BIPSS Commentary
www.bipss.org.bd November - 2024
BIPSS Towards a Secure World

# Building Digital Defenses: Securing Cyberspace in South Asia

**Alice Daversin**[1]

## Introduction

Cybersecurity is a critical issue, fundamental in an increasingly digitized world. Technological advancements, while paving the way for unprecedented opportunities for economic and social development, have also multiplied vulnerabilities within critical infrastructures[2]. In South Asia, the threat of cyberattacks has profound implications for regional stability. Cyber threats go beyond breaches of data privacy or information system security; they challenge national security and the sovereignty of states. The South Asian digital landscape, encompassing nations with varying cybersecurity capabilities, is also vulnerable to attacks orchestrated by both state and non-state actors[3]. These challenges are exacerbated by a lack of regional cooperation and often fragmented national policies. In this context, the need for a robust and integrated cybersecurity framework is more pressing than ever.

This commentary aims to analyze the current state of cybersecurity in South Asia, focusing on the region's specific vulnerabilities and ongoing institutional responses. Furthermore, it seeks to propose concrete solutions to strengthen digital defenses, emphasizing South-South cooperation and the exchange of best practices. By examining existing initiatives and suggesting innovative approaches, this paper aspires to contribute to a constructive dialogue on how to secure cyberspace in South Asia while promoting regional stability.

## State of Cybersecurity in South Asia

Cybersecurity in South Asia is at a critical crossroads, characterized by a proliferation of digital threats that challenge national security infrastructures. A typology of those threats can be outlined:

1. **Cybercrime**[4]**:** This phenomenon encompasses a range of illegal activities executed via computer systems and networks. In South Asia, the rise of cybercrime is particularly alarming, with reports indicating an increase in cases of online fraud, identity theft, and ransomware. These attacks not only cause financial losses but also undermine consumer and business trust in digital systems.

---

[1] Alice Daversin is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). She is currently completing her master's degree in Geostrategy, Defence and International Security at Sciences Po Aix-en-Provence (France).

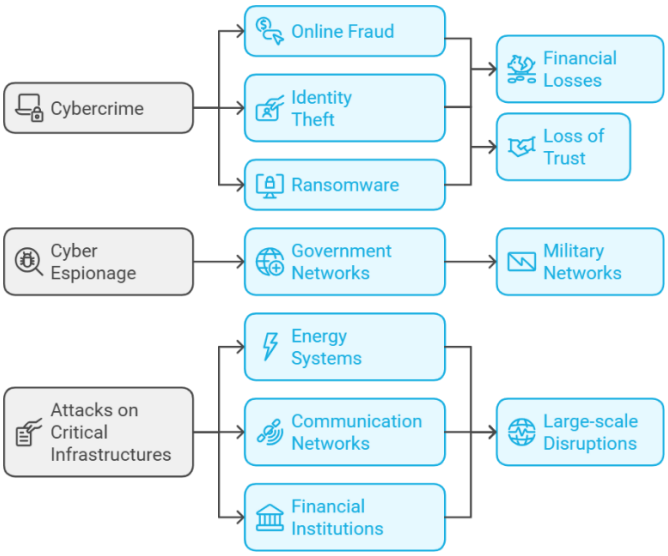
[2] Tie Xu and Anthony J. Masys, 'Critical Infrastructure Vulnerabilities: Embracing a Network Mindset', in *Exploring the Security Landscape: Non-Traditional Security Challenges*, ed. Anthony J. Masys (Cham: Springer International Publishing, 2016), 177–93. https://doi.org/10.1007/978-3-319-27914-5_9

[3] Nayan Rajiv and Shekhar Ravi, 'Paradoxes of South Asian Security', *Asian Journal of Peacebuilding* 8, no. 2 (30 November 2020): 333–56. https://doi.org/10.18588/202011.00A070

[4] Osman Goni, 'Introduction to Cyber Crime', *International Journal of Engineering and Artificial Intelligence*, 2022. https://doi.org/10.55923/jo.ijeal.3.1.701

2. **Cyber Espionage**[5]**:** Countries in the region, notably India and Pakistan, face targeted espionage threats that exploit vulnerabilities to infiltrate government and military networks.

3. **Attacks on Critical Infrastructures**[6]**:** The security of essential infrastructures, such as energy systems, communication networks, and financial institutions, is severely threatened by cyberattacks. These infrastructures, vital for the daily functioning of states, represent attractive targets for cybercriminals and state actors seeking to cause large-scale disruptions.




