Building National Cyber Security Institutional Framework and Cyber Emergency Response Team (CERT) Systems

Usama Nizamani

Feb 2021

POLICY BRIEF

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

Executive Summary

Cyber-security is one of the Achilles heels of Pakistan's security since there is an absence of policy and strategy both. A legislative, executive, institutional and international arrangement to overcome this discrepancy in the cyber-security domain is also missing. Similarly, an outright absence of national CERT and sector-specific CERTs, due to inability to handle threats of cyber incidents, is aggravating Pakistan's cybersecurity landscape. The existing state of affairs requires holistic set of intervention, to address anomalies, and strengthen cyber-security ecosystem in Pakistan.

- The government, through parliament, should adopt legislation, such as, National Cyber security Act to constitute development of National Cyber Security Agency (NACSA). Whereas, National Cyber Security Council, under this provision, to serve as an advisory or governing body over NACSA.
- Establishment of National-CERT and adoption of a National Cyber Security Policy, National Cyber Security Strategy (2021-2025) and a Master-Plan to accomplish objectives under the national strategy.

More specific recommendations to this can be found at the end of the document.

Issues to be analyzed

This research study investigated different factors that require building up of a national cyber security framework; and whether, is the establishment of National CERT critical for improving national cyber-security preparedness and response-mitigation. Some of the notable questions included:

- What is the existing nature of cybersecurity landscape involving Pakistan's corporate sector? Is the existing set of organizational practices coupled with government's measures enough to ensure resilient cyber-security preparedness?
- What are some of the practices adopted by other countries for their cybersecurity preparedness, and whether there are existing gaps in Pakistan's national cybersecurity framework?
- How Pakistan can adopt, multi-pronged measures to improve its cybersecurity framework and preparedness against cybersecurity vulnerabilities, at the national level?

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 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.

[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.

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 intel agencies are reported to have used NSO's spyware products to spy on Indian human rights activists, journalists, lawyers and members of the 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 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.

[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.

[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.

To overcome this anomaly, the situation calls for immediate and holistic set of interventions so that legislative; executive; and policy and national strategy imperatives could be more effectively addressed.

Prior to discussing critical policy interventions for Pakistan, it is vital to discuss some of the findings inferred from the cyber-security survey conducted by IPRI.

Survey Discussion and Findings

A total of 21 respondents comprising Chief Information Security Officers and Chief Information Officers were consulted for this study. 42.9 per cent of the respondents belonged to the banking sector. One respondent each belonged to energy, textile, education, manufacturing Fast Moving Consumer Goods, retail sector, and Artificial Intelligence related business. The overall proportion of such respondents was 28.8 per cent. Whereas, remaining 28.5 per cent of the respondents were from, i.e. 2 each, from healthcare sector, telecom sector and Pakistan stock exchange. The survey had a total of 27 questions: 25 of which were closed-ended, and 2 were semi-structured questions.

