SPOTLIGHT
ON REGIONAL AFFAIRS

INSTITUTE OF REGIONAL STUDIES ISLAMABAD

September 2023, Vol.41, No.9 (1)

Cyber CBMs Between India and Pakistan: A Step Towards Cooperation

Usman Akhtar[*]

Introduction

In an increasingly interconnected world, the impact of cyber-attacks on states has transcended mere digital disruptions to become a critical threat to national security and global stability. The rise of cyber-attacks and the potential for state-sponsored or non-state actors to exploit vulnerabilities in cyberspace have created an urgent need for effective strategies to counter such threats. In this context, the concept of cyber confidence-building measures (CBMs) has gained prominence as a vital tool in international relations. These CBMs offer a potential pathway to address the looming dangers of cyber warfare while fostering an environment of cooperation and stability.

The urgency of addressing cyber threats is underscored by the experiences of nations like India and Pakistan. Both countries have faced a barrage of cyber-attacks from unidentified sources, often involving non-state actors. This challenge is not bound by geographical borders and falls under the realm of non-traditional security threats. Unlike conventional conflicts where adversaries are discernible, the intangible nature of cyber-attacks makes their attribution complex and often elusive. The escalating uncertainty in cyberspace perpetuates misunder-standings and mistrust between neighbouring nuclear-armed states, aggravating existing diplomatic complexities.

The challenge of definitively attributing cyber-attacks can escalate tensions and foster a hostile environment, underscoring the imperative of establishing CBMs. These measures are designed not only to mitigate the immediate risks posed by cyber-attacks but also to promote trust, cooperation, and stability in cyberspace. However, the implementation of such CBMs presents challenges that demand careful consideration. This study delves into the ramifications of cyber-attacks on India and Pakistan, explores the role of non-state actors, and highlights the significance of Cyber CBMs. Moreover, it examines the challenges involved in realizing these measures and proposes a constructive way forward to foster meaningful collaboration.

Role of Non-State Actors

Non-state actors, ranging from hacktivist groups to criminal organizations and ideologically motivated entities have played a prominent role in the cyber domain. Both India and Pakistan have fallen victim to cyber-attacks orchestrated by these non-state entities, who have leveraged the expansive capabilities of the internet to expand their agendas[1]. The Anonymous group, known for launching numerous cyber-attacks on governments, corporations, and organizations worldwide, often in pursuit of political or social justice goals, has also targeted Indian government websites on several occasions. In 2011, the Anonymous group lent its support to a civil movement against corruption in India by hacking a government IT organization's website[2]. These actions by such groups pose a significant threat to the stability and functionality of a country's institutions, as they unilaterally determine their own notions of right and wrong and act accordingly. In such situations, the issue of attribution becomes inherently complex. Likewise, in 2022, an India-based computer hacking group WhiteInt assumed control over computers owned by Pakistani politicians, generals, and diplomats[3]. Such cyberattacks underscore that these groups operate independently of any state control, yet they pose a threat to the stability of Pakistan due to their association with India.

Impact of Cyber Attacks on India and Pakistan

The escalating threat posed by cyber-attacks is of profound concern, encompassing economic ramifications, national security implications, and the potential for damage to critical infrastructure. An illustrative attack occurred in 2016 when the Indian banking sector fell victim to a cyber-attack attributed to North Korean hackers[4]. This malevolent intrusion disrupted online banking services, resulting in substantial financial losses approximating $170 million. Similarly, Pakistan encountered its own challenge in 2018 when a private bank Bank Islami suffered a cyber assault.[5] This breach compromised customer data, leading to a monetary setback exceedingly approximately $6.5 million. In accordance with a research investigation

[*] Mr Usman Akhtar is an Intern with the Cybersecurity Programme at the Institute of Regional Studies, Islamabad.

undertaken by Comparitech, Pakistan ranked the 7th position among nations exhibiting suboptimal cybersecurity measures[6].