*Source: Typology of Cyberthreats (Daversin, 2024)*

To illustrate the gravity of these threats, two major incidents that occurred in South Asia deserve particular attention. First, there is the incident involving the banking system of Bangladesh in 2016, which resulted in the theft of $81 million by hackers using credentials from the SWIFT network[7]. The attack was orchestrated from poorly secured networks and highlighted significant gaps in the bank's cybersecurity. This theft not only caused substantial financial losses but also triggered a crisis of confidence in the country's banking system, underscoring the urgent need to improve cybersecurity in the financial sector. Similarly, India has been the target of several cyberattacks aimed at its critical infrastructures, including attempts to breach its energy and defense networks. One of the most notable threats was the attack on Mumbai's power grid in 2020, seeking to disrupt command and control systems[8]. These incidents highlight not only the vulnerability of infrastructures but also the necessity of a coordinated national response to enhance resilience against cyber threats.

---

[5] Esma Dilek and Ozgur Talih, 'Overview of Cyber Espionage Incidents and Analysis of Tackling Methods', *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)*, 19 October 2022, 55–60. https://doi.org/10.1109/ISCTURKEY56345.2022.9931893

[6] N. Abouzakhar, 'Critical Infrastructure Cybersecurity : A Review of Recent Threats and Violations', 2013, https://www.semanticscholar.org/paper/Critical-Infrastructure-Cybersecurity-%3A-A-Review-of-Abouzakhar/877c95663ad2db4845d49ed24365b4fe2584dd8e.

[7] Mohammed Mazumder and Abdus Sobhan, 'The Spillover Effect of the Bangladesh Bank Cyber Heist on Banks' Cyber Risk Disclosures in Bangladesh', *The Journal of Operational Risk*, 2021. https://doi.org/10.21314/JOP.2020.249

[8] Abhishek Pandey et al., 'Dynamic Modeling and Cascade Failure Analysis of the Mumbai Grid Incident of October 12, 2020', *IEEE Access* 10 (2022): 43598–610. https://doi.org/10.1109/ACCESS.2022.3160740

Assessing national cybersecurity capabilities in South Asia is essential to understand how countries in the region are preparing to face an increasingly threatening digital environment. This summary table has been compiled using information from the UNIDIR Cyber Policy Portal [9], which provides a comprehensive overview of national cybersecurity strategies. An examination of the cybersecurity policies implemented in India, Pakistan, Bangladesh, and Sri Lanka reveals distinct approaches and frameworks tailored to each country's unique challenges and priorities[10]:

| Country | Key Strategy documents | Key institutions & Implementations | Legal Framework |
|---|---|---|---|
| **India** | **National Cyber Security Policy** (2013, updated 2021) | - National Critical Information Infrastructure Protection Centre (NCIIPC)<br>**- Indian Computer Emergency Response Team** (CERT-In) | - Information Technology Act, 2000 (amended 2008)<br>- Personal Data Protection Bill 2018<br>- National Information Security Policy |
| **Pakistan** | Cyber Security Strategy for Telecom Sector 2023-2028 | **- National Response Centre for Cyber Crime (NR3C)**<br>- **PakCERT** | **- Prevention of Electronic Crimes Act 2016**<br>- National Cyber Security Policy 2021 |
| **Bangladesh** | **National Cybersecurity Strategy** (2021) | - Bangladesh Computer Council (BCC),<br>**- Bangladesh CERT** (BGD e-GOV CIRT) | - **Digital Security Act 2018**<br>- Information and Communication Technology Act |
| **Sri Lanka** | - **Information and Cyber Security Strategy** (2019-2023) | - **Sri Lanka CERT** | **- Cyber Security Regulatory Authority**<br>- Cyber Crime Unit |

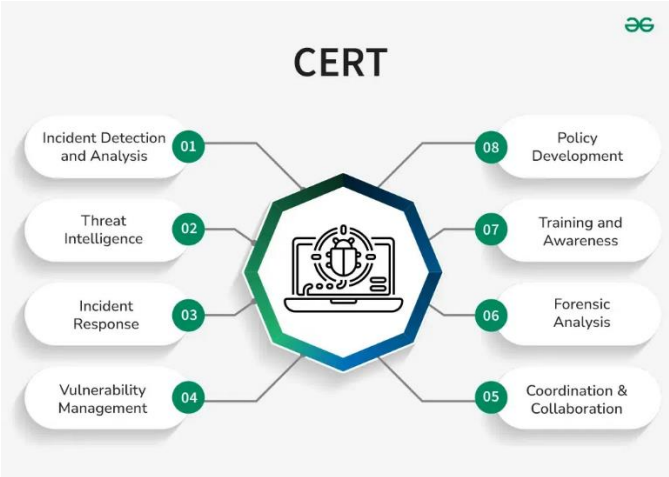
*Source: Comparative Overview of Cybersecurity Strategies in South Asia (Daversin, 2024)*

