BTTN Journal
p-ISSN 2958-1214
e-ISSN 2958-1222

RESEARCH ARTICLE

Pakistan and the New Frontier of Cyber Diplomacy: Challenges and Strategic Opportunities

Habib Ur Rehman [1] & Abdul Wadood[2]

Article Info

Keywords:
Cyber diplomacy, Cybersecurity policy, Pakistan foreign policy, Digital governance, international cyber norms, strategic communication, Cyber threats

Abstract

This study examines cyber diplomacy as a strategic tool in the realm of contemporary international politics in the context of its importance for Pakistan amid the dynamic and growing cyber environment. With a qualitative and library-based research methods reinforced by real-life policy observation, this paper critically examines how cyber diplomacy can contribute to multi-stakeholder cooperation and norm development in cyberspace. It pinpoints Pakistan's key challenges such as legal lacunas, underdeveloped cyber capacity and poor strategic communications but also opportunities in the areas of digital governance, economic growth and regional cooperation. The study recommends that there is a need for a unique cyber diplomacy division, robust legal underpinning, and mainstreaming of cyber strategies in Pakistan's foreign policy objectives. Finally, the study adds to the nascent literature on non-conventional diplomacy by providing policy-relevant insights specific to Pakistan's cyber future.

[1] Habib Ur Rehman is the Master of Science graduate in International Relations from the Balochistan University of Information Technology, Engineering, and Management Sciences (BUITEMS), Quetta. He can be reached at habib.edyfk@gmail.com.

[2] Prof. Dr. Abdul Wadood is the Professor at the Department of International Relations, Balochistan University of Information Technology, Engineering, and Management Sciences (BUITEMS), Quetta. He can be reached at abdul.wadood@buitms.edu.pk.

Introduction

In a world becoming more and more digitized and networked, cyberspace is taking on the character of an important international relations, diplomatic, and competitive strategic area. An increase in cyber threats, cyberespionage, information warfare and cross-border technology influence have in turn led to the transformation of traditional diplomacy to forms such as cyber diplomacy. No longer restrained to conventional forms of bilateral or multilateral engagement, contemporary diplomacy is required to grapple with the governance, security and ethical complexities of the digital age.[1] The rapid growth of cybersecurity has proved challenging for conventional diplomatic and international relations mechanisms, created during times when borders were physical and people travelled to meet.[2] As international powers institutionalise their strategic cyber diplomacy and become involved with the norms setting initiatives, for instance at United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG), developing countries encounter acute challenges, as well as opportunities, in aligning to this trend.[3] For Pakistan in its vantage point as a place where strategic rivalries intersect and form, becoming digital ecosystems, the new frontier of cyber diplomacy presents a two-edged path: one hampered with institutional, legal, and infrastructural constraints, and a growing one filled with multiplied promises of geopolitical relevance, digital sovereignty, and regional leadership[4]. Despite some development — for example, the launch of the National Cyber Security Policy 2021[5] — the Pakistani approach is mostly reactive, fragmented, and unrefined. The state lacks proactive participation in international cyber norm-building, its under-development of technical–

[1] Evan H. Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century* (Montreal: McGill-Queen’s University Press, 2002), https://books.google.com.pk/books?id=OdfOi3LtoZQC.

[2]Amel Attatfa, Karen Renaud, and Stefano De Paoli, “Cyber Diplomacy: A Systematic Literature Review,” *Procedia Computer Science* (2020), https://doi.org/10.1016/j.procs.2020.08.007.

[3] United Nations, “Group of Governmental Experts (GGE) Reports,” United Nations Office for Disarmament Affairs, accessed March 01, 2025, https://unoda.org/.

[4] Shahzad Munir, Muhammad Asghar Mahmood, and Rimsha Malik, “Cyber Diplomacy: Forging Pakistan’s Foreign Policy in the Digital World,” *Journal of Strategic Policy and Global Affairs* 4, no. 1 (2023): 43–60, https://jspga.com/index.php/jspga/article/view/22.

[5] Government of Pakistan, *National Cyber Security Policy 2021*, Ministry of Information Technology and Telecommunication, https://moitt.gov.pk/.

diplomatic capacity, and vulnerability to transnational cyber risk, highlight serious amenability within national level preparedness.[6]

