Crisis & Consequences: An Emerging Cyber Quandary for Sri Lanka

Divyanshu Jindal

Research Associate, Centre for Air Power Studies

Keywords: Sri Lanka, India, BIMSTEC, Crisis, Cyberspace, Cybersecurity.

Image Source: RoarMedia

Sri Lanka is amidst a deepening humanitarian and financial crisis today. The unfolding crisis has been deemed an outcome of a combination of 'bad luck, bad policy, and bad politics'.[1] In April, the island nation pre-emptively defaulted on around US$ 51 billion in foreign debt, and the Prime Minister declared the nation 'bankrupt' in early July. Many years of financial mismanagement have resulted in soaring inflation rates, and Sri Lankans are now struggling to meet daily necessities.

With the future still looking uncertain, the only certainty is that the crisis will induce far-reaching consequences at societal, national, and regional levels. While much is being talked about the economic, political, and geopolitical aspects, there has been less consideration towards how the crisis impacts Sri Lanka's interests in the cyber domain.

As seen in conflict and crisis situations around the world, societies are heavily influenced by the information they consume through the digital space. Further, national security is now deeply embedded in digital systems, through dependence on critical infrastructure sectors like communications., electricity, water, and waste management. This not only invokes a vulnerability at the societal level but also provides an exploitative avenue to shape the national discourse. Ultimately, these developments and their consequences spill over beyond the national frontiers, causing ripples in the regional dynamics.

In the past decade, Sri Lanka has risen in geostrategic significance, with China, Russia, and the US (among others) aspiring to benefit from the island nation's strategic location at the confluence of shipping routes in the Indian Ocean.[2] The Chinese 'debt-trap' diplomacy, India's concerns around it, and the absence of robust and active regional partnerships have played significant roles in shaping Sri Lanka's strategic landscape. As the world becomes increasingly dependent on digital technologies for growth and sustenance, it has to be asked what this crisis means for Sri Lanka's future in the cyber domain.

Sri Lanka in the cyber era

Sri Lanka has faced several cyberattacks in recent years. While the Liberation Tigers of Tamil Elam (LTTE) has sought to exploit cyberspace through proxy organizations like Tamil Eelam Cyber Force in recent months,[3] the Islamic State of Iraq and Syria (ISIS) has utilized Sri Lankan cyberspace to disseminate propaganda and hate speech in the recent past.[4]

In February 2021, several '.lk' domains were attacked and downed.[5] The websites were redirected to web pages highlighting social issues that impact Sri Lankans. Later in the year, a loss of an estimated 2,000 gigabytes of classified information from the Sri Lanka Cloud came to light.[6] The data was related to the National Medicines Regulatory Authority (NMRA) and contained confidential information on drug formulation.

As the economic struggle worsened, Sri Lankans sought new ways to retaliate against the government. In reaction to public uproar and pleas, the decentralized and international hacktivist collective 'Anonymous' crashed the websites of the Sri Lanka Police, the Ceylon Electricity Board, and the Department of Immigration and Emigration with Distributed-Denial-of-Service (DDoS) attacks in April.[7] These instances have highlighted the chinks in Sri Lanka's cyber armour.

However, as cyberattacks rarely remain confined to the intended battleground, this cyber campaign too had undesired consequences. The Anonymous group shared thousands of email addresses and usernames connected to students of various higher education institutions by attacking the database of 'Sri Lanka Scholar', which connects students to their institutions. In a similar attack, the hacktivist group revealed information about Sri Lankan employees working abroad who are registered with the Sri Lanka Bureau of Foreign Employment (SLBFE).

Before the crisis erupted, Sri Lanka had been taking small but gradual steps toward establishing legislation and strategies for the cyber domain. In October 2021, the Sri Lankan Cabinet granted approval to the proposals for drafting two bills on cybersecurity laws – on data protection and cyber defence.[8]

Due to Colombo's efforts towards cybersecurity, Sri Lanka's position in cyberspace improved. This was reflected in indexes like the National Cyber Security Index (NCSI) where Sri Lanka jumped from the 98th position in 2020 to the 69th position in 2021, out of 160 countries.[9] The NCSI is prepared by the International Telecommunications Union and measures the preparedness of countries to prevent cyber threats and manage cyber incidents. However, as the political and economic situation deteriorated, so did the investments and focus on cybersecurity seemingly waned. Consequently, Sri Lanka dropped to the 78th position in 2022.[10]

What Lies Ahead

Several case studies like Israel, Estonia, and North Korea raise the point that a country's size doesn't matter in the cyber domain. While this might be true to a certain extent, it cannot be ignored that the development of cyber capabilities requires legislative and strategic focus, as well as economic and human resources.

