SPOTLIGHT
ON REGIONAL AFFAIRS

November 2022, Vol.40, No.11 (2)

Pakistan's Cyber Threat Landscape and Prospects of Regional Cooperation on Cyber Security

Irta Fatima*

Information and Communication Technologies (ICTs) are playing an important role in the economic growth of states. However, at the same time, ICTs pose a threat to the national security of states in the form of cyber-attacks and industrial espionage. States are finding it difficult to combat cyber threats and are investing heavily in cyber security. In the contemporary world, conventional forms of conflict are less likely to take place and as a result cyberspace has emerged as the fifth domain of warfare. When it comes to the cyber domain, Pakistan is considered one of the most vulnerable countries to cyber-attacks. This study highlights the cyber threats posed to Pakistan and the reasons that behind Islamabad's non-prioritisation of cyber security. It also discusses the prospects of regional cooperation when it comes to cyber security and the steps Pakistan may take in order to ensure regional cooperation.

Analysing Cyber-attacks on Pakistan since 2015

Pakistan is one of the most vulnerable countries to cyber-attacks. In this context, it comes as no surprise that Pakistan is dealing with cyber-attacks, which are rising with each passing year in banking, educational, and telecom sectors as well as other critical information infrastructures. Additionally, the most sensitive areas, i.e., military and government sectors are the prime targets of hackers.[1] It is important to note that Global Cyber Security Index (GCI) published a report in 2021 and placed Pakistan at 78 out of 193 countries vis-à-vis cyber security.[2] It is pertinent to highlight that most of the cyber-attacks are directed towards the financial sector of Pakistan. Starting from 2015, Pakistan faced an increased number of cyber-attacks. A cyber security firm Symantec revealed in its 2015 report that millions of unique and new malwares were found in the networks of Pakistan.[3] The report further added that the personal records of millions were stolen or lost. The report highlighted the vulnerability of Pakistan to espionage and data theft. In 2016, Indian hackers claimed that they hacked the Pakistani government's networks leading to the loss of crucial data whereas this attack also locked government systems resulting in a halt of government services.[4]

In 2017, Habib Bank Limited (HBL) faced one of the most serious cyber instances when the accounts of over 600 individuals were hacked and over Rs 10 million (around $45,500) were stolen.[5] In the same year, Indian hackers defaced over 500 Pakistani websites.[6] In November 2018, numerous cyber-attacks occurred in Pakistan and the financial sector was once again targeted. The data of more than 8,000 accounts from 10 banks was reportedly for sale on the dark web.[7] In December 2018, another cyber-attack occurred and this time the accounts of HBL and Bank Islamic Limited were the targets.[8] In 2019, India attempted to hack the digital devices of high-ranking officials of the Pakistani government and military using Israeli spyware Pegasus.[9] In 2020, the power sector was targeted by hackers with ransomware. On 7 September 2020, Pakistan's leading electricity provider, K-electric, faced a cyber-attack that not only affected the billing and online services of K-electric, but also caused the seizure of services for days.[10] The hackers demanded around half a million dollars in ransom from K-electric to end

* Ms Irta Fatima is an Intern at the Institute of Regional Studies, Islamabad. She holds an MPhil degree in Peace and Conflict Studies from the National Defense University, Islamabad.

the attack.[11] In 2021, one of Pakistan's most crucial institutions, the Federal Board of Revenue (FBR), faced a severe cyber-attack directed towards the data centres of FBR.[12] This cyber-attack caused massive disruption and brought down the website of the FBR for over three days. Along with that, it was reported that the data of taxpayers was not only stolen but tampered with and deleted as well.[13] Later in 2022, the FBR shut down its websites for twenty-four hours due to the imminent threat of cyber-attack.[14] Similarly, there have been attempts to deface institutional websites of Pakistan including the official websites of the Ministry of the Interior, the Ministry of Foreign Affairs (MOFA),[15] the District Courts of Gujranwala, the Faisalabad Police Department, and the Lahore High Court.[16]

Challenges in Prioritising Cyber Security in Pakistan

Pakistan is struggling to prioritise cyber security owing to multiple issues including budgetary constraints, lack of political will, and most importantly political instability. Although Islamabad has released a cyber security policy, non-existence of uniformed entities to implement the policy is a prime instance of this impression that Pakistan is not prioritising cyber security.[17] In Pakistan's context, the cyber infrastructure and human resources are not up to the mark to deal with increasing cyber threats.[18] Additionally, Pakistan sees most of the issues from the security perspective and in doing so every other threat including less relevant threats are considered a national security issue. Making every other threat a national security issue plays a role in diverting the focus of the state from other important issues and this is the case with cyber security. Moreover, cyber security is a new domain of research in Pakistan which is why scholars are not as inclined towards highlighting its importance. A combination of these issues is contributing to lesser focus on cyber security.

