Appraisal of Pakistan’s approach towards cyber security: Case for CERTs, Cyber Security Agency and Cyber Command

Usama Nizamani

August, 2021

POLICY BRIEF

IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

Appraisal of Pakistan's approach towards cyber security: Case for CERTs, Cyber Security Agency and Cyber Command

By: Usama Nizamani[*]

Executive Summary

Cybersecurity for imminent reasons has gained considerable attention in Pakistan's national security ecosystem. The discourse, however, has translated into limited visible progress to bridge critical cybersecurity vulnerabilities. The government has also announced National Cyber Security Policy 2021. A previous study from IPRI, with extensive qualitative and quantitative primary input, has identified absence of strategic initiatives such as: legislative, policy, strategy, executive, institutional and international arrangement to overcome this discrepancy in the cyber-security domain. Some of the measures highlighted in the study and deliberated with relevant ministries are being catered for. However, action in some other areas still stands absent.

Apart from this critical element, this particular policy brief emphasizes the need for setting of a cyber-command under the auspices of Joint Services Headquarters (JSHQ). This requisite institutional set up will enable Pakistan's armed forces to have an all-purpose, joint set up to ensure resilience and defence of Pakistan's critical military infrastructure, command, control, computers, and communication network. Simultaneously, offensive cyber-capabilities are requisite at a time when gray-zone conflict is gaining traction by various state and non-state actors: especially those emanating from within the region. This normative measure will ensure appropriate resilience and retaliation options in the cyber domain. The paper concludes with actionable recommendations for policy makers to forge a comprehensive approach towards cyber-security preparedness of Pakistan.

Analysis

A major challenge before is absence of a cybersecurity framework. In absence of such arrangement, the overall policy actions are likely to remain rudderless, ineffective, and haphazard at best. At worst, it may result in duplication of efforts compromising principle of economies of effort: with fear of disjointed efforts being.

Preventing such an eventuality should remain utmost priority: given a wider prevalence of turf wars across institutions. Not only such an approach costs finite resources, it takes a toll on scale and quality of output. This section will a brief stock of the nature of reported cyber threats in Pakistan's cybersecurity landscape, in addition it also underscores the need for the development of CERT and Cyber Command.

Cybersecurity Landscape of Pakistan

In 2017, the notorious WannaCry ransomware infected 200,000 computers and spread to over 100 countries and it severely crippled United Kingdom's National Health Service for a week

[*] The author is an Assistant Research Associate at IPRI. Views expressed herein are personal and not reflect of institute's policy.

from 12-17 May 2017.[1] As per the report *Evil Internet Minute* released by RiskIQ, cybercriminals will cost the global economy US$11.4 million each minute[2], which will make up for a daily loss of nearly US$ 16 billion, annually costing the global economy US$ 5.8 trillion.

Pakistan too has been affected by some high-impact breaches of cybersecurity. In 2019, it was reported that cell phones of senior Pakistani officials were breached for covert surveillance. The attempted breach was reportedly undertaken through malware via WhatsApp called "Pegasus" allegedly developed by Israeli spyware firm NSO Group.[3] There are concerns that possible role of Indian intelligence agencies may not be ruled out.[4] Recently, Indian intelligence agencies are reported to have used NSO's spyware products to spy on Indian human rights activists, journalists, lawyers and members of opposition.[5] On September 7, 2020, K-Electric (KE) was also targeted ransomware attack by a malicious online entity called Netwalker gang.[6] The attack on KE jeopardized its billing and online services. Netwalker demanded KE to pay a ransom of $ 7 million. The group, eventually, leaked 8.5 Gigabytes of stolen data on the dark web.[7] KE is reported to have access to data such as "customers' names, addresses, CNICs, National Tax Numbers (NTNs), credit cards, debit cards, and bank account details."[8]

Similarly, cybersecurity breaches at one part of the world are likely to affect digital devices and ecosystems in other parts of the world, due to the inter-connected nature of the internet. In 2017, the notorious ransomware attacks WannaCry, spread to over 150 countries and impacted nearly 10,000 countries all over the world. The attack commenced on May 12, 2017, when it first affected England's National Health Service, after spreading to systems in other parts of the world.[9] This wide spread nature of cyber-threats, therefore, calls for adoption of proactive threat intelligence mechanisms in Pakistan. Furthermore, going forward FATF also stipulated Pakistan to adopt financial technologies for transfer of cash.[10] Adoption

[1] K. L. Offner et al., "Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation," *Intelligence and National Security* 35, no. 4 (2020):556-585.

[2] RiskIQ, accessed November 4, 2020, https://www.riskiq.com/wp-content/uploads/2020/08/Evil-Internet-Minute-RiskIQ-Infographic-2020.pdf.

[3] Stephanie Kirchgaessner, "Israeli Spyware Allegedly Used to Target Pakistani Officials' Phones," *The Guardian*, last modified December 19, 2019, https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones.

[4] "The Cyber Threat Facing Pakistan," *The Diplomat* – last modified June 6, 2020, https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/.

[5] "Spyware Maker NSO Promises Reform but Keeps Snooping," The New York Times - Breaking News, US News, World News and Videos, last modified November 9, 2019, https://www.nytimes.com/2019/11/09/technology/nso-group-spyware-india.html.

[6] Syeda Masooma, "8.5 GBs of K-Electric Data Dumped Online After It Failed to Pay $7 Million in Ransom," *ProPakistani* | Technology and Business News from Pakistan, last modified September 30, 2020, https://propakistani.pk/2020/09/30/8-5-gbs-of-k-electric-data-dumped-online-after-it-failed-to-pay-7-million-in-ransom/.

[7] Masooma, "K-Electric Data Dumped"

[8] Ibid.

