COUNTERING CYBER THREATS IN PAKISTAN: A POLITICAL ANALYSIS OF THE NATIONAL CYBER SECURITY POLICY (2021) AND WHOLE-OF-SOCIETY IMPERATIVE

Minaahil Kamran
Research Scholar
Department of Governance and Public Policy
NUST
minaahilkam20@gmail.com

Dr Hassan Jalil Shah
PRINCIPAL
Jinnah School of Public Policy an Leadership
NUST, Islamabad
hassanjalil@s3h.nust.edu.pk

ABSTRACT
Pakistan, with its complex geopolitical environment, faces an evolving threat landscape, where cyber threats have emerged as a critical component. State and state-sponsored cyber attacks, terrorist organizations, and other malicious actors leverage cyber space to achieve strategic, political and social objectives. The existing cyber security policy landscape and infrastructure face critical gaps, including weak inter-agency coordination, limited resources, outdated legal structure, and a lack of technical capacity to ensure a secure cyber space. This study examines the National Cyber Security Policy of Pakistan (2021) through the analytical lens of political security and policy analysis, with particular attention to the Whole-of-Society approach as a normative and strategic imperative. Drawing on policy analysis, this study considers the Policy Cycle Model to assess the degree to which NCSP incorporates threat perception, multi-actor participation, institutional coordination, and resource and capacity deficits. This study finds that while the NCSP articulates a high-level vision for cyber security, the operationalization of inclusive governance and societal engagement remains a major obstacle in achieving a secure cyberspace. By framing cyber resilience as political governance rather than solely a technical or security issue, this research

paper advances a policy perspective on cyber threats. This study concludes that cyber resilience can be enhanced through governance-centred policy recommendations that emphasize transparency, inter-agency collaboration, and the mobilization of civic and private stakeholders.

KEYWORDS
Cyber Governance, Cyber Security, Cyber Threats, Hybrid Threats, Whole-of-Society Approach.

INTRODUCTION

In the contemporary age of cyber warfare and cyber threats, cybersecurity has now become a significant part of the national security strategies of states. Modern financial systems, critical infrastructures (CI), and critical information infrastructures (CII) of states have become increasingly vulnerable to cyber threats. While cybersecurity capabilities have been considered to be an essential part of national security strategies, cyber warfare is also becoming a significant tool of statecraft. This shift is primarily because of cyber attacks tend to be of low cost and extremely high impact, making them an ideal tool for states and non-state actors to secure strategic goals without getting into a conventional war.

In relation to Pakistan, the country is encountering a range of cybersecurity threats including DDoS (Distributed Denial of Service) attacks, malware, phishing, ransomware, SQL injection, and social engineering scams. In the realm of cyberspace, states have identified three-dimensional threats: *cybercrime, cyber terrorism, and cyber warfare*. (Mirza and Akram, 2022) Owing to the complex geopolitical position of Pakistan and ongoing security challenges, cyber warfare has become a significant concern in security circles. The national security landscape of Pakistan is shaped by the internal security challenges, historical tensions with neighbouring states, and the proliferation of terrorism from over the past few decades. Over the past few decades, Pakistan has faced an increasing number of cyber threats from state actors, state-sponsored actors, and non-state actors, especially terrorist organizations. These threats included targeting critical infrastructure, public institutions, financial systems, and military assets; thus, reflecting the growing resilience of threat actors in cyber space owing to the low-cost and high-impact nature of cyber warfare.

The internet penetration in Pakistan has exceeded 45.7% with 111 million users by January 2024, according to the report of Global Digital Insights. (Kemp, 2024)

According to the global cyber security company Kaspersky, the overall cyber risks in Pakistan increased by 17% in 2023 as compared to 2022. To counter threats in cyber space, the government of Pakistan launched the Pakistan Electronic Crimes Act (PECA) in 2016, followed by the formation of the National Response for Cyber Crime (NR3C) of the Federal Investigation Agency (FIA) to counter cyber crime. (Shaikh et al., 2024) Considering the regulatory framework to address cyber security issues, the government established Pakistan Computer Emergency Response Team (PakCERT) to respond to cyber incidents. Most importantly, the introduction of the National Cyber Security Policy 2021 outlined a comprehensive framework for cyber governance, infrastructure protection, and international cooperation. However, the success of policy instruments depends on the effective implementation strategy, which remains deficient in the policy document.