What Has Pakistan Achieved So Far in the Cyber Domain?

Pakistan released its National Cyber Security Policy in 2021. However, it has been a year since the release of NCSP and Islamabad has not taken any practical steps to strengthen its cyber security vis-à-vis cyber threats. There are, however, other cyber security initiatives that are important to be highlighted. In 2018, the Higher Education Commission (HEC) and the Planning Commission authorised the establishment of the National Centre for Cyber Security (NCCS). The primary objective of NCCS was to establish Research and Development (R&D) labs in order to secure Pakistan's cyberspace. Additionally, NCCS is responsible for making international linkages to adopt best practices in cyber security domain. Apart from this, the organisation is also responsible for conducting training programmes and workshops and introducing PhD programs in cyber security to produce reliable research for the government. There are two private Computer Emergency Response Teams (CERTs) operating in Pakistan namely Pak-CERT and Pakistan Information Security Association Computer Emergency Response Team (PISA CERT). These CERTs assist the public and private sector organisations in case of any cyber security incident. National CERT, if created, would be responsible for prevention of cyber incidents, offer quick and effective recovery, control and minimise any damage, preserve evidence, and analyse the cyber threats.[19]

Moreover, in 2016 Pakistan enacted the Prevention of Electronic Crimes Act (PECA), which recognised the internet as the foundation of modern communication and highlighted the importance of establishing a cyber security authority to strengthen the security of Pakistan's digital assets. The act envisions a national CERT as a legitimate incident-response entity. This vision has not yet materialised, though. In addition to these initiatives, the National Response Centre for Cyber Crime (NR3C) was

established by the Federal Investigation Agency (FIA) in 2007 to curb cybercrimes. It is important to note that NR3C is likely to create cyber patrolling units in order to monitor and counter threats associated with social media platforms.

Prospects of Regional Cooperation in the Cyber Domain

Cyber threats are transnational, and it is difficult for a country like Pakistan to counter threats associated with cyberspace without regional or international cooperation. Regional cooperation is the most viable option at present as Pakistan is already part of two regional initiatives like the South Asian Association for Regional Cooperation (SAARC) and the Shanghai Cooperation Organisation (SCO). Although there may not have been prominent developments in advanced technology or in cyber security domain with regard to SAARC since its inception,[20] SAARC can play a role in collective fight against cyber threats. SAARC countries can extend their cooperation in the domain of cyber security as all these member states are equally in need of protecting their digital assets. The SCO is another regional initiative that identifies various areas of cooperation including cyber security. The SCO recognises cyberspace as a significant area of collaboration and this is why two offices—the SCO Expert Group on International Information Security and the Cyber Expert Group—are attempting to extend cyber security collaboration among member states. All member states of the SCO can benefit from the best practices of some of the most cyber secure countries, i.e., China and Russia, as both are important members of the SCO. These platforms can also lay the ground for establishing confidence building measures (CBMs) in the cyber domain.

Conclusion

In a nutshell, the growth of ICTs has brought immense opportunities for developing states like Pakistan. However, this development has exposed countries to multiple threats emanating from cyberspace. Pakistan is also facing a number of cyber threats in the form of ransomware, website defacing, data theft, espionage, and more. Despite increasing cyber threats, Islamabad is not prioritising cyber security due a number of factors. Although Pakistan has released its first-ever NCSP, Islamabad has not taken serious measures to implement this policy.

The Way Forward

In order to achieve the goal of regional cooperation in the cyber domain, Pakistan needs to take certain actions at the national level so that Islamabad's sincerity is reflected on forums like SAARC and the SCO. Firstly, there is a need to establish a national CERT, and a centralised organisation focused on cyber security like the Cybersecurity and Infrastructure Security Agency (CISA) of the US. Secondly, Pakistan needs to update its cyber security regulations to reflect the current state of the cyber threat landscape. Thirdly, the HEC should issue guidelines to the universities to include cyber security as a subject in all the degrees related to ICTs. Finally, it is important that researchers and scholars highlight the importance of cyber security through academic discussions and publications. In brief, there are prospects of regional cooperation in the cyber domain through the already existing forums like SAARC and the SCO. However, it is important that Pakistan shows its commitment to securing its cyberspace by prioritising cyber security.