Due to the consequential problem as a result of cyberspace, cyber diplomacy is the strategy needed, which employs diplomatic methods and a diplomatic perspective.[7] Cyber diplomacy employs the same tools and approaches used across discussions, bargaining, and consensus in traditional diplomacy to solve specific problems unfolding in cyberspace like hacking and battles of law in place of just regulation. This paper covers the complexity of the cyber domain and the concepts of the digital age to comprehend this area and option strategically. As we delve into the merits of cyber diplomacy, characterized by international cooperation, multi-stakeholder, and the development of norms for proper behaviour in the cyberspace, it is essential to highlight the shortcomings of the traditional diplomacy in addressing the issues. After that, Pakistan will be the centre of attention in this paper since it is where the two coinages meet. Considering cyber diplomacy, this paper discusses the specifics of the country. In other words, developing capacity in a technical workforce, stringent enforcement of cybersecurity laws and policies, and increased online safety awareness among the general public is involved. We will also elaborate on the importance of strategic relationships with other countries to learn from each other's experiences, intelligence reports regarding threats, and national defence potential against potential cyberattacks. Integrating cyber diplomacy and cyber security considerations as a part of foreign policy goals may make possible for Pakistan to position itself as a responsible player in the digital sphere. The subsequent sections will present a detailed guide on the way to the digital future for Pakistan, with specific recommendations, and a focus on the potential benefits of a holistic approach to cyber diplomacy for its diplomatic achievements in the emerging digital order.

[6] Muhammad Waqar Anwar and Umair Pervez Khan, "Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward," *Cyberpolitik Journal* 5, no. 10 (Winter 2020): 205–225, accessed July 2025, https://www.researchgate.net/publication/378125009_CYBERSECURITY_IN_PAKISTAN_REGULATIONS_GAPS_AND_A_WAY_FORWARD.

[7] Shaun Riordan, "Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction," *USC Center on Public Diplomacy*, May 12, 2016, accessed 2025, https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacyterminological-distinction.

Methodology

This article uses a qualitative research method and relies mainly on library studies and research work based on real policy process observation. As a non-empirical analysis, it is informed by official government communications, multilateral cyber norms, the UN reports, academia, and expert interpretations of developing cyber diplomacy doctrine. The approach is mainly interpretivist, with themes and issues in Pakistan's cyber policy environment derived from an analysis of literature and policy documents. Observational insights into regional and global cybersecurity cooperation also help in estimating the standing and preparedness of Pakistan in the cyber context. This interpretive qualitative frame also allows the paper to apply the prevailing theories of cyber diplomacy into a national level perspective of Pakistan and at the same time, project the necessary policy measures and strategic posture.

The Rise of Cyber Security Threats and Information Warfare: A Deeper Dive

The modern mode of warfare and battlefields among the states vs states, states vs non-state actors and states vs individuals have commenced with the arrival of digital age. These encounters and warfare are taking places inside the virtual cyber connected networks rather than on actual physical battlefields. In the era of cyber-connected international societies where information and communication technologies are rapidly increasing and states, non-state actors and individuals are relied upon them have increased the emergence of cyber security risks along with information warfare is a serious concern across the globe.[8] Number of cybersecurity threats and danger of cyber warfare have increased intensely which result in posing serious risks to overall social order, economic stability and national security of states along the security of individuals connected to cyberspace and digital technology.

Cyber Espionage and Information Theft

State-Sponsored Actors: Using advanced hacking tactics to steal intellectual property, military secrets, and confidential information, nation-states have been more involved in cyber espionage. A growth in cyber espionage, with an emphasis on obtaining military secrets,

[8] Aadil Ahmad Shairgojri and S. Dar, "Emerging Cyber Security: India's Concern and Threats," *Journal of Artificial Intelligence, Machine Learning and Neural Network* (2022), https://doi.org/10.55529/jaimlnn.25.1.10.

intellectual property, and confidential information, has been caused by the development of state-sponsored cybercriminal operations, especially by nations like North Korea, Russia, China, Iran, the US, Israel, and India.[9] Because it carries less danger than traditional espionage, nation-states find this sort of espionage appealing.[10] The stolen data can be used to gain a competitive advantage in negotiations, develop advanced weaponry, or disrupt critical infrastructure of rival nations.

Non-State Threats: Beyond state actors, non-state groups like terrorist organizations and criminal syndicates also engage in cyber espionage.[11] Their motives can range from acquiring funds through financial fraud to obtaining sensitive information for future attacks. In Pakistan's context, such threats become more pressing due to limited cyber deterrence, insufficient attribution capabilities, and an underdeveloped legal mechanism to respond to hostile digital intrusions.[12]

Critical Infrastructure Under Siege

Widespread Disruption: Our increasing reliance on interconnected systems, from power grids to transportation networks, makes them prime targets for cyber-attacks. These attacks, which range from data exfiltration to sophisticated worms, can have significant impacts on critical infrastructures, including energy distribution and transportation.[13] A successful attack could cripple essential services, cause widespread blackouts, and disrupt crucial supply chains. This can have devastating consequences, leading to economic losses, public panic, and even loss of life. Pakistan’s power network, NADRA’s identity systems and the Federal Board of Revenue (FBR) have all been hit with cyber intrusions.[14]

[9] Joab Kose, “Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage” (2021).