Beyond its economic repercussions, cyber-attacks assume an even graver dimension by threatening national security. In 2019, a malware attack targeted one of India's largest nuclear reactors, Kudankulam, which not only infiltrated the plant's firewalls but also allegedly stole data and information[7]. In such a way, India and Pakistan, both possessing nuclear arsenals, stand particularly vulnerable to cyber threats with potentially far-reaching military implications. An attack targeting critical infrastructure, such as power grids or communication networks, could precipitate catastrophic consequences. Furthermore, a cyberattack was perpetrated against the Election Commission of Pakistan (ECP), prompting the issuance of a security alert by its authorities.[8]

Challenges in Attributing Responsibility

The process of attribution, which involves identifying the actual perpetrators of a cyber-attack, presents a formidable challenge, especially when dealing with non-state actors. This complexity involves various issues. Firstly, non-state actors exhibit a high level of expertise in anonymity and stealth.[9] They employ techniques such as routing attacks through multiple proxies, utilizing Tor networks—encrypted networks to protect privacy and ensure anonymity on the web—and deploying sophisticated malware to obfuscate their digital footprints, making it nearly impossible to accurately trace their origins.

Secondly, challenges emerge due to jurisdictional issues, as many of these entities operate from regions or countries that are either unwilling or unable to cooperate in international investigations. This situation creates safe havens for cybercriminals. Thirdly, non-state actors often employ deceptive tactics, including false flags, to confuse investigators. They leave fabricated clues and attributes to divert attention away from their identity.

Furthermore, the collaborative nature of these actors in the dark web and underground forums adds another layer of complexity to attribution. They pool resources, tools, and tactics, making it difficult to pinpoint a specific individual or group as the primary responsible party within the intricate supply chains that often underlie cyber-attacks.

The Need for Cyber CBMs

India and Pakistan have fought four full-scale wars since their independence. In the contemporary era, both countries face a common threat of cyber-attacks. These attacks pose the risk of infliction equal harm on both countries. Consequently, the need for cyber CBMs has emerged. These measures represent the framework that will guide future diplomatic discussions. Cyber CBMs encompass structured agreements or protocols crafted to facilitate communication, understanding, and cooperation among both state against the threat posed by non-state actors operating within cyberspace. Their primary purpose revolves around bolstering security, mitigating conflicts, and diminishing the inherent risks associated with cyber activities. A central objective of cyber CBMs is the effective mitigation of risks associated with cyber-attacks. These CBMs can be established by forming channels for open dialogue and the sharing of critical information among both countries. Such initiatives serve as a potent deterrent against hostile cyber activities, when there is the fog of war. Another dimension of cyber stability revolves around promoting cyber deterrence.[10] By determining consequences for hostile cyber activities within CBMs, both countries can effectively communicate their readiness to respond to cyberattacks. This serves as a resounding message to potential adversaries and non-state actors, acting as a potent deterrent against cyber-attack.

Many technologically advanced countries are actively developing their cyber offensive capabilities under the guise of defensive measures[11]. Considering this, it is imperative for India and Pakistan to take the lead in establishing cyber CBMs that can serve as a global benchmark. These Cyber CBMs hold the potential to serve as a gateway to future diplomatic relations, particularly considering the prolonged absence of any substantive dialogues between both countries. By initiating cyber CBMs, India and Pakistan can create a platform for constructive engagement, not only addressing cyber security concerns but also facilitating discussions on a broader range of issues such as economic and trade policies, thereby fostering a more comprehensive and collaborative relationship. The ripple effect of such diplomatic progress would undoubtedly have a positive impact on other countries within the South Asian region. It is through these proactive efforts that India and Pakistan can promote stability, cooperation, and mutual understanding, ultimately contributing to the greater harmony and prosperity of the region.

