing internet governance, fostering the digital economy and focus on capacity-building. The digital public infrastructure such as the United Payment Interface, RuPay, etc., have performed an outstanding role in enhancing the CD of India forging new alliances, and magnifying the international position of the country. The MEA has also taken an advanced step in establishing the New and Emerging Strategic Technologies Division, a transformative step indeed in the era of the ‘Fourth Industrial Revolution’. Several top think tanks have also been proactive in the CD domain. In this milieu, the leading think tanks of India, the United Service Institution (USI) and the India Future Foundation have signed a Memorandum of Understanding to promote cyber security, CD, strategic affairs, defence security, privacy and data protection.[29] According to Major General (Dr) Pawan Anand, AVSM (Retd), Distinguished Fellow, and Head USI-Centre for Atmnirbhar Bharat, “The tremendous growth of cyberspace in India and the opportunities it has to offer is also fraught with danger”. In the new-fangled era, diplomacy in India has invariably accorded a prominent position to the state in its path to international negotiations. Nevertheless, the country has been ambiguous regarding apertures in international cyber security negotiations. Many multi-stakeholders such as civil society, government, private sector and media have not certainly defined the interest on how India can bring to global negotiating tables regarding the cyber security ecosystem.

Also, CyberPeace Foundation (CPF), one of leading organisations of India has been deeply involved in the cyber security domain. Furthermore, India has made momentous strides in the domain of technology, while cyber security remains a significant challenge presently according to Major Vineet Kumar, Founder and Global President of the CPF.[30] Furthermore, according to Kumar, the CPF works to combat cybercrime, cyber weapons, cyber warfare, and cyber terrorism on an international scale. Thus, CPF endeavours to make the internet a more protected, long-lasting, reliable and inclusive establishment for all cybernauts throughout the world. The organisation has often cooperated with government organisations, citizens, private companies, universities, non-government organisations, cyber security experts etc. The four pillars of CPF are Innovation and Research, Cyber Policy, Advocacy and Diplomacy, Inclusion and Outreach, Collaboration and Connection. The organisation has been further steering cyber exercises developed to enrich the cyber capabilities of countries, allowing them to engage and dissuade cyber attacks on their networks and infrastructure. Importantly, CPF aims to bring out first of its kind ‘Cyber Security Index’ which aims to grade countries and also the Indian states in the cyber security domain.

In the current geopolitics, as the bridge between the global North and South, India wants to contribute to cyberspace stability and has further exhibited to the world that technology can be harnessed for the greater good. The CD of India is seeking for 'Rules Based Order' in cyber-space and has also proposed a 'National Malware Repository' as a reference database to combat ransom ware and malware. Furthermore, the evolution of information and communications technology has led to new transformations in the domain of cyber-space and the global south has seen the quickest growth in internet users; however, it remains most susceptible to cyber hazards due to the absence of cyber capacity. India has acknowledged this quandary of the global south in cyberspace and has, therefore, assumed an alternative strategy established on active engagement and cooperation with a certain emphasis on the Global South in cyberspace. The principal pillar of the cyber approach in India lies in increasing the cyber capacity building in the global south countries. India through the Indian Technical and Economic Cooperation programme is also providing cyber security training, which concentrates on South-South Cooperation and capacity building, consisting of many fellow countries of Asia, Africa, and Latin America.

India has further integrated cyber security into the agenda of the Bay of Bengal Initiative for Multi-sectoral Technical and Economic Cooperation and The Indian Ocean Rim Association. Similarly, though the South Asian Association for Regional Cooperation (SAARC) countries have not yet set up regulatory governance and cyberspace risk management think-tank, Nepal (a SAARC member) and India have collaborated in modifying their cyber security goals via Track 1, Track 2 and Track 3 diplomacy.[31]

India, being the home to the largest world population, the government ought to design a cyber security strategy keeping in mind the national security of the country besides focusing on internet governance, cyber attacks, crypto currencies, data privacy and promoting a precise international framework for CD. Despite the wave of cyber attacks in India, the government has yet to put forth the 'National Cyber Security Strategy'. The government should consider elevating India as a trademark and reliable performer in the cyber security domain. The government is also required to drastically increase the 'Budgetary Provisions' in the cyber security domain. The government should further provide federal funds to the states to enhance cyber security capabilities. India sets to become a global leader in CD, being one of the fastest-growing digital economies and home to an extensive reservoir of young tech talent.

