CSDR
COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

SOUTH ASIAN FUTURES FELLOWSHIP

FRIEDRICH EBERT STIFTUNG

COMMENTARY

WHERE GEOPOLITICS MEETS CYBERSECURITY: EXAMINING THE CHALLENGES AND POTENTIAL FOR CYBER COOPERATION IN SOUTH ASIA

LOKENDRA SHARMA

SOUTH ASIAN FUTURES FELLOWSHIP

THE SOUTH ASIAN FUTURES FELLOWSHIP ANNUALLY SUPPORTS EARLY CAREER RESEARCHERS BASED IN THE SOUTH ASIAN REGION, INTERESTED IN EXPLORING THE IMPACT OF GEOPOLITICS ON REGIONAL COOPERATION. FELLOWS ARE AT DIFFERENT STAGES OF THEIR CAREERS WITH EXPERTISE ON NON-TRADITIONAL SECURITY ISSUES; THEY PARTICIPATE IN WORKSHOPS, PRODUCE POLICY PIECES, AND ARE PROVIDED THE OPPORTUNITY OF A 1-MONTH RESEARCH RESIDENCY IN A SOUTH ASIAN CITY. DURING THIS RESIDENCY THEY WORK AT A PARTNER THINK TANK, ENGAGE WITH EXPERTS, AND CONDUCT FIELD STUDY ON A TOPIC OF THEIR INTEREST. THE FELLOWSHIP PRODUCES, AND ENGAGES WITH, REGIONAL NARRATIVES AND FACILITATES KNOWLEDGE EXCHANGE ON SHARED CHALLENGES IN AN EVOLVING GEOPOLITICAL CONTEXT IN THE SOUTH ASIAN REGION.

ABOUT THE AUTHOR

LOKENDRA SHARMA IS A PHD CANDIDATE AT THE NATIONAL INSTITUTE OF ADVANCED STUDIES, BENGLAURU. FOR HIS PHD THESIS, HE IS RESEARCHING INDIA'S APPROACH TO THE GOVERNANCE OF CYBERSPACE AND THE INTERNET. HIS PRIMARY RESEARCH INTERESTS ARE CYBERSPACE GOVERNANCE, INTERNET GOVERNANCE, CYBERPOLITICS, CYBERSECURITY, AND ISSUES LYING AT THE INTERSECTION OF TECHNOLOGY AND POLITICS (INCLUDING NUCLEAR DEVELOPMENTS). HE HAS QUALIFIED FOR JUNIOR RESEARCH FELLOWSHIP OFFERED BY THE UNIVERSITY GRANTS COMMISSION, GOVERNMENT OF INDIA, IN TWO SUBJECTS: INTERNATIONAL AND AREA STUDIES (DECEMBER 2019); DEFENCE AND STRATEGIC STUDIES (JUNE 2019). HE'S ALSO AN ACTIVE VOLUNTEER IN THE INTERNET GOVERNANCE COMMUNITY, AND IS CURRENTLY THE CO-CONVENER OF THE PROGRAM COMMITTEE OF THE ASIA PACIFIC REGIONAL INTERNET GOVERNANCE FORUM. HE HAS PUBLISHED ON CYBER AND INTERNET RELATED ISSUES IN NEWSPAPERS AND JOURNALS, AND HAS PRESENTED HIS WORK IN ACADEMIC CONFERENCES IN INDIA AND EUROPE.

Where geopolitics meets cybersecurity: Examining the challenges and potential for cyber cooperation in South Asia

South Asia is one of the biggest targets of cyberattacks due to poor cyber hygiene and a lack of emphasis on cybersecurity at all levels: government, private, and individual. Despite the gravity of the issue, fraught geopolitics of the region has prevented any cooperation even on a non-traditional security issue like cybersecurity. This article opens with the cybersecurity threat landscape of the region; it goes on to unpack the geopolitical hurdles in the way of cyber cooperation; and concludes by highlighting avenues for potential cooperation. Given the region's cybersecurity profile and geopolitical context, the main argument is: it is feasible to develop a regional mechanism to address cybersecurity threats to peoples, critical infrastructure, and the private sector.[1]

South Asia's cybersecurity landscape

The cybersecurity profile of South Asia is concerning. According to a comprehensive report published jointly by three Bangladeshi institutions, including the country's Computer Incident Response Team, "over 4,000 various types of amplified DDoS [Distributed Denial of Service] attacks on the country" were detected in 2022.[2]

The situation in Nepal mirrors this pattern. In January 2023, Nepal faced one of its biggest cyberattacks. Around 1500 government websites were impacted and the attack "even halted international travel due to the shutdown of the immigration server".[3]

In Sri Lanka, a recent ransomware attack impacted about 5000 emails using the gov.lk domain; all this data was lost since government cloud data was not backed up for more than three months (17 May to 26 August, 2023).[4]

