ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

THE NATIONAL CYBER SECURITY POLICY OF PAKISTAN 2021

By
Aamna Rafiq
Research Associate
Arms Control & Disarmament Centre, ISSI

Edited by
Malik Qasim Mustafa

October 15, 2021

(Views expressed in the brief are those of the author, and do not represent those of ISSI)

Recently, Pakistan got its first-ever and much-needed National Cyber Security Policy[1] (NCSP). The federal government is raring to kick off its implementation by the end of June next year.[2] Like any other policy in Pakistan, the NCSP 2021 appears almost perfect on paper. However, without timely and effective implementation, the NCSP 2021 will not achieve the desired results.

Public policy is defined as "a purposive course of action taken or adopted by those in power in pursuit of certain goals or objectives."[3] According to Thomas Dye and Robert Lineberry, a public policy is "whatever government choose to do or not to do." These definitions of public policy hint at the divergences that exist among what governments decide to do, what governments actually do, and what governments failed to do.[4] In order to identify these divergences, a well-known analytical model was proposed in 1997 in the field of policy studies. This model involves analysis of any public

1 Government of Pakistan, 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%20Final.pdf

2 "All set to implement 'Cyber Security Policy' by next year," *Business Recorder*, last modified September 17, 2021, https://www.brecorder.com/news/40120703/all-set-to-implement-cyber-security-policy-by-next-year

3 R K Sapru, *Public Policy: Formulation, Implementation and Evaluation* (New Delhi: Sterling Publishers, 2004), 4-6.

4 Ibid.

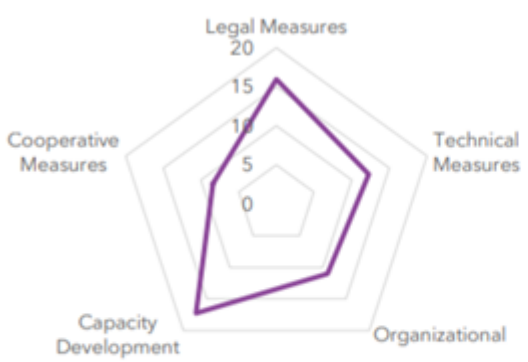
© ISSI 2021 • All Rights Reserved

policy from three major aspects: context, text and consequences.[5] The same model is being used here to analyse the NCSP 2021.

Policy Context

The policy is generally designated as the outcome of a specific political system. Various issues, pressures, interests and forces within that political system pave the way for policymaking. The main driving force behind the NCSP is the "Digital Pakistan Initiative" of the government. The initiative started in 2018 with the objective to promote connectivity, increase investment in digital skills, improve digital infrastructure, innovation and tech entrepreneurship in Pakistan. Currently, Pakistan's ranking and posture vis-à-vis cybersecurity is not very impressive. According to the ITU Global Cybersecurity Index (GCI), 2020[6] Pakistan ranked 76 among 182 countries. With an overall score of 64.88/100, Pakistan got placement at the level of a developing country. Pakistan got the highest score of 17.25/20 in the category of capacity development. It got scores of 15.97/20 and 12.26/20 in the categories of legal measures and technical measures respectively. However, Pakistan's performance in the categories of organisational measures and cooperative measures is unsatisfactory with the score of 11.01/20 and 8.38/20 respectively (Figure 1).

Figure SEQ Figure * ARABIC 1:Pakistan`s Cybersecurity Performance 2020 – 21



Development Level:
Developing Country

Area(s) of Relative Strength
Capacity Development
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
64.88	15.97	12.26	11.01	17.25	8.38

Source: ITU Global Cybersecurity Index v4, 2021

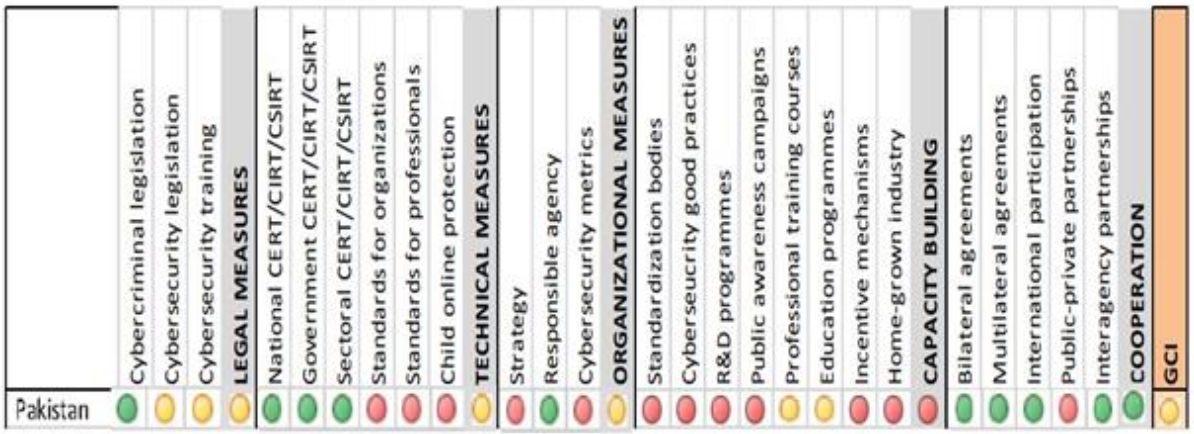
5 Carol Cardno, "Policy Document Analysis: A Practical Educational Leadership Tool and a Qualitative Research Method," *Educational Administration: Theory and Practice* 24, no. 4 (2018): 628, https://www.researchbank.ac.nz/bitstream/handle/10652/4576/PDF_Cardno_C._Policy_document_analysis_paper.pdf?sequence=1&isAllowed=y