Moving ahead, the 'National Security' for any country is always considered to be a top priority and maritime security also becomes very crucial to preserve the national security of India. Therefore, 'Maritime Cyber Security' is one of the critical areas with India playing a prominent role in the Indian Ocean Region. The country should likewise collaborate with other countries through platforms such as Quadrilateral Security Dialogue, Asia Africa Growth Corridor etc., to strengthen its CD and avert cyber-attack incidents, particularly against the growing threat from China. From the ancient to the contemporary era, 'War' has been a recurrent happening in the history of world and 'Cyber Warfare' is the modern era 'Warfare' and India ought to brace up for the new era warfare by increasing its state-of-the-art capacity building to avert future cyber attacks. The 2023 'India Threat Landscape Report' by Singapore-based cyber security firm Cyfirma states that India is the most targeted country internationally, facing 13.7 per cent of all cyber attacks.[32] State-sponsored cyber attacks against India grew by 278 per cent between 2021 and Sep 2023, with several Information Technology (IT) companies witnessing the most heightened percentage of cyber attacks. Also, the COVID-19 pandemic years led to several challenges and threats across the world including a strong upsurge in cyber attacks. CD inexorably poses a possible threat to democratic governments. For instance, China has been using its 'Sharp Power' in waging cyber attacks on India, Australia, and the US etc. However, in a recent report, India, Taiwan and the US have stepped up to counter the cyber threats from China.

The advancement of technologies such as the AI, Big Data, and the Internet of Things has led to protecting the personal data has become very critical. In this context, the Indian government in 2023 passed the much-awaited 'Data Protection Bill'.[33] The Supreme Court of India further stated that the citizens have a fundamental right to privacy, ensured principally under Article 21 of the Indian Constitution.[34] Similarly, the IT Act, 2000 that focused mainly on cyber crime and electronic commerce introduced new provisions in the 2008 amendment including cyber terrorism to protect the Indian citizens. The following act was administered by the Indian Computer Emergency Response Team to guide the Indian cyber security legislation, put forth data protection policies, and oversee cybercrime. In a special petition filed in 2021, the Supreme Court of India ruled that cyber attacks and data thefts is an offence under the IT Act of 2000 and the Indian Penal Code. As India does not have an exclusive cyber security law, it utilises the IT Act and several other sector-specific laws concerning cyber security measures. In 2013, the 'National Cyber Security Policy' set up security framework for public and private institutions to ably safeguard themselves from cyber attacks. The 'National Cyber Security Strategy' of 2020 aimed to further improve cyber security measures. At the Open-Ended Working Group established by the UN General Assembly, India has proactively advocated the necessity for the UN members to design shared insights on how international law applies to cyberspace under the auspices of the UN. However, the strategy and approach of India to cyber norms formulation will need periodic evaluation due to the largely expanding technology and security transitions in the country and overseas. Vigorous engagement supported by a dynamic multi stakeholder ecosystem will facilitate the crafting of international cyber security governance embedded in the strategic and diplomatic requirements of India.