[10] Dominik Herrmann, “Cyber Espionage and Cyber Defence,” in *Information Technology for Peace and Security*, ed. Christian Reuter (Wiesbaden: Springer Vieweg, 2019), https://doi.org/10.1007/978-3-658-25652-4_5.

[11]J. Sigholm, “Non-State Actors in Cyberspace Operations,” *Journal of Military Studies* (2013), https://doi.org/10.1515/jms-2016-0184.

[12] Anam Shah, “Cybersecurity in Pakistan: Gaps and the Way Forward,” *ISSI Journal* 39, no. 2 (2021): 133–145.

[13] Annalisa Appice, Dominik Ślęzak, Henryk Rybinski, Andrzej Skowron, and Witold Pedrycz, “Foundations of Intelligent Systems,” in *Lecture Notes in Computer Science*, vol. 10352 (Cham: Springer, 2017), https://doi.org/10.1007/978-3-319-60438-1.

[14] National Database and Registration Authority (NADRA), “Digital Governance Projects,” accessed March 16, 2025, https://www.nadra.gov.pk/services/.

Motivations for Attacks: The motivations for attacking critical infrastructure vary. Nation-states might aim to cripple an enemy's warfighting capabilities or destabilize their economy.[15] Criminal groups might seek financial gain by holding infrastructure hostage for ransom. Factors influencing individual willingness to engage in politically motivated cyber-attacks on critical infrastructure include political outlook, group equality, and involvement in cyber deviance.[16] In some cases, the attacks might be purely destructive, aimed at causing chaos and sowing discord. For instance, in 2021 FBR's data center came under an attack, a testament to the absence of a layered security and strategic cyber deterrence. Cyber diplomacy can help reduce those risks by building partnerships across borders, developing common protocols for cross-border behavior, and promoting international norms for cyberspace that reduce attacks on critical infrastructure.[17]

Weaponizing Information Warfare

Social Media Battlegrounds: Social media platforms have become a potent tool for information warfare. These platforms, including Telegram, Facebook, and YouTube, are used for citizen monitoring, data collection, and the spread of disinformation and fake news.[18] Malicious actors use these platforms to spread disinformation, manipulate public opinion, and sow discord within societies. This can be used to undermine democratic processes, influence elections, and erode public trust in institutions.

Creating False Narratives: Through fabricated news stories, deep fakes (manipulated videos), and targeted social media campaigns, these actors create false narratives and exploit existing political and social divisions. The potential for deep fakes to be used for politically nefarious ends is

[15] Martin Rudner, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge," *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (2013): 453–481, https://doi.org/10.1080/08850607.2013.780552.

[16] Max Kilger and Thomas J. Holt, "Examining Willingness to Attack Critical Infrastructure Online and Offline," *Crime & Delinquency* 60, no. 5 (2014): 748–769, https://doi.org/10.1177/0011128712452963.

[17] United Nations Group of Governmental Experts (UNGGE), *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (2015), https://undocs.org/A/70/174.

[18] Olha Herus, "The Role of Social Media in the Information Warfare in the Context of War," *Sociology – Social Work and Social Welfare: Regulation of Social Problems* 3, no. 1 (2023), https://doi.org/10.23939/sosrsw2023.031.

also a major concern.[19] This can lead to polarization, radicalization, and even violence. In Pakistan's complex socio-political landscape, such campaigns risk inciting violence and destabilizing governance. A well-stocked cyber diplomacy toolbox should encompass partnership with platform companies, cooperation within global disinformation reduction communities, and capacity building in the form of domestic counter-narratives.

The Need for a Comprehensive Response

The rise of these cyber threats necessitates a multi-pronged approach. This includes adopting cyber diplomacy, strengthening cybersecurity defenses, fostering international cooperation on cyber norms, and promoting media literacy to counter disinformation campaigns. It is within this context that cyber diplomacy emerges as a crucial tool for navigating the complexities of cyberspace and mitigating these evolving threats.

Understanding the Multifaceted Nature of Cyberspace

Physical Layer: The underlying infrastructure that supports the digital world, encompassing computers, servers, and communication networks. This layer is often referred to as the "critical infrastructure" of cyberspace, and its security is paramount for the functioning of the entire digital ecosystem. This infrastructure, which includes systems for energy distribution, banking, and air traffic control, is vulnerable to a range of threats, from theft of information to attacks on privacy.[20]

Logical Layer: The software and protocols that govern the flow and processing of information within cyberspace. This layer includes operating systems, network protocols, and applications that facilitate communication and data exchange. Vulnerabilities in this layer can be exploited by attackers to gain unauthorized access to systems or manipulate data. There is need for a global response to privacy protection

[19] Chandell Gosse and Jacquelyn Burkell, "Politics and Porn: How News Media Characterizes Problems Presented by Deepfakes," *Critical Studies in Media and Communication* 38, no. 3 (2021): 222–235, https://doi.org/10.1080/15295036.2020.1832697.