In India, while the National Cyber Security Policy of 2013 and the establishment of CERT-In have laid solid foundations, gaps remain due to a lack of coordination among agencies and insufficient qualified personnel[11]. In Pakistan, despite the advancement represented by the Prevention of Electronic Crimes Act (PECA) of 2016, the absence of a coherent national strategy and modern infrastructure limits the effectiveness of responses to cyber threats, even with the presence of the National Response Centre for Cyber Crimes (NR3C) and a dedicated CERT. Bangladesh, despite notable efforts to enhance its cybersecurity with its 2020 strategy and the establishment of a CERT, faces persistent vulnerabilities and a lack of resources and training. Finally, Sri Lanka, having intensified its efforts following the 2019 attacks, suffers from technical and organizational shortcomings, with insufficient investments and limited public awareness, although it has also established a CERT.

[9] UNIDIR Cyber Policy Portal https://cyberpolicyportal.org/

[10] Mark Linscott and Gopal Nadadur, 'Mapping South Asia's Digital Landscape', *Atlantic Council* (blog), 14 November 2024. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mapping-south-asias-digital-landscape/

[11] Hannes Ebert, 'Hacked IT Superpower: How India Secures Its Cyberspace as a Rising Digital Democracy', *India Review* 19, no. 4 (7 August 2020): 376–413. https://doi.org/10.1080/14736489.2020.1797317




*Source: GeeksforGeeks*

These combined challenges underscore the need for an integrated and collaborative approach to improve cybersecurity in the region.

## Challenges to Cybersecurity in South Asia

Cybersecurity in South Asia faces a multitude of internal and external challenges that compromise states' abilities to protect their critical infrastructures and ensure the safety of their citizens in an increasingly complex digital environment.

One of the primary challenges confronting South Asian countries is the lack of dedicated financial and human resources for cybersecurity[12]. Many states face budgetary constraints that limit their ability to invest in robust cybersecurity infrastructures. Furthermore, there is a shortage of qualified professionals in the cybersecurity field[13]. Educational and training programs are insufficient to meet the growing demand for experts capable of designing and implementing effective defense strategies. This skills gap renders organizations vulnerable to cyberattacks, as they lack the necessary expertise to anticipate, detect, and respond to emerging threats.

Another major challenge lies in the often-insufficient coordination among the various government agencies responsible for cybersecurity[14]. In many cases, efforts are fragmented, with each agency working in isolation without a comprehensive and integrated strategy. This lack of synergy hinders the effective implementation of policies. Ineffective inter-agency communication can also exacerbate security risks, as inappropriate or poorly synchronized responses increase the likelihood of crisis escalation.

[12] Rohit Karki, 'Cybersecurity Governance in South Asia' (Geneva Centre for Security Sector Governance, 2023).https://www.dcaf.ch/sites/default/files/publications/documents/Cybersecurity_Governance_in_South_Asia_EN.pdf

[13] Falendra Kumar Sudan, 'Technological Disruptions, Youth Unemployment and Vocational Education Challenges in South Asia: A Short Report', *Global Economics Science*, 11 June 2021, 80–97. https://doi.org/10.37256/ges.222021769

[14] Tanvir Hassan Zoha and Sifat Nur Billah, 'The Implications of State-Sponsored Cyber Attacks in South Asian Countries', *International Journal of Chaotic Computing*, 30 June 2022, 204–8. https://doi.org/10.20533/ijcc.2046.3359.2022.0026

About external challenges, persistent geopolitical tensions and border disputes, particularly between India and Pakistan, represent a significant barrier to cybersecurity cooperation[15]. The relationship between these two nuclear powers is marked by deep mistrust, often manifesting in reciprocal cyberattacks[16]. This dynamic creates an environment where security cooperation is perceived as a risk, making it difficult to establish the trust mechanisms necessary to address common challenges.


*Source: The Economist*

Finally, the growing influence of non-state actors and cybercriminals poses a major challenge to cybersecurity in South Asia[17]. Terrorist groups and criminal organizations exploit vulnerabilities in cyberspace to conduct attacks, finance their operations, and recruit new members. Additionally, the decentralized and often anonymous nature of the Internet complicates the attribution of cyberattacks. Governments struggle to respond effectively to threats as they navigate a landscape where the boundaries between state and non-state actors are blurred.