Hybrid threats are not new, but the recognition of such multi-model threats commands a 'holistic' approach, which combines traditional and non-traditional responses by the state along with the society as a whole. Responses to hybrid threats have to be measured and proportionate: from civil defence and policy responses to counterinsurgency (COIN) and military measures. This paper aims to explore the dynamics of cyber threats in Pakistan, its impact on national security, and potential policy response measures. This research is intended to identify policy gaps from a policy cycle lens and provide effective policy recommendations to make the cyber space of the country safer and secure.

LITERATURE REVIEW

In the early 1990s, the concept of soft power was introduced as a "gentle" influence strategy, allowing nations to extend their strategic reach through non-coercive tools such as public diplomacy rather than military or economic power. This concept was introduced by American political scientist Joseph Nye, and further expanded it with the introduction of the concept of 'cyber power'. Nye defined cyber power as, ***" a set of resources tied to the creation, control, and communication of electronic and computer-based information, encompassing infrastructure, networks, software, or human expertise."*** (Nye, 2010)

In the age of cyber warfare, cyber defense and cyber security have become critical for policy makers. The intersection of cyber threats and national security has emerged as a critical area of concern, particularly for states like Pakistan, facing both traditional and non-traditional security threats. A key theme in the literature is the emergence of hybrid threats as a defining characteristic of contemporary cyber

conflict. Hybrid threats are described as coordinated and synchronized attacks targeting systematic vulnerabilities through a blend of military, paramilitary, and cyber tools. Scholars identify the complexity of these threats and maintain that cyber threats are not considered under conventional warfare or crime. (Calabres, 2023 ; Jaspal, 2020) In the context of Pakistan, hybrid warfare is manifested through cyber attacks on government information infrastructure and information warfare to manipulate political narratives to weaken public trust. This conceptualization underscores the need for cyber security strategies that account for both technical vulnerabilities and the national database ecosystem. This theme reflects a convergence of cyber security with national security concerns, where disruptions of digital infrastructure translate into social, political, and economic instability. The wider security framework of the Copenhagen School reinforces this idea that security should encompass military as well as non-military sectors, including digital infrastructure. (Ali et al, 2022)

The literature further highlights the lack of cybersecurity readiness in the institutional frameworks of Pakistan. Despite growing awareness of cyber threats, the cyber security landscape of the country is characterized with legislative gaps, fragmented institutional responses, insufficient coordination among stakeholders, and inadequate financial and technical resources. (Adeel & Shan, 2020) Similarly, Riaz (2019) in this article maintained that although the Global Cybersecurity Index (GCI) categorized Pakistan as a "maturing state," which reflects progress but there exists persistent deficiencies in legal, technical, and operational dimensions. The literature indicates that while Pakistan has implemented regulatory measures such as the Prevention of Electronic Crimes Act (PECA), these efforts remain focused more on cybercrime than on comprehensive threats of cyber warfare and cyber terrorism. (Mirza & Akram, 2022). This readiness gap is particularly critical given the role of state-sponsored and non-state actors in cyber space, leveraging digital tools to challenge stability.

The literature highlights that Pakistan is considered has been facing three-dimensional cyber threats: cyber warfare, cyber terrorism and cyber crime. Riaz (2019) defined cyber warfare as **'a *state-sponsored cyber attack, which is usually well-funded, organized, and carried out by highly skilled personnel.***' The author further mentions that India has been developing cyber capabilities and Indian military strategies, such as the Cold Start Doctrine, which considers cyber warfare entailing attacks on the critical information infrastructure of the enemy. In December 2010, thirty-six websites of the government of Pakistan were hacked by

an Indian group of the Indian Cyber Army, followed by hacking the websites of the Pakistan Navy, National Accountability Bureau (NAB), and NADRA. The Pakistani hackers took revenge, and two days later, a group named Predators PK hacked more than 200 Indian websites. Pakistani APT focused principally Indian military and strategic staff concerning national security secret activities. (Mustafa, Murtaza and Murtaza, 2020) Similarly, reports reveal that Pakistan is one of the top ten targeted countries in the world. Snowden's data revealed that the National Security Agency of the USA was deploying malware named SECONDDATE to spy on the civilian and military leadership of Pakistan. (Babar, Mirza and Hasnain Qaisrani, 2021)