[20] Sherali Zeadally and Cristina Alcaraz, "Critical Infrastructure Protection: Requirements and Challenges for the 21st Century," *International Journal of Critical Infrastructure Protection* 8 (2015): 53–66, https://doi.org/10.1016/j.ijcip.2014.12.002.

in cyberspace, highlighting the role of regulatory, technical, and social factors.[21]

User Layer: The human element, consisting of individuals and communities who interact with information and systems within the digital space. Users can be both victims and perpetrators of cyber threats. Their behavior, including lack of awareness or poor cybersecurity practices, can create vulnerabilities that attackers can exploit. Thus, prevalence of human error in data breaches and the need for effective security awareness training is of utmost importance.[22]

Interpretation Layer: The subjective understanding and use of information by individuals and states within cyberspace. This layer highlights the importance of fostering a culture of cyber hygiene and critical thinking skills to combat the spread of disinformation and misinformation. Meanwhile, the internet in disseminating misinformation, media manipulation, and propaganda can influence individual and state behavior.[23] These layers are intricately intertwined, and any security breach or disruptive activity has the potential to cascade across them, causing widespread disruption. A comprehensive understanding of cyberspace's multifaceted nature is crucial for developing effective strategies for cyber diplomacy.

Cyber Diplomacy Blending into Traditional Functions

Approaches that have traditionally been state-centric have significantly changed with the introduction of cyber diplomacy into traditional diplomatic activities. Hans J. Morgenthau's principles of diplomacy, which emphasize national interests and strategic objectives, provide a foundational framework for understanding state behavior in the cyber domain.[24] However, the dynamic nature of cyberspace necessitates a

[21] Virgílio A. F. Almeida and Danilo Doneda, “Privacy Governance in Cyberspace,” *IEEE Internet Computing* 19, no. 3 (2015): 60–64, https://doi.org/10.1109/MIC.2015.66.

[22] Joshua Crumbaugh, “Common Mistakes in Delivering Cybersecurity Awareness,” in *Cybersecurity Education for Awareness and Compliance*, ed. Yukiko Koga (Hershey, PA: IGI Global, 2019), https://doi.org/10.4018/978-1-5225-7847-5.CH002.

[23] M. Tanaś, “Issues of Misinformation, Media Manipulation, Propaganda in Cyberspace,” *Journal of Security and Sustainability Issues* 13, no. 1 (2023): 407–421, https://doi.org/10.47459/jssi.2023.13.31.

[24] André Barrinha and Thomas Renard, “Cyber-Diplomacy: The Making of an International Society in the Digital Age,” *Global Affairs* 3, no. 4–5 (2017): 353–364, https://doi.org/10.1080/23340460.2017.1414924.

paradigm shift in diplomatic strategies to effectively address emerging challenges. Traditional diplomacy, rooted in state-to-state relations and geopolitical negotiations, is ill-equipped to confront the multifaceted nature of cyber security threats. Cyber diplomacy extends beyond traditional boundaries, encompassing a diverse array of actors, including non-state entities, transnational networks, and individual stakeholders.[25] In this context, a network-centric approach to diplomacy becomes imperative, emphasizing multilateral engagements, strategic communication channels, and public-private partnerships. Multilateral engagements serve as a cornerstone of cyber diplomacy, enabling states to collaborate on shared objectives, such as enhancing cyber resilience, combating cybercrime, and upholding norms of responsible behavior in cyberspace.[26] Platforms such as the United Nations, regional organizations, and bilateral agreements facilitate dialogue and cooperation among diverse stakeholders, fostering trust and confidence-building measures (CBMs). Strategic communication channels play a crucial role in shaping perceptions, countering disinformation, and promoting transparency in cyberspace.[27] Public-private partnerships, involving collaboration between government agencies, technology companies, academia, and civil society, can enhance information sharing, capacity-building, and crisis response mechanisms. Moreover, cyber diplomacy encompasses a wide range of activities, including cyber security negotiations, diplomatic engagements in international forums, and the development of cyber norms and regulations. Cyber diplomacy, a crucial tool in the competition between great powers, is increasingly important in the digital age.[28] States must adapt to the evolving cyber landscape by integrating cyber diplomacy considerations into their foreign policy objectives, strategic planning processes, and diplomatic engagements. By embracing a network-centric approach to diplomacy, states can effectively navigate the complexities of cyberspace, mitigate

[25] Carmen Elena Cîrnu, “Cyber Diplomacy, Strategic Instrument in Foreign Affairs Policy,” *Romanian Cyber Security Journal* 1, no. 1 (n.d.), https://rocys.ici.ro/spring-2019-no-1-vol-1/cyber-diplomacy-.