## Frameworks for Digital Cooperation and Defense

In this context, establishing a multilateral cybersecurity framework appears to be a strategic necessity. Cooperation in cybersecurity could not only enhance mutual trust but also reduce potential escalations due to cyberattacks. One key aspect of this framework could be the creation of Cybersecurity Working Groups composed of experts from each country. These groups would be tasked with developing a

[15] Sameer Patil, 'India's Cyber Security Landscape', in *Varying Dimensions of India's National Security: Emerging Perspectives*, ed. Anshuman Behera and Sitakanta Mishra (Singapore: Springer Nature, 2022), 75–90. https://doi.org/10.1007/978-981-16-7593-5_6

[16] Tughral Yamin, 'Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan' (Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), 1 June 2014), https://doi.org/10.4018/978-1-4666-8456-0.CH009

[17] Ryan Clarke, *Crime-Terror Nexus in South Asia: States, Security and Non-State Actors* (London: Routledge, 2011), https://doi.org/10.4324/9780203818947

framework that could include measures for transparency, information sharing, and emergency protocols in the event of cyber incidents. Regional organizations, such as the South Asian Association for Regional Cooperation (SAARC), could have a crucial role to play in promoting cybersecurity in South Asia[18].


*Source: South Asian Association for Regional Cooperation members (IPIS & Somesh Upadhyay (UPSC))*

SAARC could revitalize its efforts to include cybersecurity initiatives within its agenda. Although SAARC has often been paralyzed by political tensions, cybersecurity represents a domain where members could find common interest[19]. Regional workshops to train incident response teams, as well as conferences on best practices in cybersecurity, could be organized to strengthen the capabilities of each member state.

Experiences from other regions of the world offer relevant examples of best practices in cybersecurity. The European Union, for instance, has developed implemented several initiatives, including the General Data Protection Regulation (GDPR), the EU Cybersecurity Strategy, which emphasizes coordination, and the European Union Agency for Cybersecurity (ENISA), which plays a central role in coordinating cybersecurity efforts, providing guidelines and resources to help countries strengthen their infrastructures[20]. On its side, ASEAN has demonstrated the effectiveness of cybersecurity cooperation

[18] Munish Sharma and Cherian Samuel, 'A South Asian Regional Cybersecurity Cooperation (SARCC) Forum: Prospects and Challenges', *Secyring Cyberespace*, 2016. https://www.idsa.in/system/files/book/book_securing-cyberspace_0.pdf#page=270

[19] Arpita Mukherjee and Divya Satija, 'Regional Cooperation in Industrial Revolution 4.0 and South Asia: Opportunities, Challenges and Way Forward', *South Asia Economic Journal* 21, no. 1 (March 2020): 76–98. https://doi.org/10.1177/1391561420908078

[20] Predrag Škundrić, Vanja Korać, and Zoran Davidovac, 'EU Cyber Initiatives and International Cybersecurity Standards — An Overview', *Arheologija i Prirodne Nauke* 18 (2022): 269–78. https://doi.org/10.18485/arhe_apn.2022.18.18

through its Cybersecurity Cooperation Strategy[21]. This initiative has enabled member countries to share information on threats and harmonize their cybersecurity legislation.

## Strategies to Strengthen Digital Defenses in South Asia

To address these challenges, it is essential to implement multidimensional strategies aimed at building capacities, developing appropriate policies, and promoting trust and transparency among states. The development of cybersecurity capabilities begins with adequate training and widespread awareness. South Asian governments must invest in educational programs to train qualified professionals in cybersecurity[22]. This includes not only technical training for IT experts but also awareness sessions for the general population to cultivate a culture of cybersecurity[23]. Initiatives such as *Cybersecurity Days* and *awareness weeks* can be organized to educate citizens about digital risks and best practices. Concurrently, academic institutions should be encouraged to develop specialized cybersecurity curricula that integrate the technical, legal, and ethical aspects of this evolving field.

Collaboration between the public and private sectors is crucial for developing innovative cybersecurity solutions[24]. Technology companies could provide technical skills and resources to bolster states' digital defenses. For example, public-private partnerships can be established to design cybersecurity tools tailored to the specific needs of critical infrastructures.

To establish a secure digital environment, it is also imperative for countries in the region to develop harmonized laws regarding cybersecurity and data protection[25]. A unified approach would facilitate the exchange of information on threats and the implementation of incident response protocols. Asia.