[9] Andrew Liptak, "The WannaCry Ransomware Attack Has Spread to 150 Countries," *The Verge*, last modified May 14, 2017, https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries.

[10] Umar Farooq, "Pakistan Government Announces New Instant Digital Payment System," U.S, last modified January 11, 2021, https://www.reuters.com/article/pakistan-economy/pakistan-government-announces-new-instant-digital-payment-system-idUKL4N2JM349.

of such methods of financial transactions and broader moves towards financial inclusion will also create vulnerabilities from malicious actors in the cyber-domain. In the Global Cyber Security Index – 2018, Pakistan is ranked at 94th position globally.[11] Given these set of circumstances, Pakistan appears highly impeded to provide cyber-secure environment for corporations, Critical Information Infrastructure (CIIs), government agencies, and national institutes.

CERT and Cyber Command: The Difference and the Complementing Factor

The establishment of Cyber Emergency Response Team (CERT) and Cyber Command are both critical for Pakistan's national security. The primary roles of the two are entirely different: the CERT is responsible in providing a round the clock situational awareness of the national and international cyber landscape; whereas, the cyber command demands military institutional capability to undertake defensive and offensive cyber interventions against enemy assets. The CERT, under National Cyber Security Agency, shall be responsible for ensuring situational awareness of CNII and to improve its cyber security and resilience measures. The cyber command, on one hand, albeit limitedly, works closely with improving the defensive or resilient measures of the CERT, on the other end, it works towards meeting the offensive cyber interventions against enemy targets for fulfillment of national security objectives in the cyber domain. At present, cyber security apparatus under armed forces work directly under their respective arm. An overarching combined effort, in interest of reducing the cost of economies, still remains missing. Cyber command under a joint arms command is critical lynchpin towards overcoming this deficit.

Cyber command under Joint Staff Headquarters will enable military to have an overarching cyber capability towards improving joint operations: both in peace times and crises. The command will attract diverse pool of resources from combined arms. Optimal use of talent, operational planning and cyber preparedness for respective arm of the armed forces may be enabled as a result of this strategic initiative. The establishment of cyber command has also become indispensable after India's plans and decision to set one up under the Integrated Defence Staff.

On the other hand, apart from the development of the CERT, Pakistan also needs an array of measures to fill the void: National Cyber Security Strategy, and Master Plan; National Cyber Security Agency; National Cyber Security Act; and a separate regime on Data Privacy and Protection.

Recommendations

- Establishment of Cyber Command, under the Joint Services Headquarters, in order to improve armed forces capability to have a combined and joint situational awareness. The capability will also enable design and execution of defensive and offensive cyber posture, where necessitated. The establishment of Cyber Command will significantly complement independent measures, already in place, under respective arms of the armed forces.

- Composition of National Cyber Security Strategy (2021-2025), needs to be drafted along the lines of National Cyber Security Strategy of Canada or Singapore. In order to meet this strategy, Pakistan requires a Master plan for accomplishment of the National Cyber

[11] International Telecommunication Union, *Global Cyber Security Index - 2018*, (Information Telecommunication Union, 2018), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Security Strategy. Similarly, the time bound accomplishment of the National Cyber Security Policy verticals requires these two instruments for clarity of roadmap.

- The National Cyber Security Agency (NACSA) to have a National Cyber Security Council assigned as an advisory body, for advising NACSA on composition of the National Cyber Security Strategy and Master Plan and for composition of cyber-security health scorecard. The NACSA will be responsible for ensuring compliance of the strategy and master plan from public and private sector. However, regulatory bodies, such as PTA, State Bank, etc., will be mandated under Cyber Security Act, to work in close coordination with NACSA to ensure compliance of the strategy and master plan verticals from respective public and private entities falling under their domain. Overall compliance with strategy and master plan remains the responsibility of NACSA.

- Establishment of the national CERT as Pak-CERT for CIIP from incidents of cyber-attacks. The national CERT will report to NACSA and, hence, all sector specific CERTs belonging to CIIP, such as, banking, education, hospital, energy and power, information, telecommunication communication, transportation (air, sea, and land), food and agriculture sector and national institutes of strategic importance will be connected and integrated with Pak-CERT.

- Existing National Centre for Cyber Security to be set up as a premier Research and Development body on cyber-security related programs and products, including funding development of products for indigenous use and software exports. Products designed by NCCS to be in compliance with future data regulation procedures of Pakistan and international regulations such as General Data Protection Regulation (GDPR) of the EU.

ABOUT THE AUTHOR

Usama Nizamani

Mr. Usama Nizamani joined IPRI as a Consultant in 2017, and later as an Assistant Research Associate, bringing along his professional experience of behavior sciences, after having conducted national and international training sessions as a Psycho-Social Trainer (2015-2017) with IREX and Bytes for All, Pakistan. At IPRI, he has developed extensive experience on emerging technologies, application of Artificial Intelligence and cyberspace and maps their impact on future strategic landscape. He also augments his academic and professional experience of behavioral sciences in studying strategic decision making. On strategic affairs, he focuses on Pakistan-India, India-China, US-China engagement in South Asia and Asia Pacific. Mr. Nizamani has published rigorous research based policy papers on technology and policy related issues. He has featured as a speaker, discussant and panelist in various national and international conferences/webinars. He regularly contributes in national and international dailies. Mr. Nizamani has also participated as a delegate of Track-II dialogues. Mr. Nizamani is a graduate of National Defence University (NDU), Islamabad where his post-graduate research specialized on “Emerging Shifts in India’s Nuclear Strategy: From No First Use to First Use?” He also holds a BS in Psychology from Virtual University of Pakistan, Lahore.

He can be reached at: usama.nizamani@ipripak.org