[26] Amel Attatfa, Karen Renaud, and Stefano De Paoli, “Cyber Diplomacy: A Systematic Literature Review,” *Procedia Computer Science* 177 (2020): 503–510, https://doi.org/10.1016/j.procs.2020.08.007.

[27] M. Mitrović and A. Vulić, “Project Management of Strategic Communication in Digital Era,” in *Proceedings of the 5th IPMA SENET Project Management Conference (SENET 2019)*, (2019): 79–84, https://doi.org/10.2991/senet-19.2019.13.

[28] E. Zinovieva, “Cyber Diplomacy under Increased Competition Between the Great Powers,” *MGIMO Review of International Relations* Special Issue (2022), https://doi.org/10.24833/2071-8160-2022-olf5.

cyber security threats, and promote international cooperation. The integration of cyber diplomacy into traditional functions heralds a new era of diplomacy, characterized by agility, resilience, and adaptability in the face of emerging challenges.

Traditional Diplomacy vs. Cyber Diplomacy: A Tale of Two Worlds

The rise of cyberspace has fundamentally altered the landscape of international relations. Traditional diplomacy, built on a foundation of face-to-face meetings, formal treaties, and established channels of communication between state actors, struggles to address the complexities and rapid pace of cyber threats.[29] This necessitates the emergence of a new paradigm – cyber diplomacy.

The Limitations of Traditional Diplomacy

Slow and Bureaucratic: Traditional diplomacy thrives on established protocols and well-defined hierarchies. However, the fast-paced nature of cyber threats demands a more agile and flexible response. The lengthy negotiations and bureaucratic processes inherent in traditional diplomacy are ill-suited to address constantly evolving cyber risks. The failure of the UN GGE to produce a consensus report on cyber norms highlights the limitations of traditional diplomatic processes in addressing cyber risks.[30]

Limited Scope: Traditional diplomacy primarily focuses on interactions between state actors. But cyberspace is a borderless realm, and cyber threats can originate from non-state actors like criminal groups or lone hackers. Traditional diplomacy lacks the framework to effectively engage with these diverse players. This shift requires a rethinking of strategy and statecraft, with an emphasis on big-picture and longer-term priorities.[31]

[29] Evan H. Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century* (Montreal: McGill-Queen's University Press, 2002), accessed 2024, https://books.google.com.pk/books?id=OdfOi3LtoZQC.

[30] Stefania Pia Grottola, "Proliferation of Cyber Norms: The Limitations of Traditional Diplomacy in Discussing Cyberconflict" (paper presented at the GigaNet Annual Symposium, 2020), https://www.giga-net.org/2020symposiumPaper/Grottola.pdf?_t=1602675804.

[31] Jochen Prantl and Evelyn Goh, "Rethinking Strategy and Statecraft for the Twenty-First Century of Complexity: A Case for Strategic Diplomacy," *International Affairs* 98, no. 1 (2022): 317–336, https://doi.org/10.1093/ia/iiab212.

Focus on Physical Conflict: Traditional diplomacy excels at mitigating physical conflict between nations.[32] However, cyberwarfare operates in a new domain, with its own set of rules and motivations. Traditional diplomatic tools, honed for resolving territorial disputes or political disagreements, may not translate effectively to cyberspace.

The Rise of Cyber Diplomacy

Cyber diplomacy recognizes the limitations of the traditional approach and seeks to address the unique challenges of cyberspace.[33] It embraces a more multifaceted and network-centric approach, characterized by the following key features:

Multi-Stakeholder Engagement: Cyber diplomacy recognizes that cyberspace is not solely the domain of governments. It necessitates collaboration with a wider range of actors, including:

Private Companies: Critical infrastructure like power grids and communication networks are often owned and operated by private companies. Their involvement is crucial for developing robust cyber defenses and coordinating responses to attacks.

Civil Society Organizations: Civil society groups play a vital role in advocating for digital rights, promoting good internet governance practices, and ensuring public accountability in cyberspace.

Technical Experts: Cybersecurity is a complex field requiring specialized knowledge and technical expertise. In conducting cyber diplomacy, cyber diplomats collaborate with cyber domain specialist in order to analyse the cyberattacks, enhance technological capabilities and develop competent cyber threats mitigation plans and strategies.

International and Regional Organizations: The UN and other regional and international organizations can help in building common best practices, foster cooperation on cyber standards, and provide peaceful mechanisms for resolving disputes in cyberspace.

[32] Robert F. Trager, "The Diplomacy of War and Peace," *Annual Review of Political Science* 19 (2016): 205–225, https://doi.org/10.1146/ANNUREV-POLISCI-051214-100534.

[33] Saeed Seyed Agha Banihashemi, *Cyber Diplomacy* (Iran: School of International Relations, Ministry of Foreign Affairs; B P International, 2021), https://doi.org/10.9734/bpi/mono/978-93-91473-74-7.