In the present scenario, Colombo will find it difficult in the short term to attend to cyber issues while its population struggles to meet basic necessities. In the long term, Sri Lanka will have to make significant efforts toward cyber capacity and capability building.

The crisis has exponentially increased the cyber threat profile in Sri Lanka. A 2021 estimate revealed that Sri Lanka will have 10,000 cybersecurity-related roles in the job market over the next five years but only a few hundred cybersecurity graduates to fill these positions.[11] As and when the Sri Lankan market looks to recover from the crisis, it will now need to put even more emphasis on securing its cyber interests.

The legislative process regarding Sri Lanka's cyber laws is bound to face delays. Further, as cybersecurity requires robust investments, Colombo will be in a quandary for balancing Sri Lanka's interests in the cyber and non-cyber domains. However, as the two domains are now deeply entrenched in each other, these delays will in turn affect Sri Lanka's prospects for attracting investments amidst an unsecured cybersecurity ecosystem.

South Asia remains one of the least integrated regions in the world in political, economic, and security cooperation. As the South Asian Association for Regional Cooperation (SAARC) remains deadlocked, the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) has gained currency in recent years. In an effort to rejuvenate cooperation through the BIMSTEC framework, the member nations adopted a long-overdue charter at the recently held fifth edition of the BISMTEC Summit in March this year.[12] The summit, hosted by Sri Lanka, formalized the structure and functioning of the grouping and reoriented the sectors to be led by the BIMSTEC members. With India focusing on the security pillar and Sri Lanka expected to lead the science, technology, and innovation in the new BIMSTEC framework, Colombo should formulate a strategy for improved engagement with New Delhi in the cyber domain.[13]

To solve its emerging cyber quandary, Colombo will not only have to fast-track the legislative processes in the coming years but will also need to find ways to develop education frameworks and infuse infrastructural upgrades. Invariably, strong regional cooperation will be a necessity. As Colombo battles with economic and political turbulences, Sri Lanka's cyberspace remains at more risk than ever before.

NOTES:

[1] Roshan Kishore. "Bad luck, policy mess, politics hit economy: Why the Sri Lankan economy tanked", *Hindustan Times,* July 13, 2022, https://www.hindustantimes.com/india-news/bad-luck-policy-mess-politics-hit-economy-why-the-sri-lankan-economy-tanked-101657723674798.html. Accessed on July 14, 2022

[2] N Sathiya Moorthy, "Guess, who is wooing Sri Lanka now?", *Observer Research Foundation,* February 11, 2020, https://www.orfonline.org/expert-speak/guess-who-is-wooing-sri-lanka-now-61282/. Accessed on July 14, 2022

[3] "Potential Internet Risks", *Ceylon Today,* June 27, 2022, https://www.orfonline.org/expert-speak/guess-who-is-wooing-sri-lanka-now-61282/. Accessed on July 14, 2022

[4] Ibid.

[5] "Sri Lankan Domain Attack: Exposed Credentials available in Dark Web for Eight Years!", *Cyber Security Works.* February 11, 2021, https://cybersecurityworks.com/blog/cyber-risk/sri-lankan-domain-attack-exposed-credentials-available-in-dark-web-for-eight-years.html. Accessed on July 14, 2022

[6] AP, "Sri Lankan Cabinet approves to draft two bills on cyber security laws", *Economic Times,* October 13, 2021, https://cio.economictimes.indiatimes.com/news/digital-security/sri-lankan-cabinet-approves-to-draft-two-bills-on-cyber-security-laws/86982753. Accessed on July 14, 2022

[7] Dimuthu Attanayake, "Anonymous wanted to help Sri Lankans. Their hacks put many in grave danger", *Rest of World,* May 10, 2022, https://restofworld.org/2022/anonymous-sri-lankans-hacks-danger/. Accessed on July 14, 2022

[8] "Sri Lankan Cabinet approves to draft two bills on cyber security laws", n. 6.

[9] "Potential Internet Risks", n. 5.

[10] Ibid.

[11] Naveed Rozais, "Sri Lanka's future lies in its cybersecurity", *The Morning,* August 8, 2021, https://www.themorning.lk/sri-lankas-future-lies-in-its-cybersecurity/. Accessed on July 14, 2022

[12] Diksha Munjal, "Explained | What is the BIMSTEC grouping and how is it significant?", *The Hindu,* April 6, 2022, https://www.thehindu.com/news/international/explained-what-is-the-bimstec-grouping-and-how-is-it-significant/article65275690.ece. Accessed on July 14, 2022

[13] Sripathi Narayan, "5th BIMSTEC Summit", *Indian Council of World Affairs,* April 22, 2022, https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=7277&lid=4914. Accessed on July 14, 2022