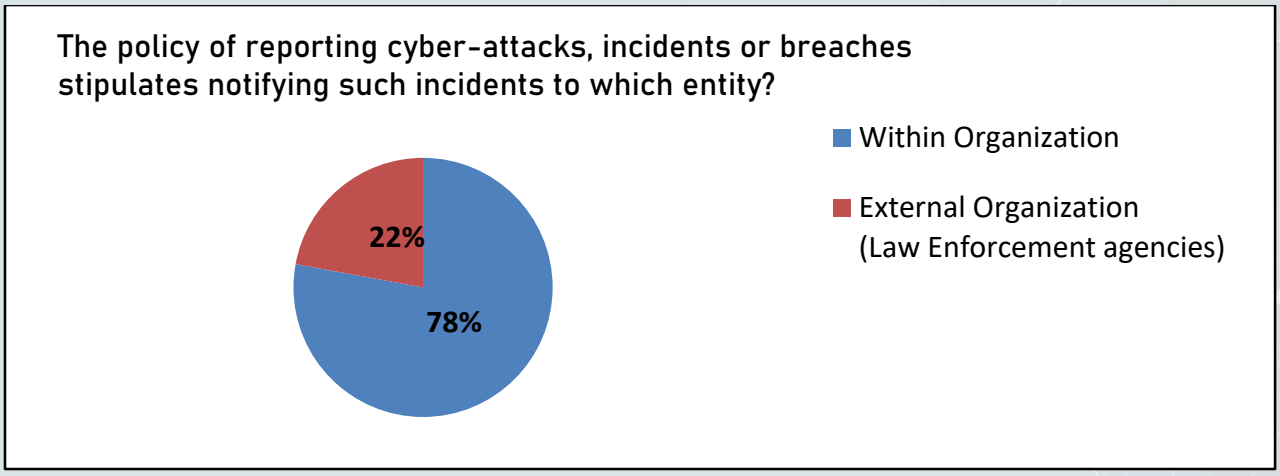
Risk Assessment

Identify all the malicious activities in the digital domain that your organization was affected by? Plea select all the options that apply.	
Ransomware attacks and Denial of Services attacks	33 %
Spyware attacks	28.6 %
Phishing Scams	76.2 %
Crypto-jacking attacks	14.3 %

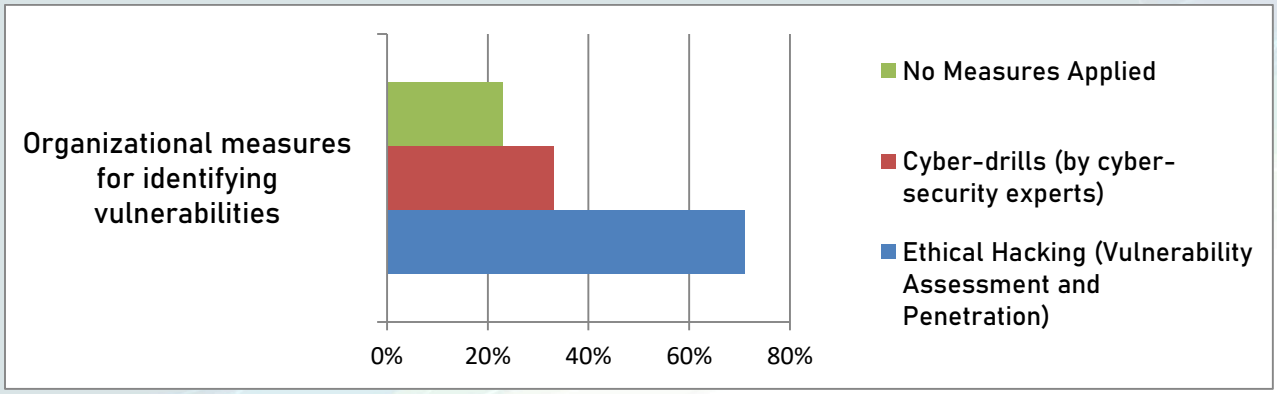
Our data illustrates that a possible relationship exists between attempts to social engineer through phishing scams, spyware attacks, which may also lead to high-impact attacks: such as, cyber-espionage, cyber-terrorism and unavailability of infrastructure through Advanced Persistent Attack (APA). A large number of organizations have measures in place to improve digital security practices of their staff such as, organizational SOPs on data protection, password protection, phishing scams, and data back up and capacity building programs such as in-house trainings. About 85.7 per cent organizations were using local servers to store (organizational and personnel) data, whereas 81 per cent of all such respondents used in-house servers. About 71.4 per cent of organizations were storing data on private cloud service. This illustrates, that in-house servers, for storage of large data, may experience growing incidents of breaches from malicious actors.

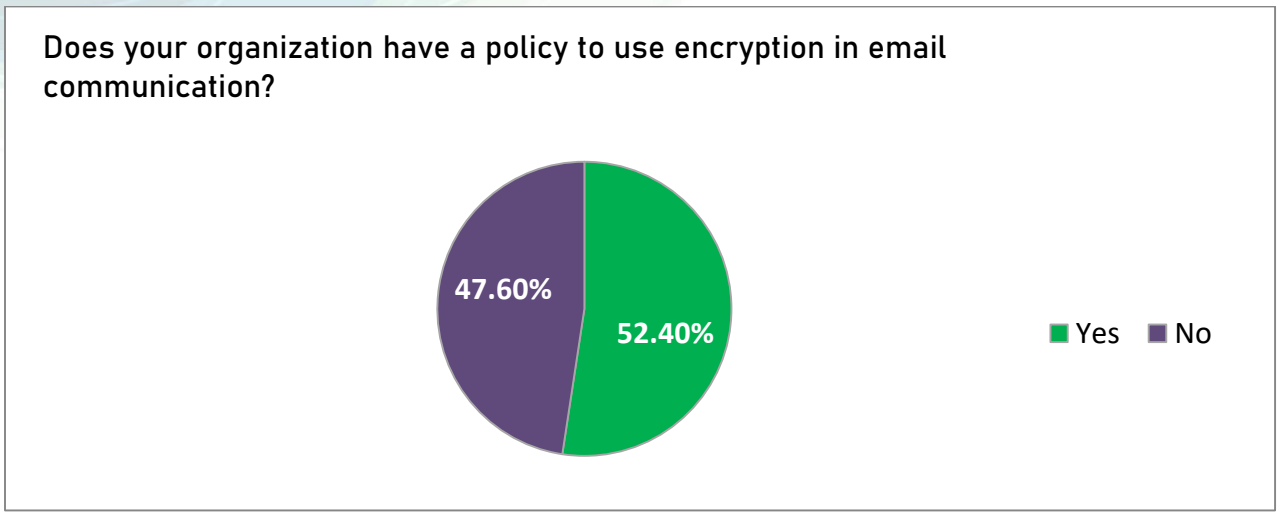
Counter Measures

Almost 81 per cent of the organizations had a mechanism to report incidents of cyber-security. However, only 22 per cent reported these breaches to law enforcement authorities.



Cumulatively, as per this study, about 57 and 49 per cent of organizations remain susceptible to data breaches of sensitive organizational data and client data, respectively, due to unsafe practices of data handling.





Future Policy Interventions

An overwhelming 90.5 per cent of the respondents agreed to setting up of sector-specific CERTs for healthcare, bank, telecom, energy and power, transportation, water, etc. Similar proportion supported future government-led mechanism to engage and build capacity of private sector and enforce compliance measures for improving organizational cybersecurity policy and practices. Similarly, 90.5 per cent of respondents agreed that government should undertake extensive and comprehensive consultation for setting up industry/sector-specific CERTs. 76.2 per cent support linking up National Cyber Emergency Response Team with sector-specific CERTs. Whereas, a complete consensus existed that sector-specific CERTs will enable organizations across sector to adopt improved cybersecurity practices for organizations. On adoption of holistic government led initiatives on cyber-security, 76.2 per cent supported the constitution of a dedicated National Cyber Security Agency to coordinate between private and public sector organizations falling under the Critical Information Infrastructure (CII). Whereas, 52.4 per cent supported adoption of legislation to strengthen cyber-security regime, and 90.5 per cent supported building up of research and development, expertise and capacity initiatives at academic and industry level in Pakistan.

Taking Cues from Other Countries

Based on case-studies of Canada, Singapore, Malaysia and Croatia, which were, consulted for this study, institutional arrangements, operational mechanism for handling cyber incidents, legislative, policy and strategy documents are mapped in the table below. This illustrates a holistic approach by these states to improve their cybersecurity landscape.

Table 1: Comprehensive Framework adopted by Canada, Singapore, Malaysia and Croatia

Country	CERT	National Institute	Legislation	Policy/Strategy/Master Plan
Canada	OpenCERT	Canadian Center for Cyber Security (C3S) Federal Steering Committee on Cyber Security	(a) Personal Information Protection and Electronic Documents Act 2000, (b) Data Privacy Act 2015	(a) National Cyber Security Strategy (b) National Cyber Security Strategy (c) National Cyber Security Action Plan 2019-2024
Singapore	SingCERT	Cyber Security Agency of Singapore (CSA)	(a) Cyber Security Act 2018 (b) Computer's Misuse Act	(a) Singapore Cyber Security Strategy (b) National Cyber Security Master plan 2020 (c) Singapore's Operational Technology Cybersecurity Plan 2019

Malaysia	MyCERT	National Cyber Security Agency (NACSA) Cyber Security Malaysia (R&D and Programme development body) National Security Council	(a) Personal Data Protection Act 2010 (Act 709) (b) Digital Signature Act 1997 (Act 562)	(a) National Cyber Security Policy (b) Malaysia Cyber Security Strategy (2020-24)
Croatia	National CERT ZSIS CERT	National Cyber Security Council National Operational and Technical Cyber Security Coordination Group Information Systems Security Bureau (ISSB)	(a) Critical Infrastructure Act[12] (b) Law on Information Security 2007. (c) Law on Protection of Personal Data 2003. (d) Law on the Security and Intelligence System 2006. (e) Ordinance on protection safety and integrity of networks and services 2012. (f) Regulation on Information Security Measures 2008.	National Cyber Security Strategy and the Action Plan

Pakistan and Learning from Best Practices

In 2016, parliament legislated Prevention of Electronic Crimes Act 2016; the legislation broadly bridged the need for penalizing cybercrimes. However, section 49 of PECA 2016, only caters for cyber-security readiness by mandating setting up of Computer Emergency Response Teams to handle incidents of cyber threats and attacks. This too, appears as an ad-hoc arrangement, without proper delineation of roles, responsibilities and compliance measures for public and private sector. The National Center for Cyber Crime (NR3C) under the Federal Investigation Agency (FIA) caters for investigation and prosecution of cybercrimes: including, breaches of the Critical Infrastructure. One of

[12] Magicmarinac.hr, "Zakon O Kritičnim Infrastrukturama," Zakon.hr, accessed November 4, 2020, https://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama.

the critical components of improving cyber security is having a dedicated national CERT and sector specific CERTs. At heart of a CERT is Cyber-Threat monitoring and Intelligence.

Of the case-studies consulted for policy brief: Canada[13], Croatia[14], Malaysia[15] and Singapore[16], all the countries provide an illustrative way forward in adopting a resilient cyber-security eco-system. The reported countries have a dedicated executive institute, such as, National Cyber Security Agency, Information and Systems Security Bureau or National Center in place (Please refer to the Table 1). It was also found, during this study, that the reported countries have national and sector specific CERTs in place for handling cyber-attacks and incidents.[17] [18] [19] [20] These countries also have specific legislation focusing on two primarily critical areas: cyber-security and data protection; and cybercrime legislation to complement cybersecurity regime.

In terms of reporting mechanism, national agencies on cyber security of Canada, Malaysia and Singapore report to respective Prime Minister's office.[21] Malaysia's NACSA reports through National Security Council and Canada's C3S reports to Prime Minister through a Federal Steering Committee, whereas in Singapore, CSA, it reports directly to Prime Minister's office. In Croatia, Information Systems Security Bureau, reports to the National Security Council, and the latter reports to the President.[22] As policy measures, these countries also have comprehensive policy and national strategy in place to achieve cyber security verticals, improve compliance, and an enforceable monitoring and evaluation mechanism (See Table 1).

Points for Consideration

It's important to consider some critical aspects before discussing policy recommendations for the relevant stakeholders:

- Pakistan's National Security Division can play a critical role in undertaking liaison with different civil (public and private) institutes. The National Cyber Security Agency may be placed under the office of the National Security Division.[23] This arrangement, however, should be arbitrary in nature for a period of one-year and may be extended to the satisfaction of government of Pakistan. The NACSA, after mainstreaming of its functions may be converted into an autonomous institute. A serving senior officer, equivalent to the rank of Lt. General of Pakistan Army/Armed Forces, in

[13] Canada, globally, is ranked at 9th position in the Global Cyber Security Index, 2018. Regionally, in Americas, it is ranked at 2nd position.
[14] Croatia, globally, is ranked at 24th position in the Global Cyber Security Index, 2018. Regionally, in Europe, it is ranked at 14th position.
[15] Malaysia, globally, is ranked at 8th position in the Global Cyber Security Index, 2018. Regionally, in Americas, it is ranked at 2nd position.
[16] Singapore, globally, is ranked at 6th position in the Global Cyber Security Index, 2018. Regionally, in Asia-Pacific, it is ranked at 1st position
[17] Leonard Ong/Information Systems Audit Control Association, Zoom Interview, Islamabad, October 7, 2020
[18] Zahri Yunis/CybserSecurity Malaysia, Email Interview, October 10, 2020.
[19] Khawaja M. Ali/Agriculture Development Bank of Pakistan, Zoom, Islamabad, October 3, 2020.
[20] Farooq Naiyer/Ontario Research Innovation Optical Network (ORION), Zoom Interview, October 8, 2020.
[21] Ong/ISACA
[22] Darko Galinec, Darko Možnik, and Boris Guberina, "Cybersecurity and cyber defence: national level strategic approach," Automatika 58, no. 3 (2017):273-286.
[23] Khawaja M. Ali.

ex-officio capacity, may be appointed as Chief of NACSA, while a senior cyber-security expert may be appointed as Deputy Chief of the national institute. CERTs and establishment of NACSA can serve as critical linchpins of cyber-diplomacy, as the CERTs, of other countries, help in communication of real-time threats to national CERT, which can help in proactive handling of cyber security risks and threats.

- The Chief Information Security Officers of organizations and installations falling under the Critical Information Infrastructure Protection (CIIP) be declared as Critical Information Operators mandating close liaison, under Cyber Security Act, with NACSA and Pak-CERT. This practice is, also, prevalent in Singapore.
- Data breaches need to be made mandatory under the future Data Protection legislation. In the absence of any such mechanism, it was evident from this research, that 22 per cent organizations have only reported incidents to external entities such as law enforcement or regulatory bodies. Breach of (customer or other critical) data, beyond a certain number of consumer, must entail a deduction of a 10 per cent of annual revenue.
- The government may also offer financial assistance to companies in the private sector, which may not have the resources at disposal to improve their cybersecurity. This may be done by several measures, such as, subsidizing 30-40 per cent of the cost of improving cyber security capacity of small and medium sized enterprises.[24]
- Establishment of NACSA in Pakistan will need to perform certification of medium and small sized businesses; awareness on cyber-security at a massive level; CERT, under NACSA, to provide free-of-cost alerts, notifications, to all stakeholders; fourth is development of competency matrix (framework of what elements of competencies at private and public level are needed).
- Each province must also be mandated to have a Chief Information Security Officer, as provincial governments will also bring up their security competency up to national cyber security standards. The CISO will be an employee of the provincial government, with the status of a deputy provincial minister, and also report to provincial government, however, in terms of meeting compliances and other critical requirements related to cyber-security will receive directions from the Chief of NACSA.

Recommendations

Pakistan, therefore, needs a similar holistic intervention to create a resilient cyber security ecosystem:

- Pakistan will need to come up with a comprehensive legislation, such as the National Cyber Security Act, at the earliest. The bill should delineate roles, responsibilities and tasks of bodies, institutes, private and public sector, including identification of Critical CIIP. Keeping in line with it, a 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 can develop a Master plan for the accomplishment of a National Cyber Security Strategy.
- The National Cyber Security Agency (NACSA), to have a National Cyber Security Council (Refer Annex-A), could be assigned as an advisory body, for advising NACSA on the 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

[24] As per Leonard Ong, Singapore offers a subsidy of about 50-70 per cent to build capacity of organizations, in case they have a shortfall of resource to improve their capacity.

plan from public and private sector.[25] 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 the responsibility of NACSA.

- Establishment of the national CERT, as Pak-CERT for CIIP from incidents of cyber-attacks is recommended. 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 and telecommunication, transportation (air, sea, and land), food and agriculture sector and national institutes of strategic importance will be connected and integrated with Pak-CERT.[26]
- 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.
- Pakistan needs to expedite the legislation on Data Protection, only after exhausting consultative process, to account for broader reservations of industry, civil society and academia. Since, legislation on Data Protection is critical for the accomplishment of having robust legislative mechanism on cyber related aspects. It will also help delineate matters related to data protection, privacy and cyber-security.

[25] Ibid.
[26] Khawaja Muhammad Ali