6 International Telecommunication Union, "Global Cybersecurity Index 2020," accessed October 4, 2021, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

© ISSI 2021 • All Rights Reserved

In the category of regional ranking, Pakistan ranked 14 among the 18 countries of the Asia-Pacific region. Previously, Pakistan was ranked 94/175 and 67/165 in the GCI 2018 and GCI 2017 respectively[7] (Figure 2).

Figure 2: Pakistan`s Cybersecurity Performance 2017



Source: *International Telecommunication Union (ITU)*

The Government of Pakistan believes that digitalisation is revolutionising socio-economic and cultural development in the world. The introductory section of the NCSP 2021 itself explains this digital transformation. The unprecedented easy and low-cost access to advanced technologies and networks has resulted in a highly connected modern world. The people of Pakistan deserve entry and participation in this era of the Fourth Industrial Revolution (4IR) with all relevant services, protection and tools. Unfortunately, digitalisation has also revolutionised the security risks, challenges and threats.[8] Cyberspace has become the fifth domain of warfare where attacks are more diverse, fast and lethal than ever before. According to the Microsoft Digital Defense Report 2018-19[9] Pakistan is the second most affected country by malware attacks. The monthly malware encounter rate in Pakistan is 18.94. Many cyber security experts are concerned that this malware encounter rate might have increased in the last two years of the coronavirus pandemic. In the last decade, cyberattacks against the critical infrastructures in the public as well as the private sector in Pakistan have resulted in huge financial and informational losses.

7 International Telecommunication Union, "Global Cybersecurity Index 2018," accessed October 4, 2021, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf ; International Telecommunication Union, "Global Cybersecurity Index 2017," accessed October 4, 2021, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

8 *National Cyber Security Policy 2021*

9 Microsoft, "Microsoft Security Intelligence Report (January – December 2018)," accessed on October 6, 2021, https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original

© ISSI 2021 • All Rights Reserved

Policy Text

The NCSP 2021 is fundamentally a "national security policy document." For a state, a national security policy is considered the most significant and critical document as it outlines a framework for the formulation of strategies, laws, rules and procedures for the mitigation of risks, challenges and threats to national security. Although every state enjoys the liberty to tailor the core attributes of its national security policy, the policy studies identify a set of common attributes a security policy must possess to qualify as a credible, effective, successful, reliable and implementable policy.[10] Therefore, it is necessary to do a text/documentary analysis of the NCSP 2021 to identify the presence or absence of those key attributes and determine whether it has the potential to stand the test of time or not.

1. Vision / Policy Statement

The vision or policy statement is thorough and clearly defined in the second section of the policy text. The vision is to design a robust, secure and progressive digital ecosystem in Pakistan that will ensure the availability of digital assets leading to national security and socio-economic development with integrity, confidentiality and accountability.

2. Scope of Policy

The NCSP 2021 covers the entire cyberspace of Pakistan including information and communication systems used by the citizens of Pakistan, all digital assets, "data processed, managed, stored, transmitted or any other activities carried out by the public and private sectors in the cyber domain." Despite repeated references to the protection and management of data in the entire policy text, the issue of data created or produced by the public and private sectors within the cyber domain of Pakistan has not been specifically included in the defined scope of NCSP 2021.

3. Objectives and Policy Deliverables

The second section of the NCSP 2021 contains a list of clearly defined objectives to achieve. It calls for the establishment of the institutional framework, information sharing mechanisms and national cyber security standardisation to enhance governance, create a culture of compliance and audits and ensure the integrity of ICT products. It also aspires to develop public-private partnerships, create cyber security awareness and culture, encourage indigenisation through Research & Development (R

10 Christopher Keller, "Elements of Security Policy," Global Information Assurance Certification Paper (SANS Institute), accessed October 4, 2021, https://www.giac.org/paper/gsec/3495/elements-security-policy-considerations-small-businesses/102691.

© ISSI 2021 • All Rights Reserved

& D) and capacity building. It also aims for designing a framework for cooperation at national and global levels.