Through the ongoing National Cyber Security Policy (2020-2025), India has the prospects to align its domestic policy with its international aspirations.[35] Indispensably, while the cyber security initiatives of India have been predominantly defensive, the government should however increase the ability for 'Offensive Pursuits' to deal with state and non-state threats.[36] The Ministry of Home Affairs and also the Ministry of Defence should be altogether prepared to handle the increasing cyber attacks and also contemporising to avert such threats in the coming years in the present unstable geopolitical setting. Presently, as per the State of Cyber Security 2023 report by Information Systems Audit and Control Association, 40 per cent of Indian cyber security teams are understaffed.[37] Consequently, in this regard the Indian government should consider increasing the openings in the cyber security domain focusing on research and development in both technical and non-technical segments. Furthermore, as India has often been facing two front cyber threats from Pakistan and China, it becomes really crucial to India to strengthen its cyber security and leading-edge technology capabilities. The role of Public-Private Participation is further essential to shape the CD of India in several aspects. In this context, the Indian National Security Council Secretariat has recently released proposals by a collaborative public-private working group on cyber security that sought to bolster the capability to curb the increasing threats from cyberspace. Also, the regular involvement of armed forces along with bureaucrats, diplomats and the other government agencies in devising cyberspace strategies is highly crucial.

Conclusion

On the whole, India in the 'Multipolar world order' must thus consider playing the role of a 'Rule-Shaper' apart from actively supporting the rising powers to increase cooperation in CD and also create awareness among the citizens about its risks.

Endnotes

[1] "What is cyber diplomacy?", Cyber Diplomacy Toolbox. https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html#:~:text=Cyber%20diplomacy%20is%20the%20art,relations %2C%20while%20maintaining%20peaceful%20relationships

[2] Bhattacharya, Arindam. "Cyber-diplomacy and International Relations: The Good, the Bad, and the Ugly". Advocacy Unified Network. September 2, 2021. https://doi.org/10.57939/NSHH-5853

[3] Ibid

[4] Ibid

[5] Ibid

[6] Ibid

[7] Ibid

[8] Cameran Ashraf. "Defining cyberwar: towards a definitional framework", *Defense & Security Analysis*, 37:3, (August 2021) 274-294. 10.1080/14751798.2021.1959141

[9] Ibid

[10] Barrinha; Renard. "Cyber-diplomacy: the making of an international society in the digital age", Global Affairs, 3:4-5, (July 2017): 353-364. 10.1080/23340460.2017.1414924

[11] Domingo, Francis. “Diplomacy in the time of cyber conflict”. East Asia Forum. June 2, 2022. https://eastasiaforum.org/2022/06/02/diplomacy-in-the-time-of-cyber-conflict/

[12] “Freedom Online Coalition”. Wikipedia. https://en.wikipedia.org/wiki/Freedom_Online_Coalition

[13] “Cyber Diplomacy and Cyber Foreign Policy”, Stiftung Neue Verantwortung, https://www.stiftung-nv.de/en/subproject/cyber-diplomacy-and-cyber-foreign-policy

[14] Hogeveen, Bart. “The UN norms of responsible state behavior in cyberspace”. March 22, 2022. Australian Strategic Policy Institute. https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

[15] “India excelling in the art of Cyber Diplomacy”. DD India. August 14, 2023. http://ddindia.php-staging.com/india-excelling-in-the-art-of-cyber-diplomacy/

[16] Ibid

[17] “India acing the game of Cyber Diplomacy”, Niti Post, March 31, 2023. https://nitipost.com/news/india-acing-the-game-of-cyber-diplomacy

[18] Jindal, Soliman. “Understanding the growing Indo-Israeli strategic cyber partnership”. Middle East Institute. July 6, 2023. https://www.mei.edu/publications/understanding-growing-indo-israeli-strategic-cyber-partnership

[19] Ibid

[20] Ibid

[21] Ahuja, Namrata Biji. “How India, UAE, Israel are trying to build secure cyberspace”. The Week. July 16, 2023. https://www.theweek.in/theweek/specials/2023/07/08/building-a-secure-cyberspace-through-the-india-uae-israel-cyber-security-partnership.html

[22] “India, EU discuss cyberspace and combating the criminal use of ICTs”. DD News. October 6, 2023. https://ddnews.gov.in/international/india-eu-discuss-cyberspace-and-combating-criminal-use-icts