Finally, promoting trust among South Asian states involves establishing effective communication mechanisms for managing cybersecurity incidents. Transparency in cybersecurity operations is essential to build trust among states. Governments must be willing to share information about their cybersecurity capabilities and the threats they face, while respecting concerns related to national security. By publishing regular reports on the state of their cybersecurity and engaging in open dialogues with other nations, South Asian countries can contribute to creating a trustworthy environment conducive to cooperation.

---

[21] Khotimah Estiyovionita and Afandi Sitamala, 'Asean's Role In Cybersecurity Maintenance And Security Strategy Through An International Security Approach', *Lampung Journal of International Law* 4, no. 2 (14 October 2022): 77–86. https://doi.org/10.25041/lajil.v4i2.2556

[22] Ruth Shillair et al., 'Cybersecurity Education, Awareness Raising, and Training Initiatives: National Level Evidence-Based Results, Challenges, and Promise', *Computers & Security* 119 (1 August 2022): 102756,. https://doi.org/10.1016/j.cose.2022.102756

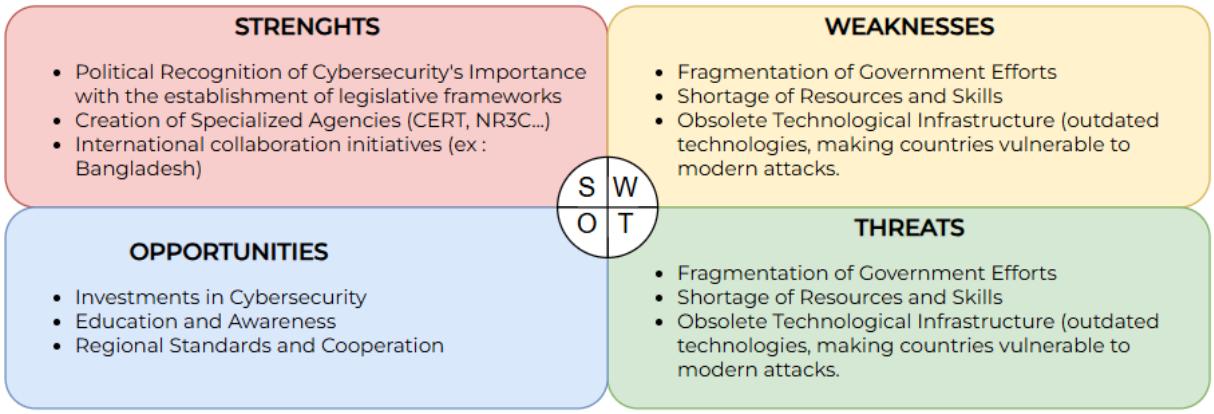
[23] Nadeem Ahmed et al., 'Cybersecurity Awareness Survey: An Analysis from Bangladesh Perspective', in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, 2017, 788–91. 10.1109/R10-HTC.2017.8289074

[24] Vasaki Ponnusamy, N. Z. Jhanjhi, and Mamoona Humayun, 'Fostering Public-Private Partnership: Between Governments and Technologists in Developing National Cybersecurity Framework', ed. Vasaki Ponnusamy, Khalid Rafique, and Noor Zaman, 2020, 237–55. https://doi.org/10.4018/978-1-7998-1851-9.ch012

[25] Muhammad Imran Ali and Khadeeja Ahmad Hussain, 'Unveiling the Tapestry: A Comparative Investigation into Data-Protection Legislation in India and Pakistan', *Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law.* 2024, no. 1–28 (28 May 2024): 1–8. https://doi.org/10.25143/socr.28.2024.1.01-08

## Conclusion

The SWOT diagram presented below summarizes the strengths, weaknesses, opportunities, and threats related to cybersecurity in South Asia, highlighting the need for a collective and proactive approach to strengthen digital defenses.




*Source: Strengths, Weaknesses, Opportunities, and Threats in South Asia's Cybersecurity Landscape (Daversin, 2024)*

Indeed, the assessment of cybersecurity capabilities in South Asia has revealed critical issues, including the fragmentation of government efforts, resource shortages, and geopolitical tensions. In response to these challenges, solutions such as the establishment of cooperative frameworks, the development of harmonized policies, and the promotion of cybersecurity awareness must be implemented. It is imperative to call for enhanced cooperation among states in the region to secure the digital space, building strategic partnerships and sharing resources. By mobilizing political and financial efforts, South Asian countries can envision a secure future where cybersecurity is integrated into national priorities, allowing citizens to navigate cyberspace with confidence.