Challenges in Implementing Cyber CBMs

The pursuit of effective cyber CBMs within the India-Pakistan is confronted with a series of formidable obstacles. Foremost among these challenges is the longstanding history of distrust and conflict that has deeply entrenched itself between two countries. This historical backdrop of hostility has the potential to obstruct sincere collaborative efforts and diminish the willingness to exchange crucial cyber-related information.

Another substantial challenge lies in the absence of standardized frameworks governing cyber activities, cyber threats, and cyber warfare. The absence of agreed-upon frameworks hinders the capacity to articulate intentions clearly and respond to incidents in a foreseeable and de-escalatory manner. Furthermore, a notable imbalance in cyber capabilities and technological advancements exists between India and Pakistan. India, with its technological superiority, may approach CBMs with caution, fearing that engagement might be exploited by Pakistan to close the gap and catch up in terms of cyber capabilities. An additional challenge in establishing a foundation for bilateral discussions between India and Pakistan lies in India's steadfast position against third-party mediation. On numerous occasions, India has openly stated its firm refusal to permit any external intervention[12]. India's stance on talks with Pakistan is unequivocal. It has been clarified by the Indian authorities that there is no room for third-party involvement, and the resolution of issues between neighbouring countries is exclusively the responsibility of their respective governments. Lastly, non-state actors, such as hacktivist groups or terrorist organizations, can exploit the absence of well-defined CBMs to carry out disruptive or destructive cyber activities. Such actions could inadvertently trigger a crisis and exacerbate tensions between India and Pakistan.

Conclusion

The escalating cyber threats confronting India and Pakistan from non-state actors pose a multifaceted challenge outstripping the geographical boundaries. The realm of cyber warfare is marked by the challenge of attributing attacks and the potential for severe consequences, underscoring the call for action. Thus, the necessity for cyber CBMs is evident, with their primary aim to mitigate cyber risks and promote stability. Furthermore, these CBMs can contribute to the deterrence of cyber threats. However, implementing effective CBMs faces various challenges. To move forward constructively, India and Pakistan should work on building frameworks against third party attacks. Through the adoption recommendations and collaborative efforts to confront cyber threats, India and Pakistan can not only fortify their security but also foster regional stability and cooperation within the broader South Asian context. In the ever-evolving sphere of cyberspace, proactive collaboration stands as an imperative for safeguarding the national interests and nurturing a more harmonious future for the region.

A Constructive Way Forward

Cyber Space is predominantly dominated not by the states, but by the activities of non-state actors and organizations. The activities of states can help build trust while those of non-state actors can erode it. Thus, the role of CBMs to build trust and cooperation particularly in realm of cyberspace is paramount to consider. According to a report published by Atlantic Council, there are four types of CBMs that can be established to mitigate potentially escalatory effects of activities in cyberspace[13]. These are collaboration, crisis management, restraint, and engagement measures. These CBMs are some-how difficult to implement in context of India and Pakistan. Here are some of the recommendations for constructive way forward between India and Pakistan:

Track II Diplomacy

The promotion of Track II diplomacy initiatives and people-to-people exchanges is crucial in building trust and creating a favourable atmosphere for cyber CBMs. It is important for Pakistan to initiate talks. This approach will contribute significantly to the establishment of a robust framework for cyber diplomacy and security.

Establish Clear Cyber Norms and Rules

It is crucial for both countries to form legal frameworks to counter future cyber-attacks from third party. To establish a coherent framework for cyber governance, initiate bilateral discussions to create clear rules of engagement in cyberspace, including defining what constitutes cyberattacks and the proportionate response to them. In addition, encourage dialogue on cyber ethics, responsible state behaviour, and the protection of critical infrastructure.

Mutual Cyber Threat Assessments

Facilitating mutual cyber threat assessments is of paramount importance. It is advisable for both countries to promote the exchange of non-sensitive cyber threat intelligence between, thereby augmenting situational awareness and fortifying collaborative defences against cyber threats.