In early 2023, Maldives' major air tourism company, Trans Maldivian Airways, was dealing with a ransomware attack.[5] Bhutan has also been a victim of cyberattacks over the years.[6]

India remains the most targeted country for cyberattacks in the region, largely due to its sheer size and geopolitical circumstances. According to an IBM report, India was one of the most attacked countries in Asia in 2021.[7]

South Asia's worrying cybersecurity profile is reflected in global rankings. According to the Global Cybersecurity Index (GCI) 2020, published by the International Telecommunications Union, Bangladesh ranked 53rd, Nepal 94th, Sri Lanka 83rd, Maldives 177th, Bhutan 134th, and India ranked 10th.[8] While India is comparatively better ranked by the 2020 GCI, another estimate—Cyber Defense Index 2022/23 by the MIT Technology Review—ranks India at 17 out of 20 major economies of the world.[9]

While the statistics above may suggest that South Asian countries are individually recipient of cyberattacks, that is not that case. Certain cyberattacks have targeted multiple countries within the region. For instance, government, aviation, telecom and educational entities were targeted in 2022-2023 by an advanced persistent threat known as Lancefly.[10] A recent report claimed that a China-based group called RedHotel had targeted South Asian countries including Bangladesh, Bhutan, Nepal and India.[11]

South Asian countries have many shared characteristics such as developing economies, historically low digital penetration rates, recently expanding internet user bases, relatively cheaper consumer electronics, and low cyber awareness.

This has meant that many cyber vulnerabilities are shared beyond national borders and across the region.

However, despite being under threat from common actors as well as shared cyber vulnerabilities, the response to cybersecurity incidents has primarily been country-centric (led by the respective computer emergency response teams). Cyber cooperation among South Asian countries could have helped thwart cross-border attacks looking to exploit shared vulnerabilities.

It is widely acknowledged that weak laws and regulations, inadequate institutional structures, and limited cyber awareness contribute significantly to the region’s poor cybersecurity. One factor that is often overlooked is the lack of cyber cooperation due to the region’s geopolitics.

Geopolitical hurdles

Given the geopolitically sensitive nature of South Asia, and a lack of regionalism, South Asia has witnessed very limited cooperation on traditional security issues. There has been subpar cooperation even on cybersecurity that straddles both traditional security (for example, cyberattacks on military assets) and non-traditional security (for example, cybercrime and cyberattacks on private companies). In contrast to regions like ASEAN, Europe and North America, which have established cybersecurity cooperation mechanisms, South Asia lacks any such framework.

While India’s size—geographical, economic and demographic—provides New Delhi with economic and political heft to assist its smaller neighbors (primarily Bhutan, Nepal and Sri Lanka) in cybersecurity challenges, it also produces insecurity and a heightened threat perception about New Delhi’s cyber capabilities. Alleged cyberattacks originating from India directed at neighboring countries further complicate its situation. For example, India-linked Advanced

Persistent Threat actor SideWinder has allegedly been involved in cyberattacks against entities in Afghanistan, Bhutan, Myanmar, Nepal and Sri Lanka.[12]

Geopolitics is also enmeshed with the attribution problem of cyberspace. It is difficult, if not impossible, to reliably attribute a cyberattack to an actor in a short span of time given the technical challenges involved. Mutual lack of trust resulting from geopolitics makes the exercise of attribution (and acceptance of an attribution as reliable) all the more difficult.

Further, geopolitical contestations often spill over into the cyber domain, as seen in the cyber tit-for-tat case of India and Nepal in 2020 when both countries were engaged in a boundary dispute over the Limpiyadhura-Kalapani-Lipulekh area.[13]

Potential for cooperation

Despite these hurdles, avenues for fostering cybersecurity cooperation do exist in South Asia. There are multiple bilateral cooperation mechanisms in place in South Asia that can be built upon to develop a regional mechanism. For instance, Indian Computer Emergency Response Team and Bangladesh e-Government Computer Incident Response Team have signed an MoU for cooperation on cybersecurity matters.[14] India also cooperates on cybersecurity with Bhutan and Maldives.[15] Building on these initiatives, computer emergency (or incident) response teams of South Asian states could come together to form a regional mechanism to address cybersecurity threats to peoples, critical infrastructure, and the private sector in the region.

To establish trust, it may be necessary to exclude cyberattacks on governments and militaries from the scope of such a regional mechanism due to the deeply securitized nature of these attacks. This mechanism can be tried at a limited scale, and as it matures it can eventually expand to include countries from the extended South Asian region. Such a regional mechanism could at least succeed in achieving the limited yet crucial goal of fortifying civil cyber infrastructure in South Asia.

