SPOTLIGHT
ON REGIONAL AFFAIRS

August 2023, Vol.41, No.8 (1)

Enhancing Cyber Resilience: Challenges and Opportunities in South Asia

Warda Ghafoor*

Introduction

In contemporary times, cyberspace has transformed into a theatre of geopolitical competition. Concurrently, as states embrace digital transformation, the use of cyber technologies like cloud computing and Artificial Intelligence (AI) in cyberattacks has profoundly impacted national security and societal cohesion. Furthermore, in the aftermath of the Russia-Ukraine war, hacker groups like Anonymous and Squad303 have assertively displayed their solidarity with one side of the conflict. The skyrocketing cyber warfare underscores the significance of cyber resilience in confronting digital threats. Therefore, to address the security challenges posed by big data, various states have intensified their regional cyber security initiatives, recognising that regional cooperation in advancing cyber readiness yields a more significant influence than individual national efforts.

However, South Asia continues to be a volatile region, where the adoption of cyber technology and awareness about cyber security are both limited. As a result, the cyber security resilience framework remains fragmented, resulting in many national and regional constraints that impede the region's efforts to improve its cyber resilience. This study aims to shed light on these challenges, with a primary focus on India and Pakistan as major nuclear powers in South Asia. It also highlights the ASEAN efforts in implementing viable alternative frameworks within the cyber realm. Additionally, it investigates the prospects for collaborative efforts within the cyber domain across South Asia. Consequently, it provides a road map for South Asian countries to effectively secure their digital assets while also strengthening their overall cyber defences.

Cyber Threat Landscape in South Asia

South Asia has limited cyber resilience due to countries' uneven levels of development in their cyber response mechanisms. The International Telecommunication Union's Global Cybersecurity Index (GCI) 2020 rankings reflect this diversity. According to the 2020 GCI report, India is at the 10th position, with Bangladesh at 53rd, Pakistan at 79th, Sri Lanka at 83rd, Nepal at 94th, Bhutan at 134th, and Afghanistan at 171st position.[1]

Correspondingly, the region is a prominent target for cyberattacks, encompassing ransomware attacks, phishing, and data breaches, among others. One of the most overarching reasons is the lack of policy readiness and institutional regulations in South Asian states when it comes to cyber security concerns. In 2021, for example, Pakistan's Prime Minister Imran Khan fell victim to surveillance hacking by Israeli Pegasus spyware.[2] Similarly, in 2021, this software was used to hack into the smart devices of several journalists and political opponents in India and Bangladesh.[3]

Moreover, South Asian states, with distinct levels of cyber preparedness, actively participate in cyber warfare as both victims and offenders. Even with advanced cyber sophistication, India experienced a cyber-attack in 2019 that targeted its nuclear power plant in Kudankulam, breaching its firewalls and stealing data.[4] The Kudankulam attack highlighted the vulnerabilities of South Asian countries to cyber-attacks from other state and non-state actors, which have the potential to escalate tensions between historic rivals.

Following the 2019 Pulwama attack, cyber tensions between India and Pakistan reached a new high, leading to a surge in malware and phishing

* Warda Ghafoor is a Research Intern at the Cyber Security Program, Institute of Regional Studies (IRS), Islamabad.

attempts.[5] Increased cyber espionage attempts have heightened concerns for South Asia's cyber security framework, given that the region's information infrastructure is still in its early stages. Consequently, the evolving cyber threat landscape in South Asia necessitates urgent efforts to construct a more secure environment. Amidst the backdrop of cyber warfare, ASEAN has successfully implemented cyber security measures, offering valuable lessons that South Asia can learn from.

ASEAN Regional Cybersecurity Success Stories:

The Association of Southeast Asian Nations (ASEAN) has been making significant strides in increasing regional cooperation in the cyber domain. A notable step in this direction was taken on July 18, 2023, when the member states of ASEAN officially established the headquarters of a cyber research centre at Changi Naval Base in Singapore. This centre, known as the 'ASEAN Defense Ministers' Meeting Cybersecurity and Information Centre of Excellence (ACICE),' was initially founded in June 2021.[6]

According to Singapore's Ministry of Defence, cybercrime in Southeast Asia surged by 82 per cent between 2021 and 2022, with 80 per cent of internet users receiving misinformation and threats.[7] Accordingly, ACICE has developed three key objectives to help counter the rising cyber challenges. The first objective is to share information on cyber threats to the defence sector of ASEAN countries. This involves providing early warnings, such as ransomware alerts, and reporting on phishing attacks and misinformation.