Apart from cyber warfare, Pakistan has been facing the threats of cyber crime and cyber terrorism. Bernadette Hlubik Schell and Martin (2005), in their book *'Cyber crime: a Reference Handbook*', defined cyber crime as crimes related to activities of individual hackers and groups for personal gains. According to a cyber security firm, Kaspersky, the financial sector of Pakistan experienced a 114% increase in malware and phishing attacks. The report further revealed that 13.7% of Pakistani users encountered cyber-based threats, such as phishing, during the last quarter of 2024. Spyware attacks, which aim to collect and transmit unauthorized user data, has been increased by 63% in 2024. These attacks raise concern of data protection of public and private sector organizations and institutions. (Profit, 2024) Cyber terrorism, on the other hand, is aimed to exploit the social and political landscape of the country through attacking computer-based systems and critical infrastructure of the government. Mirza and Akram (2022) argued in their research article that terrorist organizations have been leveraging cyber space to achieve their interests. The author further maintained that organizations such as ISIS, al-Qaeda, and Hizb-ul-Tahrir expand their radical agenda through cyber space. Similarly, Zaheema Iqbal (2021) in her research article '*Terrorism in Cyber Space: a Case Study of Terorist Organizations Operating in Pakistan*', argued that terrorist organizations have been using cyber space for propaganda, planning, recruiting, and funding terrorist attacks. (Iqbal, 2021)

Pakistan's response to emerging cyber threats has materialized through legislative, institutional, and policy measures, culminating in the introduction of the National Cyber Security Policy (2021). Similar to the cyber security strategies of the USA, UK, Russia, and China, the NCSP aligns cyber security with broader national security goals. This policy articulates a framework for protecting critical infrastructure, promoting public awareness, and developing indigenous cyber

security technological capabilities. Nevertheless, the policy fails to align cyber security with national security. The underlying structural challenges, such as the absence of dedicated cyber security institutions, a persistent traditional security culture resisting integrating cyber security concerns, a lack of cyber security risk awareness among the public and public officials, and limited public engagement, create barriers to effective operationalization of the policy. (Ahmad, 2022) These institutional and structural weaknesses are further compounded by budgetary constraints and capacity deficits, limiting the ability of the state to invest in advanced cyber security capabilities and retain skilled cyber security professionals. The literature further considers policy responses and strategic frameworks for enhancing cyber security. Scholars emphasize that effective cyber security policy must move beyond reactive measures towards adopting a proactive posture. (Ali et al, 2020) Recommendations in the literature call for multi-stakeholder collaboration, including government institutions, regulatory and technical authorities, private firms, international partners, academia, and think tanks. (Adeel and Shan, 2020) This theme reflects upon the whole-of-society approach to cyber security, adopted from comprehensive governance models, including disaster risk reduction and public health. This approach primarily highlights the interconnection of state institutions, the private sector, media, academia, and individuals. The Cooperative Cyber Defence Centre of NATO defines this approach as ***"a comprehensive engagement where cybersecurity is a shared responsibility."*** (CCDCOE, 2019) Similarly, the US National Cyber Security Director, Chris Inglis, recently called for a ***"new social contract"*** to manage cyber risks. (Staff, 2022) The idea is that effective cyber security cannot be achieved by the government alone and requires a collective action across all sectors of society. Jason Smith's article titled "*Forget a Whole-of-Government Cybersecurity Strategy - It's time for a Whole-of-Nation Approach*," calls for a cybersecurity strategy that extends beyond government to include the private sector and the general public. Smith maintains that current cybersecurity models are highly government-centric and are insufficient in countering sophisticated cyber threats. The involvement of the private sector will improve sophistication owing to the innovation and agility of the sector. Smith further suggests that a whole-of-nations approach should include coordinated efforts between public and private entities, clear guidelines on roles and responsibilities, public education on cyber security, and the establishment of legal frameworks to facilitate collaboration. (Smith, 2022)