Notes and References

1 Rubab Syed, "Cyber Security: Where Does Pakistan Stand," *Sustainable Development Policy Institute* 167 (2019):6.

[2] Emma Woollacott, "Pakistan government approves new cybersecurity policy, cybercrime agency," *The Daily Swig,* 09 August 2021, available at https://portswigger.net/daily-swig/pakistan-government-approves-new-cybersecurity-policy-cybercrime-agency.

[3] Ammar Sheikh, "Cyber security: Inside Pakistan's first digital forensic research lab," *The Express Tribune*, 27 November 2016, available at https://tribune.com.pk/story/1246290/cyber-security-inside-pakistans-first-digital-forensic-research-lab.

[4] Shashank Shekhar, "Cyber-attack post-surgical strike: Indian techies hack into Pakistan government network," *India Today,* 09 October 2016, available at https://www.indiatoday.in/mail-today/story/indian-hackers-surgical-strike-pakistan-cyberspace-345349-2016-10-06.

[5] Zubair Ashraf, "In Pakistan, banking sector most vulnerable to cyber-attacks," *The News*, 18 December 2017, available at https://www.thenews.com.pk/print/257280-in-pakistan-banking-sector-most-vulnerable-to-cyber-attacks.

[6] Swarajya Staff, "Indian Hackers Take down over 500 Pakistani Websites in Response to Cyber Attacks against Universities," *Swarajya,* 26 April 2017, available at https://swarajyamag.com/insta/indian-hackers-take-down-over-500-pakistani-websites-in-response-to-cyber-attacks-against-universities.

[7] Rafay Baloch, "Dark web hackers allegedly found selling data from nearly all Pakistani banks", *Cyware Social* (2018): 1.

[8] Aamna Rafiq, "Increasing Cyber Threats to Pakistan," Institute *of Strategic Studies Islamabad* (2017): 2.

[9] Stephanie Kirchgaessner, "Israeli spyware allegedly used to target Pakistani officials' phones," *The Guardian,* 19 December 2019, available at https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones.

[10] Deeba Ahmed, "Pakistani power supplier K-Electric hit by NetWalker ransomware attack," *Hackread,* 09 September 2020 available at https://www.hackread.com/netwalker-ransomware-hits-pakistan-power-supplier-k-electric/#:~:text=Pakistan%E2%80%99s%20leading%20electricity%20provider%2C%20K-Electric%2C%20which%20is%20the,disrupted%20the%20billing%20and%20online%20services%20of%20K-Electric.

[11] Ibid.

[12] Shahbaz Rana, "FBR reels under a major 'cyber-attack," *Tribune,* 15 August 2021, available at https://tribune.com.pk/story/2315712/fbr-reels-under-a-major-cyberattack.

[13] Syed Talat Hussain, "What caused Pakistan's largest data centre attack," *Gulf News,* 24 August 2021, available at https://gulfnews.com/opinion/op-eds/what-caused-pakistans-largest-data-centre-attack-1.81758508.

[14] Shahbaz Rana, "FBR reels under a major 'cyber-attack," *Tribune,* 15 August 2021, available at https://tribune.com.pk/story/2315712/fbr-reels-under-a-major-cyberattack.

[15] Naveed Siddiqui, "Ministry of Foreign Affairs website hacked, inaccessible in several countries," *Dawn*, 16 February 2019, available at https://www.dawn.com/news/1464217.

[16] "Indian hackers deface LHC website," *Dawn*, 14 October 2014, available at https://www.dawn.com/news/1137929/indian-hackers-deface-lhc-website.

[17] Ahmed Minhas, "Pakistan's security challenges and political instability," *Tribune,* 14 November 2019, available at https://tribune.com.pk/story/2098987/pakistans-security-challenges-political-instability.

[18] Ibid.

[19] Syed, "Cyber Security", 9.

[20] Fizza Batool, "Why Dismissing SAARC's Revival is Premature," *South Asian Voice,* 15 April 2020, available at https://southasianvoices.org/why-dismissing-saarcs-revival-is-premature.