Concentrate on Norms and Developing Confidence: While traditional diplomacy relies on accords and treaties, the purpose of cyber diplomacy is to establish norms on acceptable conduct in cyberspace. This could range from agreements on responsible disclosure of software vulnerabilities, noninvolvement with critical infrastructure, and joint effort on cybercrime probes. To help reduce tensions and create a more secure atmosphere in cyberspace, confidence-building measures such as information sharing and joint cyber events might be advantageous. This will lead to a more secure cyberspace by fostering openness, removing misconceptions and improving confidence between governments.[34]

Mechanisms for Quick Response: First of all, cyberattacks are quick, and they cannot be addressed through a long sluggish judicial process. Secondly, the increasing threat of cyberattacks and especially targeted cyberwar is increasing the demand for efficient detection and response instruments.[35] Properly established lines of communication and protocols for rapid information sharing, joint attack attribution, and cooperation in response to a major cyber incident are the objectives of cyber diplomacy.

Cyber diplomacy aims to put in place a multi-stakeholder approach that prioritizes international partnerships including its emphasis on norms and quick response protocols. Cyber diplomacy also offers a better path to navigating the complexities and ever-evolving risks of cyberspace.

Cyber diplomacy: Challenges and Opportunities for Pakistan

Like many other underdeveloped countries, Pakistan has its own set of challenges and opportunities while handling the complicated world of cyber domain. Below is a closer examination of both:

Challenges:

Absence of Adequate Cybersecurity Laws and Legal Framework: Pakistan currently lacks defined enforcement tools and a fragmented cyber security law framework. Therefore, for cyber diplomacy to be effective and sufficient, it needs the following steps:

[34] Jürgen Altmann, "Confidence and Security Building Measures for Cyber Forces," in *Information Technology for Peace and Security*, ed. Christian Reuter (Wiesbaden: Springer Vieweg, 2019), https://doi.org/10.1007/978-3-658-25652-4_9.

[35] Aditya K. Sood and Richard Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," *IEEE Security & Privacy* 11, no. 1 (2013): 54–61, https://doi.org/10.1109/MSP.2012.90.

Reformed Law: It is essential to pass legislation that are thorough in addressing cybercrime, data security, and critical infrastructure protection. To remain current with the ever-evolving cyber threats, these laws have to be periodically reviewed and modified.

Effective Implementation: To properly investigate and prosecute cybercrime, law enforcement authorities must establish a specialised cybercrime unit that operates around-the-clock and has the required resources and skills.

Lack of Cyber Capacity: There is a scarcity of qualified cybersecurity experts in Pakistan. Cyber diplomacy can assist in addressing this issue:

Allocating Resources to Cyber Education: In order to combat cyber risks, universities and technical institutes may generate a trained workforce by working with international states and private partners to establish cyber diplomacy and security training programs.

Partnerships Between the Public and Private Sectors: In order to improve the cyber diplomacy and security proficiency of Pakistani workers, collaboration with private IT businesses can be used to set up training courses and knowledge-sharing projects.

Inadequate Strategic Communication: Pakistan faces inadequate strategic communication in the cyber realm. A clear and consistent narrative about Pakistan's position on cyber issues is essential for effective cyber diplomacy. In that manner, Pakistan needs to act on the following imperatives:

Formulate a Strategy for National Cybersecurity: Pakistan’s objectives in the cyberspace should be outlined in this strategy, along with its dedication to international collaboration, internet governance, peaceful use of cyberspace and cybersecurity.

Campaigns for Public Awareness: Pakistan’s overall cyber security posture can be greatly enhanced by educating its people about cyber diplomacy, public domain, and cyber hygiene measures, such as formulating effective and positive content for online engagement in cyber domain, creating strong passwords and identifying phishing attempts.

Retaining Neutrality: Major nations are rapidly turning the digital sphere into a battlefield. Therefore, Pakistan is required to:

Refuse to Align with the Predominant Powers: Supporting a multi-stakeholder approach to global cyberspace governance can be hampered if Pakistan aligns itself with a particular large power on cyber matters.

The Multipolar Worldview: Pakistan has the potential to utilise its status as a developing country to advocate for a more comprehensive approach to cyber governance, guaranteeing that the perspectives of all countries are acknowledged and taken into consideration.

Opportunities:

Encouraging Openness and Responsible Leadership: Pakistan can effectively demonstrate its efforts towards openness and good governance by utilising cyber diplomacy. Through the use of e-government projects and other likely initiatives, Pakistan can:

Raise Involvement of Citizens: Citizens may be empowered and their faith in government institutions increased via the use of online citizen feedback tools and open data platforms.