Capacity Building and Technical Assistance

Efforts should be directed towards the facilitation of capacity-building programs that assist

Pakistan in bolstering its cyber capabilities, thereby addressing India's concerns and reducing the technological disparity. Additionally, it is crucial to promote collaborative initiatives in cybersecurity research, training, and education, with the aim of nurturing a proficient cyber workforce in both countries.

Regional Cooperation

It is advisable to actively encourage the participation of both nations in regional cybersecurity forums and initiatives, as these platforms can effectively serve as a foundation for constructive dialogue and collaborative efforts with neighbouring countries. Furthermore, leveraging regional organizations such as the South Asian Association for Regional Cooperation (SAARC) can provide a structured framework for collective discussions and measures.

Third-Party Involvement

It is crucial to acknowledge and respect India's position against third-party mediation, emphasizing the importance of direct bilateral discussions. Simultaneously, it is prudent to leverage diplomatic backchannels, international organizations, and regional forums as discreet channels for dialogue and confidence-building initiatives.

Notes and References

[1] T.X Hammas, "Technology Converges; Non-State Actors Benefit," *Hoover Institute, 25 February 2019. https://www.hoover.org/research/technology-converges-non-state-actors-benefit.*

[2] John Ribeiro, "Anonymous hacks Indian site in fight against corruption," *Info World*, 7 June 2011. https://www.infoworld.com/article/2621489/anonymous-hacks-indian-site-in-fight-against-corruption.html

[3] "Hackers targeted Pakistani 'generals, politicians," *The Express Tribune, 6 November 2022. https://tribune.com.pk/story/2385004/hackers-targeted-pakistani-generals-politicians*

[4] Julie Steinberg and Gabriele Parussini, "Was North Korea Behind the Hacking of a Bank in India?", *The Wall Street Journal, 10 April 2017. https://www.wsj.com/articles/cybertheft-attempt-on-indian-bank-resembles-bangladesh-heist-1491816614*

[5] Eleazar Bhatti, "BankIslami becomes victim of $6.5 million cyber-attack," *Profit,* 29 October 2018. https://profit.pakistantoday.com.pk/2018/10/29/bankislami-becomes-victim-of-6-5-million-cyber-attack/

[6] PAUL BISCHOFF, "Which countries have the worst (and best) cybersecurity?" Comparitech, 26 September 2022. https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

[7] Ayaz Hussain Abbasi, "Cyber Threats in a Nuclear World," *Tribune Magazine*, 27 March 2022.
https://tribune.com.pk/story/2349802/cyber-threats-in-a-nuclear-world

[8] News desk, "ECP's website faces cyber attack, security alert issued," *Pakistan Observer,* 8 July 2023. https://pakobserver.net/ecps-website-faces-cyber-attack-security-alert-issued/

[9] Ayshwariya Raman, "States' use of non-state actors in cyberspace," *Observer Research Foundation*, 17 August 2023. https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace/

[10] Joseph S. Nye, Jr,"Deterrence and Dissuasion in Cyberspace," *MIT Press Direct,* 1 January 2017. https://direct.mit.edu/isec/article/41/3/44/12147/Deterrence-and-Dissuasion-in-Cyberspace

[11] Pool, Phillip. "War of the Cyber World: The Law of Cyber Warfare." *The International Lawyer* 47, no. 2 (2013): 299–323. http://www.jstor.org/stable/43923953.

[12] Manish Tewari, "Of India-Pakistan ties and third-party mediation," *Hindustan Times,* 5 May 2011. https://www.hindustantimes.com/opinion/of-india-pakistan-ties-and-third-party-mediation-101620236858359.html.

[13] Jason Healey, John C. Mallery, Klara Tothova Jordan, Nathaniel V. Youd," CONFIDENCE-BUILDING MEASURES IN CYBERSPACE," *Atlantic Council, BRENT SCOWCROFT CENTER ON INTERNATIONAL SECURITY,* November 2014. https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf.