SPOTLIGHT
ON REGIONAL AFFAIRS

August 2022, Vol.40, No.8 (1)

Cyber Security Policing: Analysing National Cyber Security Policies of India and Pakistan

Ahmad Ali*

The Fourth Industrial Revolution (4IR) has blurred the lines between the physical and digital world, and cyberspace has emerged as the fifth domain of warfare. In this context, India released its first National Cyber Security Policy (NCSP) in 2013 which included several action points. Keeping in view the NCSP 2013, India has made crucial developments to secure its cyberspace. New Delhi has drafted an updated National Cyber Security Strategy that is set to be released after the approval of the Indian federal cabinet.[1] Relatedly, in July 2021, Pakistan released its first-ever and much-needed National Cyber Security Policy (NCSP) which provided a coordinated and organised approach to secure the digital assets of Pakistan. The NCSP is very comprehensive and appears perfect on paper, but it is yet to be seen if it is likely to be implemented effectively or not. This paper offers a thorough insight into the cyber security policies and cyber developments of India and Pakistan whereas it also points out the areas in which Pakistan lags behind. Additionally, it provides the way forward for Pakistan in order to secure its digital assets.

India's National Cyber Security Policy 2013

The 2013 NCSP of India highlighted several objectives in order to secure Indian cyberspace including strengthening regulatory framework, creating national and sectoral level mechanisms to gain information regarding cyber threats so that effective countermeasures can be ensured and operationalizing the National Critical Information Infrastructure Protection Centre (NCIIPC) to protect critical information infrastructure of India.[2] To address national security requirements, the NCSP also aimed to develop indigenous security technologies. Additionally, India aimed to create a workforce of 500,000 professionals skilled in cyber security by 2018 and establish an effective mechanism for the investigation and prosecution of crimes associated with cyberspace. Furthermore, the NCSP outlined the development of public-private partnerships, initiation of Research & Development (R&D) programs and promotion of global cooperation to ensure the security of Indian digital assets.

To achieve these objectives, the NCSP outlined several strategies including the establishment of a central agency at national level to oversee all the matters related to cyber security and to ensure that all the organisations designate a specific budget for the implementation of cyber security initiatives. To ensure the protection of digital assets, India aimed to adopt proactive measures and procure indigenously manufactured information and communication technology products. Another important strategy to reduce the vulnerability of digital assets, the NCSP aimed to operationalise Computer Emergency Response Teams (CERTs) at the national and sectoral levels and organize cyber security drills and exercises to test the security features in place and preparedness in case of any cyber incident.

Pakistan's National Cyber Security Policy 2021

The introductory section of the National Cyber Security Policy (NCSP) outlined Pakistan's cyber security landscape, course of action and challenges that are posed to Pakistan in cyberspace. These challenges include lack of ownership at national level, inadequate resources, lack of data governance, absence of indigenous information, and communication technology industry leading to dependency on external resources, the

[*] Ahmad Ali is an Intern at Cyber Security Programme, Institute of Regional Studies, Islamabad.

nonexistence of CERTs, lack of coordination among institutions, and weak enforcement.[3]

The vision of NCSP in this case was to have a secure, robust, and progressive digital ecosystem that guaranteed the availability of digital assets leading to socio-economic development and national security. The likely objectives to be achieved after implementation of NCSP were the establishment of governance and institutional framework to secure cyberspace, security of national information systems, protection of online privacy of citizens, enhancement of cyber security awareness, taking part in global cooperation and collaborations on cyber security and the development of public-private partnership. NCSP also sought to train skilled cyber security professionals, indigenise the cyber security industry through Research and Development (R&D) programs, make an appropriate legal framework for cyber governance, and adopt a risk-based approach.

NCSP highlighted that in case of a cyberattack, the Government of Pakistan will lead the response with the assistance of public and private entities keeping in view the international cyber security framework. Whereas such an attack on Critical Information Infrastructure (CII) would be regarded as an act of aggression against national sovereignty. To oversee cyberspace-related policies, the government has established Cyber Governance Policy Committee (CGPC), an organisation which is also responsible to formulate and recommend the approval of the Cyber Security Act. Apart from CGPC, the federal government was to designate a central entity that was to develop an institutional framework to implement NCSP and to oversee cybersecurity-related matters on national, sectoral, and organisational levels. The establishment of Computer Emergency Response Teams (CERTs) is also an important feature of NCSP.

Active defence is a defensive strategy and in the cyber security arena, it is referred to as asymmetric defence which increases the cost of cyberattacks for the adversary. To achieve the strategy of active defence, the government planned to restrict access to websites and domains that may be sources of malware, ensure security best practices through Internet governance organisations, collaborate with international law enforcement channels, and secure the routing of internet traffic for government departments.

Indian Developments in Cyber Domain

India took major steps toward securing its cyberspace under the directions outlined in NCSP 2013. Indian Computer Emergency Response Team (ICERT) formed in 2004, was designated as a nodal agency under the Ministry of Electronics and Information Technology (MeitY). ICERT works as an umbrella organisation for coordinated action against cyber threats and provides guidelines to public and private organisations to minimise the vulnerability to cyberattacks. India has also established sectoral CERTs to mitigate cyber threats. In this regard, four sectoral CERTs were formed in the power sector and India is in the process of forming a CERT for the financial sector.[4] ICERT has inked cyber security agreements with various countries including Singapore, Japan, and Malaysia.[5] Furthermore, India has signed Memorandum of Understanding (MoU) with Australia, Bangladesh, France, Indonesia, Qatar, the US, and UAE to cooperate in the cyber security domain.[6] India has also concluded agreements with Israel and Russia to strengthen cyber security capabilities. India is also part of the Quadrilateral Dialogue (Quad) and one of the key areas of cooperation in the Quad is cyber security.[7]

To protect Critical Information Infrastructure (CII), India operationalised National Critical Information Infrastructure Protection Centre (NCIIPC) in 2014. NCIIPC has identified six critical sectors that impact national security if cyberattacks take place in these sectors. These critical sectors include transport, government, power and energy, telecom, financial sector, and strategic enterprise.[8] NCIIPC is also responsible for issuing guidelines and perform advisory role to reduce vulnerability, undertake R&D and act promptly in case of any cyberattacks. Apart from this, in 2013 India gave the go ahead to establish an E-surveillance agency, National Cyber Coordination Centre (NCCC), with the responsibility to monitor internet traffic to prevent cyberattacks of domestic and international origin.[9] There are other initiatives such as the Cyber and Information Security (C&IS) Division that fall under the Indian Ministry of Home Affairs (MHA).

Achievements and Setbacks in Securing Pakistan's Cyberspace

Pakistan has adopted a number of cyber laws over the years whereas the Prevention of Electronic Crime Act (PECA) 2016 is considered as the most important and comprehensive cyber security law that includes a range of cyberspace issues including cyberterrorism and unauthorised access to critical infrastructure. Albeit, due to the limited institutional framework, PECA lacks a clear and comprehensive enforcement mechanism. Presently, two private CERTs are operating in Pakistan namely Pakistan Computer Emergency Response Team (PakCERT) and Pakistan Information Security Association Computer Emergency Response Team (PISA CERT).[10] On provincial level, KPK established a Cyber Emergency Response Centre. Also, Pakistan Telecommunication Authority (PTA) introduced a CERT portal for telecom sector and established the Cyber Vigilance Division that is responsible for capacity-building in industrial sector, controlling unauthorised IP addresses, and providing guidelines to counter cyber threats. Additionally, the Ministry of Information Technology and Telecommunication is in the process of forming CERTs on national and regional levels to counter cyberattacks adequately. Furthermore, National Response Centre for Cyber Crime (NR3C) of the FIA is likely to establish cyber patrolling units that would be focused on monitoring cyberspace platforms in Pakistan. The government has established National Center for Cyber Security (NCCS) to promote cyber security in the form of academic degrees as well. In 2014, Pakistan Computer Bureau (PCB) and Electronic Government Directorate (EGD) were merged to form the National Information Technology Board (NITB). However, the NITB is primarily focused to promote the E-governance in all public departments.

Despite the aforementioned initiatives, Pakistan has not been able to fully implement NCSP due to a number of reasons including budget constraints, political instability, and lack of political will. Although no timeline has been given in the policy document about its implementation, literature suggests that NCSP was to be implemented within first year of its release.[11] It has been stated in the policy document that federal government will form a central entity to implement the NCSP, however nothing has been specified in the document nor has the government confirmed anything about such entity even after a year of NCSP's release. In addition, there is no government organisation dedicated to solely deal with cyber security in Pakistan, and this is the primary hurdle in the implementation of NCSP. Threats in cyberspace are transnational and these can only be countered if a multilateral approach is followed. Many states including India, are following multilateralism to combat cyber threats by concluding international cyber security agreements whereas Pakistan is neither making any such agreements, nor has it engaged in any negotiations, as of late.

Way Forward for Pakistan

Where NCSP is Pakistan's first step towards securing cyberspace and is a very comprehensive policy, it lacks a proper implementation mechanism. It was to be implemented by June 2022 but most of the objectives have not been yet achieved. The foremost step that Pakistan should take is to establish an organisation under the Ministry of Information Technology and Telecommunication (MOITT) that oversees cyber security related issues and can act as a central organisation at the national level. It is important that such organization is only tasked to address cyber security related threats. Secondly, it is crucial for Pakistan to have a 'National CERT' that can respond to cyberattacks of domestic or international origin and provide guidelines to the public and private sectors to minimise the risk of cyberattacks. National CERT should directly come under MOITT and not under any subsidiary of MOITT so that there is minimum red tape. For the formation of national CERT, MOITT can collaborate with the already existing private CERTS namely PISA CERT and PakCERT.

Thirdly, after the formation of central organisation and National CERT, the central organisation should identify the Critical Information

Infrastructure (CII) of Pakistan so that sectoral CERTs can be formed to secure the identified CII sectors. These critical sectors may include power, financial, telecom, public and private enterprise, government, and other sectors of national importance. Fourthly, Cyber Governance Policy Committee (CGPC) should review Pakistan's developments in the cyber domain every year with regards to NCSP. Finally, Pakistan should take initiatives to conclude cyber security agreements with major countries including China and Russia. In 2017, Pakistan joined the Shanghai Cooperation Organisation (SCO) as a full member so Islamabad should consider cyber security cooperation with the member states, especially Iran as in 2009 the SCO member states signed an agreement on cyber security. Furthermore, the SCO has identified cyber security as an important area of cooperation, and this is the reason that two agencies namely the SCO Expert Group on International Information Security and the Cyber Expert Group are working to deepen cyber security cooperation among member states. Additionally, Pakistan should also sign bilateral cyber security agreements with the SCO member states.

Notes and References

[1] "India in final stages of clearing national cybersecurity strategy," *Business Standard*, 27 October 2021, https://www.business-standard.com/article/current-affairs/india-in-final-stages-of-clearing-national-cybersecurity-strategy-121102700663_1.html.

[2] Ministry of Electronics and Information Technology, *National Cyber Security Policy 2013*, (New Delhi: 2013), https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.

[3] Ministry of Information Technology & Telecommunication, *National Cyber Security Policy 2021*, (Islamabad: July 2021), https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Consultation%20Draft(1).pdf.

[4] Ministry of Power, Four Sectoral Computer Emergency Response Teams to mitigate Cyber Security Threats in Power Systems (New Delhi: 2017), https://pib.gov.in/newsite/PrintRelease.aspx?relid=159537.

[5] "Indian cybersecurity agency CERT-In signs pacts with 3 countries," *The Times of India*, January 27, 2016, https://timesofindia.indiatimes.com/tech-news/indian-cybersecurity-agency-cert-in-signs-pacts-with-3-countries/articleshow/50743169.cms.

[6] Leilah Elmokadem and Saumyaa Naidu, "Mapping of India's Cyber Security-Related Bilateral Agreements," *The Centre for internet Society,* 29 December 2016, https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016.

[7] Sarosh Bana, "Quad Prioritises Cybersecurity in the Indo-Pacific," *Asia Pacific Security Magazine,* 2 June 2022, https://www.asiapacificsecuritymagazine.com/quad-prioritises-cybersecurity-in-the-indo-pacific/#:~:text=The%20Quad%20Cybersecurity%20Partnership%20seeks,cybersecurity%20vulnerabilities%20and%20cyber%20threats.

[8] Maj Gen PK Mallick, "Cyber Security in India: Present Status," *Vivekananda International Foundation*, October 2017, https://www.vifindia.org/sites/default/files/cyber-security-in-india-present-status.pdf.

[9] Saikat Datta, "Cyber protection body pushes ahead," *Hindustan Times*, 20 January 2014, https://web.archive.org/web/20140119201552/http://www.hindustantimes.com/india-news/cyber-protection-body-pushes-ahead/article1-1174753.aspx.

[10] Muhammad Riaz Shad, "Does Pakistan's First Cybersecurity Policy Go Far Enough?," *The National Interest*, 10 June 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/does-pakistan%E2%80%99s-first-cybersecurity.

[11] Aamna Rafiq, "The National Cyber Security Policy of Pakistan 2021," *Institute of Strategic Studies Islamabad (ISSI)*, 15 October 2021, https://issi.org.pk/issue-brief-on-the-national-cyber-security-policy-of-pakistan-2021/.