4. Risks, Challenges and Threat Assessment

Risks and Challenges	Threats
● Lack of ownership at the top ● Weak enforcement of existing statutes ● Absence of continual improvement and assessment of national cyber security framework. ● Inadequate resources ● Skills shortage ● Absence of CERTS ● Lack of inter-departmental coordination ● Weak accreditation standards	● Cyber-attacks from unprotected infrastructure overseas against national critical infrastructure ● Lack of data governance ● Reliance on external resources (hardware and software)

5. Policy Values

There is no such thing as a value-free policy. States understand this fact and try to identify and achieve relevant policy values. As David Easton defines public policy as "the authoritative allocation of values for the whole society."[11] Therefore, not only the presence but also the absence of certain core values reflect the real intentions and ethics of policy-makers of that particular state.[12] The references to the malicious use affecting the integrity, privacy and other civil rights at various points in the policy text highlights the importance of human values for policymakers. Furthermore, the usage of terms like integrity, transparency, trust and confidence of people, respect for digital sovereignty, confidentiality, availability, equilibrium, empowerment of organisations, promotion of online businesses and digital payments and public prosperity in the policy text indicates that policymakers have given due weight to the socio-economic values.

6. Crisis Management

The second section of NCSP 2021 clearly states that Pakistan will regard a cyber-attack on critical information infrastructures (CII) as an act of aggression against its national sovereignty and reserves the right of self-defence with an appropriate national response. According to the policy text, the energy, telecom, finance, water and healthcare sectors come under CII.

11 Sapru, *Public Policy.*
12 Cardno, "Policy Document Analysis," 624.

© ISSI 2021 • All Rights Reserved

7. Policy History and References

The policy can change with time and it is important to keep the history of modifications for future audits. As NCSP 2021 is the first policy of its kind, therefore, the issue of policy history is not relevant as of now. Furthermore, the NCSP text itself has not addressed this issue. On the other hand, the issue of policy references is significant because policies either stand on their own or achieve their objectives by extending, overriding or complementing other policies, strategies and laws. The NCSP 2021 text highlights the weak enforcement of existing initiatives but does not categorically indicates any overriding. However, the third section talks about the formulation of a new Cyber Security Act by the Cyber Governance Policy Committee (CGPC). How this new legislation will affect the existing mechanisms is yet to be seen. The various existing initiatives mentioned in the first section of the NCSP 2021 are as follows:

i. The Pakistan Telecommunication (Re-Organisation) Act, 1996

ii. The Electronic Transaction Ordinance, 2002

iii. The Investigation for Fair Trial Act (IFTA), 2013

iv. The Prevention of Electronic Crime Act (PECA), 2016

v. The State Bank of Pakistan Guidelines on Information Technology Security

8. Policy Implementation

The government has planned to achieve the capacity building of relevant stakeholders within the first year of the policy. However, the policy text is vague on the issue of the overall implementation timeline. No specific time limit has been set for the achievement of proposed mechanisms. The fourth section of the policy text acknowledges that the implementation will take considerable time. Therefore, in the interim period, the federal government will prioritise initiatives for the banking, telecom, educational and provincial institutions. Yet, the term “interim period” also remains undefined. The policy text also calls for the establishment of a centralised designated federal organisation that will not only coordinate and implement the cybersecurity framework at the national level but also do regulate CERTs at the sectoral and organisational levels.

9. Policy Review

The fifth and last section deals with the policy review process. The NCSP 2021 will go under a comprehensive and inclusive review after every three years. However, this time the timeframe has

© ISSI 2021 • All Rights Reserved

been kept flexible which is a key positive aspect. The NCSP could also be reviewed in consultation with all relevant stakeholders at any time, depending on the major technological advancements by national organisations or emerging global trends in the cyber domain.

Policy Consequences

Policy consequences refer to the ways in which any policy is implemented. The NCSP 2021 is a recent policy, its implementation is yet to be initiated but the procedures, process, principles and structures proposed in the policy text provide signs of its actual potential and expected challenges in the implementation process. Apparently, the major challenge in this policy would be the establishment of the proposed centralised body, which will regulate cybersecurity matters starting from the national level to the individual level. This level of scope is unrealistically ambitious which could make the implementation process impractical. Furthermore, the funding sources of this centralised body as well as many other proposals are unspecified. This lack of harmony between the policy decision-making and fiscal demands could be a huge problem for the implementation process of such a huge scale in a country with limited resources like Pakistan. Whether this new body would resolve the issue of the absence of a central cybersecurity organisation or not but it would definitely create a tug of war among various federal organisations for budget allocation.

Overall, the NCSP 2021 is a comprehensive policy document according to the criteria defined in the policy studies and well placed in the overall national and international security context. However, the placement of this policy in an overall order is improper. Generally, governments first formulate policies that further guide the strategies and legislation. However, in the case of cybersecurity in Pakistan, a policy is being formulated years after legislation has been done especially in the absence of a relevant strategy. The attention of those applauding the NCSP 2021 at this stage, is drawn to the fact that policy-making and policy implementation are two different things. In Pakistan, policy implementation is a bigger problem as compared to policy formulation and therefore requires greater attention to details. Without timely and effective implementation, NCSP 2021 will remain well short of creating the impact it intends to achieve.

© ISSI 2021 • All Rights Reserved