Endnotes

1. Afghanistan is out of scope of this article due to the country's prevailing security situation. Pakistan is out of scope too because the presence of Pakistan could lead to failure of a regional mechanism to take-off due to the perennial India-Pakistan problem (much similar to what happened to the South Asian Association for Regional Cooperation). However, as argued in the concluding paragraph of this article, Pakistan and Afghanistan can be included in a regional cybersecurity cooperation mechanism at a later stage when the mechanism matures.
2. BGD e-GOV CIRT. *Bangladesh Cyber Threat Landscape 2022*. Govt. of Bangladesh, 2022,https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/publications/effc311d_5097_46ba_afa4_5f44b60a93e6/Bangladesh%20Cyber%20Threat%20Landscape%202022.pdf (last accessed 23 Oct. 2023).
3. Ojha, Anup. "Cybercrime-Related Cases See an Alarming Rise in Nepal." *Asia News Network*, 17 Apr. 2023, https://asianews.network/cybercrime-related-cases-see-an-alarming-rise-in-nepal/ (last accessed 23 Oct. 2023).
4. Antoniuk, Daryna. "Sri Lankan Government Loses Months of Data Following Ransomware Attack." *The Record*, 11 Sept. 2023, https://therecord.media/sri-lanka-loses-months-of-government-data-in-ransomware-attack (last accessed 23 Oct. 2023).
5. "Trans Maldivian Data Breach: RansomHouse lists Airways as Victim." *The Cyber Express*, 13 Jan. 2023, https://thecyberexpress.com/trans-maldivian-data-breach-ransomhouse-lists-airways/ (last accessed 23 Oct. 2023).
6. Choejey, Pema. *Cybersecurity Challenges and Practices: A Case Study of Bhutan*. 2018. Murdoch University, PhD Dissertation.

https://researchportal.murdoch.edu.au/esploro/outputs/doctoral/Cybersecurity-challenges-and-practices-A-case/9910055418207078 91#file-0 (last accessed 23 Oct. 2023).

7. "Cyber Attacks: India Among Top 3 Most-Affected Nations in Asia in 2021." *Business Standard*, 24 Feb. 2022, https://www.business-standard.com/article/international/cyber-attacks-india-among-top-3-most-affected-nations-in-asia-in-2021-122022400945_1.html (last accessed 23 Oct. 2023).
8. ITU. *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity.* International Telecommunications Union, 2020, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (last accessed 23 Oct. 2023).
9. "The Cyber Defense Index 2022/23." MIT Technology Review, https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/ (last accessed 23 Oct. 2023).
10. Roy, Mousume. "South Asian organizations under cyberattack—how to mitigate the threat." *HCLTech*, 18 May 2023, https://www.hcltech.com/trends-and-insights/south-asian-organizations-under-cyberattack-how-mitigate-threat
11. Greig, Jonathan. "Chinese hackers targeted at least 17 countries across Asia, Europe and North America." *The Record*, 8 Aug. 2023, https://therecord.media/chinese-military-hackers-redhotel-target-countries-across-asia-north-america-europe
12. "India-Linked APT Group Carried Out Phishing Attacks Against Government Organisations in Asia, Say Analysts." *The Hindu*, 16 Feb. 2023, https://www.thehindu.com/sci-tech/technology/india-linked-apt-group-carried-out-phishing-attacks-against-government-organisations-in-asia-say-analysts/article66516032.ece (last accessed 23 Oct. 2023).

13. Dhungana, Shuvam. “Nepali and Indian ‘Hackers’ Attack Websites over ‘Boundary Dispute’.” *The Kathmandu Post*, 23 May 2020, https://kathmandupost.com/national/2020/05/23/nepali-and-indian-hackers-attack-websites-over-boundary-dispute; Kshatri, Shaurya. “Nepal-India Cyber War Might Get Uglier.” *The Himalayan*, 25 May 2020, https://thehimalayantimes.com/nepal/no-backing-off
14. “Cabinet Apprised of MoU Between India and Bangladesh for Cyber Security Cooperation.” *Press Information Bureau, Government of India*, 12 Jul. 2017, https://pib.gov.in/newsite/PrintRelease.aspx?relid=167341 (last accessed 24 Oct. 2023).
15. “India-Bhutan Cooperation on Cyber Security.” *Bhutan Today*, http://www.bhutantoday.bt/india-bhutan-cooperation-on-cyber-security/ (last accessed 24 Oct. 2023); Laskar, Rezaul H. “India Signs 6 Pacts with the Maldives; Cybersecurity, Defence Take Centrepoint.” Hindustan Times, 2 Aug. 2022, https://www.hindustantimes.com/india-news/india-signs-6-pacts-with-the-maldives-cybersecurity-defence-take-centrepoint-101659446885024.html (last accessed 24 Oct. 2023).

21, BLOCK C, QUTAB INSTITUTIONAL
AREA, NEW DELHI, DELHI 110016

PHONE: 011-43104566
EMAIL: OFFICE@CSDRONLINE.ORG
WEB: WWW.CSDRONLINE.ORG TWITTER:
@CSDR_INDIA