Enhance The Provision of Services: Citizens across can benefit from increased accessibility, decreased corruption, and streamlined procedures when government services are provided through online portals. As an illustration of how e-government might enhance service delivery, consider Pakistan's attempt to offer online birth and death certificates through NADRA.

Promotion of Economic Growth: Rely on a dependable and safe digital infrastructure; Pakistan could more fully engage in the global digital economy. Following are some approaches that Cyber Diplomacy can help:

Getting Foreign Investment: By displaying a dedication to cyber diplomacy, cyber security and enacting cyber regulatory frameworks for data protection, Pakistan might potentially acquire foreign investment in sections of the digital economy such as fin-tech, cybersecurity, as well as e-commerce.

Encouragement of Innovation: Collaboration with foreign partners on cyber diplomacy and security research and development, as well as the practice of cyber diplomacy, could stimulate homegrown technological innovation, create new employment opportunities, and offer the potential for economic expansion.

Enhancing International Collaboration: Being susceptible to cyber threats, Pakistan can apply cyber diplomacy in order to:

Establish Partnerships: Through active involvement in regional and global organizations such as the Asia-Pacific Economic Cooperation (APEC) and the Shanghai Cooperation Organization (SCO), Pakistan can collaborate with other states to conduct joint cyber exercises, trade threat intelligence, and share best practices.

Encouraging Responsible State Behavior: Pakistan can furthermore advocate for the creation and implementation of world norms in cyberspace, such as agreements prohibiting interference in critical infrastructure and responsible vulnerability disclosure. By doing so and embracing the opportunities provided by cyber diplomacy to address various policy challenges, Pakistan can position itself as a responsible stakeholder in cyberspace that promotes good governance of the sector, fosters economic development, and enables a more secure and stable online environment.

Policy Recommendations for Strengthening Pakistan's Cyber Diplomacy

The recommendations presented below form a blueprint that can be used by Pakistan to enhance their cybersecurity defence infrastructure and employ cyber diplomacy to support their economic and national security objectives. The following is an explanation of each policy suggestion:

Create a Formal Division for Cyber Diplomacy inside Pakistan's Ministry of Foreign Affairs:

Cyber Diplomacy Division: MoFA should create a new division for cyber diplomacy, which would be headed by the Ministry of Foreign Affairs and include all other governmental agencies, intelligence agencies, and military experts.

Cyber Diplomats: Pakistan needs to start recruiting cyber diplomats for performing effective cyber diplomacy like rest of the international states and agencies are doing to adequately protect their country’s interests, build cooperative and coordinative relations across the globe and promote responsible state behaviour in the cyber realm.

Cyber Diplomacy Framework: Pakistan needs to have in place a well formulated framework for cyber diplomacy in order to efficiently address the complication of cyberspace. This framework can guide on how to address issues that emanate from the cyber domain and can also set perimeters on how Pakistan relates with foreign nations. The option of a legal cyber diplomacy framework benefits Pakistan in that it can enhance international cooperation and even establish guidelines for responsible actions in the digital realm.

Create and Execute All-encompassing Cybersecurity Laws, Policies and Plans

Modified Legal Framework: Cyber regulations in Pakistan have been weakly connected. It is vital to reintroduce all-encompassing changes that include:

Legislation Against Cybercrime: To keep cybersecurity professionals responsible and cybercriminals away from hacking, data breaches, cyber espionage and online abuse, laws are essential.

Laws Regarding Data Protection: Establishing confidence with citizens who undertake online transactions depends on the implementation of strong data protection rules that govern the gathering, storing, and use of personal information.

The Security of Critical Infrastructure: To protect vital infrastructure from cyberattacks, such as power grids and banking systems, specific legislation defining security standards are required.

Reliable Enforcement Techniques: Within law enforcement organisations, Pakistan must create specialised cybercrime units with the tools and knowledge necessary to successfully investigate and prosecute cybercrimes. Investigative capacities can be further improved by cooperation with foreign law enforcement authorities.

Invest in the Advancement of Cybersecurity Expertise and Technologies through Research and Development

Filling the Skill Gap: Professionals with expertise in cyber diplomacy and security are in great demand in Pakistan. Putting money into R&D can close this gap in the following ways:

Providing Funds for Academic Programs: Encouraging academic institutions to establish focused cybersecurity programs can provide a pool of highly qualified graduates ready to join the profession.

Encouraging Collaboration Between Public and Private Sectors: By establishing training programs and knowledge-sharing efforts, partnerships with think tanks and technology businesses can prepare the staff with the most recent cyber diplomatic methods and defence measures.

Development of Technology and Indigenous Policy: One way to lessen Pakistan's dependency on foreign technology and increase overall cyber resilience is to invest in research and development (R&D) for the purpose of creating domestic cyber diplomacy policies and cyber security solutions that are relevant to Pakistan's requirements and challenges.