The second objective entails gathering intelligence on possible threats using ACICE's Malware Information Sharing Platform (MISP). It became operational in February 2023 and enables ASEAN countries to share information on important cyber and malware threats in order to provide early warnings and mitigate cyberattacks. The third objective is to provide a networking platform for regional and international experts from the private sector, industry, and academic institutions. This year also saw the formation of an ACICE Experts Panel, comprised of academics and industry experts, to stimulate meaningful discussions about cybersecurity challenges.[8]

Limitations of South Asian Cyber Cooperation Architecture

Among South Asian countries, India, Sri Lanka, and Afghanistan have fairly well-developed national Computer Emergency Response Teams (CERT) for monitoring and protective operations, known as CERT-In, SLCERT, and AFCERT respectively. Instead of a national CERT, Pakistan has two private entities that provide cyber threat information: the Pakistan Computer Emergency Response Team (PakCERT) and the Pakistan Information Security Association Computer Emergency Response Team (PISA-CERT).

Moreover, Bangladesh, Bhutan, and Nepal each have their own national Computer Incident Response Teams (CIRT) for assessing and responding to computer security incident reports, known as BGD e-Gov CIRT, BtCIRT, and Nepal CERT respectively. The Maldives, on the other hand, lacks a cyber security mechanism to detect and mitigate cyber threats, leaving government websites open to hacking and vandalism.[9]

Overall, South Asian countries lack a centralised authority, primarily due to the asymmetrical distribution of responsibilities among several cyber security agencies. For instance, India's cyber security architecture includes several agencies and ministries with ambiguous roles in managing cyber security issues in India, including the Ministries of Home Affairs, Defense, and Electronics and Information Technology.[10] Hence, the major challenge for South Asian countries is integrating numerous cyber security arms to form a coordinated response to cyber intrusions.

Another impediment to establishing a regional cyber cooperation capability is the absence of a shared cyber lexicon that defines the relative implications of a cyber emergency on information

infrastructure. Furthermore, many inter-state conflicts, such as the India-Pakistan dispute, obstruct the prospects of regional cyber collaboration. In this complex historical environment, there is a lack of trust and transparency, resulting in a restricted exchange of threat intelligence. The porous nature of cyber networks further complicates the evaluation of countries' engagement in regional cyber impact operations.

Additionally, the South Asian Association for Regional Cooperation (SAARC), an intergovernmental organisation, has been unable to fully perform because it has failed to identify shortcomings and create coherence in cyber response. Hence, South Asia lacks institutional frameworks for a cyber response in which relevant stakeholders can share threat intelligence and coordinate, as ASEAN states are attempting.

Recommendations for the South Asian Cyber Response Framework

South Asian countries have various cyber development drivers at their disposal. However, comprehensive information-sharing remains insufficient in the region, as a culture of transparency between countries remains elusive. To address this issue, South Asian countries should establish a regional working group comprising technocrats and policymakers from each country in the region. This group could facilitate regular dialogues on diverse cyber terminologies and interpretations. A solid foundation for the common Cyber Lexicon of South Asia could also be provided by referring to recognised international cyber security frameworks, such as the National Institute of Standards and Technology (NIST).

Moreover, Standard Operating Procedures (SOPs) have to be ensured for effective information sharing at the regional level. To that end, respective countries should reach an agreement on a standard model for cyber-incident classification as well as the types of cyber-emergency response operations required at each level. Following that, response operations could be categorised, with each stakeholder assigned specific tasks and responsibilities.

Another critical step in establishing effective cyber governance in South Asia is to appoint overarching authority for coordinating in the event of a cyber emergency. The ASEAN Cybersecurity Coordinating Committee (Cyber-CC) plays a similar role within the ASEAN countries.[11] In South Asia, such a committee should be formed to approve emergency response protocols when a cyber crisis is declared a regional emergency. Pakistan could take the lead in initiating the establishment of such a committee.