[23] “India, Netherlands hold 2nd Cyber Dialogue in New Delhi”. ANI News. February 3, 2023. https://www.aninews.in/news/world/asia/india-netherlands-hold-2nd-cyber-dialogue-in-new-delhi20230203201044/

[24] “Fifth India-Japan Cyber Dialogue”. Ministry of External Affairs. September 14, 2023. https://www.mea.gov.in/press-releases.htm?dtl/37119/Fifth_IndiaJapan_Cyber_Dialogue

[25] Patil, Sameer. "India's cyber security priorities for G20 Presidency". Observer Research Foundation. December 4, 2022. https://www.orfonline.org/expert-speak/indias-cybersecurity-priorities-for-g20-presidency

[26] "India-Australia taking bilateral trade, cyber security & AI inter alia, to new heights", Ministry of External Affairs, December 6, 2020. https://indbiz.gov.in/india-australia-taking-bilateral-trade-cybersecurity-ai-inter-alia-to-new-heights/#:~:text=Australia%20and%20India%20plan%20to, at%20the%20Bengaluru%20Tech%20Summit.&text=India%20and%20Australia%20signed%20a,intelligence%2C%20internet%20of%20things%20etc

[27] "India, UK agree to deepen cooperation in cyber domain". Economic Times. November 26, 2021. https://cio.economictimes.indiatimes.com/news/digital-security/india-uk-agree-to-deepen-cooperation-in-cyber-domain/87922212

[28] "Framework for the U.S.-India Cyber Relationship", U.S Embassy and Consulates in India. https://in.usembassy.gov/framework-u-s-india-cyber-relationship/

[29] "India Future Foundation and United Service Institution of India sign MoU to promote digital diplomacy, cyber security", Financial Express. September 27, 2022 https://www.financialexpress.com/business/defence-india-future-foundation-and-united-service-institution-of-india-sign-mou-to-promote-digital-diplomacy-cyber-security-2692916/

[30] Das, Kumud. "Ransomware attacks on startups, MSMEs on the rise in India: CyberPeace Foundation". Bizz Buzz. November 3, 2023. https://www.bizzbuzz.news/bizz-talk/ransomware-attacks-on-startups-msmes-on-the-rise-in-india-cyberpeace-foundation-1261320

[31] Sarkar, Sreemoyee. "Indo-Nepal Cyber Diplomacy and Regime Formation". Political Reflection. July 3, 2021. https://politicalreflectionmagazine.com/2021/07/03/indo-nepal-cyber-diplomacy-and-regime-formation/

[32] "State-Sponsored Cyber Attacks Against India Went Up by 278% Between 2021 and September 2023: Report". The Wire. November 6, 2023. https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report

[33] Burman, Anirudh. "Understanding India's New Data Protection Law". Carnegie India. October 3, 2023. https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624#:~:text=Introduction-,In%20early%20August%202023%2C%20the%20Indian%20Parliament%20passed%20the%20Digital,(DPDP)%20Act%2C%202023

[34] Subramaniam and Associates. “In a nutshell: data protection, privacy and cybersecurity in India”. Lexology. October 9, 2023. https://www.lexology.com/library/detail.aspx?g=174412a6-fa19-4055-90f9-dec6bb229ac1

[35] Waghre; Mehta. “India’s National Cybersecurity Policy Must Acknowledge Modern Realities”. The Diplomat. December 20, 2019. https://thediplomat.com/2019/12/indias-national-cybersecurity-policy-must-acknowledge-modern-realities/

[36] Nachiappan. “Going on the Offensive: India’s Cyber Capabilities”. Institute of South Asian Studies- National University of Singapore. December 29, 2022. https://www.isas.nus.edu.sg/papers/going-on-the-offensive-indias-cyber-capabilities/

[37] “40% Of Cyber security Teams Are Understaffed In India: ISACA Research”. NDTV Profit. October 9, 2023. https://www.ndtvprofit.com/technology/40-of-cybersecurity-teams-are-understaffed-in-india-isaca-research