Encourage Public Education and Awareness of Online Safety, Threats, and Cyber Diplomacy

Giving Citizens More Power: The first line of defence and diplomacy in cyberspace is an informed populace. Pakistan has the following options to spread awareness:

Initiatives for Public Awareness: Across-the-country initiatives that make use of social and conventional media channels to instruct people on cyber hygiene and diplomatic techniques like as making secure passwords, avoiding dubious links, and identifying phishing efforts.

Curriculums for Academics: The Higher Education Commission of Pakistan and other pertinent institutions can incorporate cyber diplomacy and safety instruction into academic curricula to provide the next generation of learners with the information, interest, and abilities to safely traverse the internet environment.

Community Engagement Initiatives: Community engagements depending on which population segment is addressed may include government workers, think tanks, businesses and enterprises, and research institutes; provide targeted training on the best practices of cyber security and cyber diplomacy that are relevant to the community served.

Engage in Partnerships and Strategic Conversations on Cyber Issues with Other Nations

Developing Partnerships: Building partnerships on cyber issues demands actively engaging with the UN, the APEC or the SCO plus other regional and international organisations; and developing collaborative cyber exercises to evaluate general cyber defenses. Pakistan needs to actively contribute to the negotiating and developing of international norms in cyberspace especially in the framework of the UN GGE and

Open-ended Working Group (OEWG) processes.[36] Cyber diplomacy will need to move beyond the defence field to include norm promotion, transparency mechanisms and confidence building measures.[37]

Collaborative Cyber Exercises: Pakistan, through participating in international cyber drills, may evaluate its cyber defence side by side with other nations and further develop reaction tactics by sharing best practices.

Exchange of Threat Intelligence: Pakistan could be kept informed of the most recent cyber threats and vulnerabilities and get the chance to act proactively to mitigate risks with such forms of cooperation as cyber threat intelligence.

Initiatives to Build Capacity: Cyber diplomats and cybersecurity experts from Pakistan might obtain cutting-edge teaching and knowledge by teaming with industrialized nations on joint capacity-building initiatives.

Align Cyber Diplomacy and Cybersecurity Aspects with Foreign and Domestic Policy Goals

Pakistan must prioritise national security and interest by advancing cyber diplomacy and cyber defense. It includes:

National Cyber Diplomacy and Security Strategy: Creating a thorough national plan for cyber diplomacy and security that describes Pakistan's policy for dealing with the internet, including its adherence to international standards, cyber security, cyber collaboration, and the goal of a safe and secure online environment.

Engaging in Diplomatic Relations: Pakistan should incorporate cybersecurity concerns into its cyber diplomatic exchanges with other nations. Pakistan may push for multi-stakeholder global cyberspace governance, encourage international cooperation against cybercrime, and advocate for responsible state behaviour in cyberspace.

[36] United Nations, “Group of Governmental Experts (GGE) Reports,” United Nations Office for Disarmament Affairs, accessed January 02, 2025, https://unoda.org/.
[37] Joseph S. Nye Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security* 41, no. 3 (2017): 44–71.

Conclusion: Pakistan's Path Forward in a Digital Age

Cyber diplomacy represents the vanguard of 21st-century diplomacy – blending the exigencies of national security, the governance challenges of the digital sphere and the eternal necessities of the multilateral ideal. Cyber diplomacy is increasingly becoming a necessity rather than a luxury for states such as Pakistan, moving from being a sideline observer to an active participant. As cyberspace is emerging as a turf for power projection, norm creation and influence, Pakistan would have to recalibrate its strategic priorities in its foreign policy that are designed to adapt to the realities of the new cyber frontier.

This study brings out the incomplete but considerable journey of Pakistan in institutionalizing the cyber diplomacy through domestic policy measures and institutional redesigns. Nonetheless, major challenges persists such as the lack of a specific cyber diplomacy division and cyber foreign policy, lack of coordination between cyber-security and foreign policy related structures, under-investment in building digital capacity, and limited representation in setting normative standards for the world. These flaws run the risk of excluding Pakistan from important international dialogues on digital realm, cyber conflict prevention and technological sovereignty. To take opportunities of the strategic windows available through cyber diplomacy, Pakistan needs to rethink and adopt the proactive attitude.

This would involve mainstreaming cyber considerations into its national security strategy, improving inter-agency coordination, fostering digital literacy among its diplomatic cadre, and partnering with other cyberpositivist states to shape global cyber norms. Pakistan should focus on engagement with regional mechanisms and contribute positively to UN-led processes to improve its normative footprint. Thus, integrating the field of cyber diplomacy enables Pakistan not only to protect its digital terrain but to assert its sovereignty, to project its values and to engage in the meaningful governance of the cyber domain. By successfully addressing the challenges and exploiting the opportunities, Pakistan can evolve from a digitally insecure country to a responsible and capable player in the global digital architecture.