Noteworthy, the aforementioned regional initiatives will remain ineffective unless national-level improvements are implemented. At the national level, there should be effective mechanisms in place to regulate policymaking for cyber threat identification and mitigation. This can be problematic in South Asia, where cyber security is not often a top priority for countries. Given the uneven growth of national digital capacities, achieving the needed consensus to drive the regional discourse on cyber regulations seems less plausible.

For this reason, public-private partnerships on cyber-security mechanisms should be improved, as robust coordination between government agencies and the private sector could more evenly strengthen each country's digital assets. In a similar vein, strong levels of collaboration among Computer Emergency Response Teams (CERTs) are critical. The remaining South Asian countries that have not established national CERTs should do so in order to progress toward formalising CERT collaboration.

Conclusion

In a post-truth world, cyberspace is evolving into an arena of strategic influence and assertive actions. The Russia-Ukraine war has also underlined the significance of regional cooperation frameworks among states in addressing information risks stemming from geopolitical conflict. In addition, the rising threat posed by non-state actors or hacking groups like Anonymous and Squad303 further

emphasises the need for South Asian countries to develop a robust cyber security architecture to improve cyber resilience across the region.

Consequently, a clearly defined national cyber security architecture among countries is critical for the region's leap forward in the cyber realm. However, the priority accorded to cyber security in national interests varies across South Asia. The challenge lies in synchronising collaboration to establish a robust cyberspace in the region. To that end, the region's cyber security architecture should ensure that states with limited capabilities in dealing with cyber crises or building cyber-centric frameworks receive adequate support.

Furthermore, threat intelligence-sharing agreements in South Asia could pool collective knowledge of countries to provide early warnings and effective cyberattack mitigation. Cyber security cooperation within SAARC member states would have been desirable, however, due to interstate rivalry, this organisation has failed in regionalism. The frequent clashes over traditional security issues have left Pakistan and India with limited incentives to engage with each other. Nevertheless, with cyber security gaining prominence as a critical non-traditional security concern, creating a new regional framework could prove pivotal for fostering confidence-building measures (CBMs) between India and Pakistan to address the emerging cyber threat landscape in the foreseeable future.

Notes and References

1 "Global Cybersecurity Index," *ITU*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

2 "Pegasus Snooping: Pakistan Probes Whether PM Khan's Phone Hacked," *Al Jazeera*, 20 July 2021, https://www.aljazeera.com/news/2021/7/20/pegasus-snooping-pakistan-imran-khan-phone-hacked.

3 "Investigation Finds NSO Group Spyware Sold to Governments Used Against Activists, Politicians & Journalists; Company Denies Allegations," *Business & Human Rights Resource Centre*, 27 September 2021, https://www.business-humanrights.org/en/latest-news/nso-group-spyware-sold-to-governments-used-to-target-activists-politicians-journalists-according-to-pegasus-project-investigation-company-denies-allegations/.

4 Palwasha Khan, "Building a Bilateral Framework for Cybersecurity in South Asia," *Stimson Center*, 12 November 2021, https://www.stimson.org/2021/building-a-bilateral-framework-for-cybersecurity-in-south-asia/.

5 "Cybersecurity Governance in South Asia: India and Pakistan," *EFSAS*, August 2022, https://www.efsas.org/publications/articles-by-efsas/cybersecurity-governance-in-south-asia-india-and-pakistan/.

6 Gabriel Dominguez, "ASEAN Sets Up Regional Office for Cybersecurity Cooperation," *The Japan Times*, 18 July 2023, https://www.japantimes.co.jp/news/2023/07/18/asia-pacific/asean-cyberattacks-operations-center/.

7 Ibid.

8 "Fact Sheet: ASEAN Defence Ministers' Meeting (ADMM) Cybersecurity and Information Centre of Excellence (ACICE)," *MINDEF Singapore*, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2023/February/27feb23_fs.

9 E. Dilipraj, "South Asian Cyber Security Environment: An Analytical Perspective," *Asian Defence Review* 2014-2015, ed. Vinod Patney (Knowledge World Publishers, 2015), 161-190. https://www.academia.edu/15710049/SOUTH_ASIAN_CYBER_SECURITY_ENVIRONMENT_AN_ANALYTICAL_PERSPECTIVE.

10 EFSAS, "Cybersecurity Governance in South Asia."

11 Kai Lin Tay, "ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework," *International Institute of Strategic Studies*, June 2023, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/06/asean-cyber-security-cooperation.pdf.