The literature review thus illustrates that existing literature, although it considers the emerging threats in cyber space and governmental responses to them, but there exists a limited academic scrutiny on the operationalization of these policy infrastructures. This research addressed this policy-to-practice gap and explored the connection between policy formulation and policy implementation. The policy cycle enables the exploration of the National Cyber Security Policy (2021) from agenda setting, policy formulation and policy implementation. While scholarly discourse focuses on cyber security in Pakistan, there remains a critical gap in applying structured policy analysis frameworks, especially the policy cycle model, to understand and assess policymaking and implementation mechanisms related to cyber security. In addition, the an absence of an Operationalized Whole-of-Society Cyber Security Framework for Pakistan. The concept is considered normative, especially in the context of cyber security in Pakistan, and lacks practical application or policy integration in the cyber security landscape of the country. Most importantly, this research paper explores the consideration of governance mechanisms to address cyber security issues, rather than solely relying on technical or security models.

RESEARCH METHODOLOGY

DATA COLLECTION

For ***primary data collection***, this study conducted in-depth interviews from government ministries, such as the Ministry of Interior, Ministry of Planning and Development, Ministry of Information Technology and Telecommunication (MoITT) and Ministry of Law and Justice. Cyber security experts from regulatory authorities, including Pakistan Telecommunication Authority and the technical authority National CERT (Computer Emergency Response Team), were consulted to assess the gaps in the existing policy landscape related to cyber security. To analyse the stakeholder coordination during the policy formulation and implementation phase, experts from think tanks (Center for Aerospace and Security Studies, CASS and Pakistan Institute of Policy Studies, PIPS), academia (NUST CIPS) and civil society organizations (Institute for Public Opinion Research, IPOR) were interviewed.

For ***secondary data collectio***n, this study relies for data collection on academic literature, government reports and policies, think tank reports, and cyber security threat reports to understand the threat landscape and mechanisms to improve cyber security landscape through policy intervention.

DATA ANALYSIS

This study conducted systematic ***content analysis*** on cyber security reports, policy documents and case studies to identify patterns of cyber threats and gaps in the cyber security infrastructure and policies of Pakistan. To systematically examine the context of Pakistan, this study employs qualitative content analysis as the primary data analysis method. The data set for content analysis included the National Cyber Security Policy of Pakistan (2021), government reports and press releases by institutions such as MoITT, PTA, and FIA Cyber Crime Wing. Policy speeches, parliament reports, think tank reports, and cyber security briefings were also consulted for data analysis.

Thematic analysis is used to identify recurrent themes and issues across the data collected, especially during the interview process. Thematic analysis techniques in Nvivo were used to measure the frequency and occurrence of key concepts such as 'cyber threat perception', 'cyber security governance', ' capacity building', etc.

IMPLICATIONS AND LIMITATIONS OF THE STUDY

This research has significant implications for academic research, curriculum development, and interdisciplinary collaboration, especially by bridging cyber security, governance, and societal engagement through a holistic and multisectoral model. For national and sub-national policy makers, this study offers a road map for inclusive and sustainable cyber security governance through whole-of-society integration. Multistakeholder stakeholder engagement is encouraged between law enforcement agencies, IT regulators, government ministries, civil society organizations, think tanks, and academia. For digital rights and empowerment, this study provides a rights-based framework to prevent misuse of cyber crime laws for political surveillance and censorship. For the education sector, this study will have a positive impact and will facilitate the integration of cyber security along with digital rights and civic engagement.

While this study offers valuable insights into the gaps and challenges within the National Cyber Security Policy of Pakistan in addressing cyber threats, limited access to classified sensitive information was the major limitation of this study. Given the national security implications of cyber governance, many relevant documents, security assessments, and internal policy drafts were either classified or inaccessible to the public. The restricted scope of stakeholder recognition was another major obstacle. Although interviews were conducted from a diverse set of

stakeholders, but this study was unable to secure interviews with certain key actors, such as military intelligence agencies and private security firms. Cyber security is a rapidly changing field, and thus cyber threats and policy responses are rapidly evolving. The findings of this study will only consider the threats and policy environment until the year 2025 and may not capture subsequent updates.

DISCUSSION

With the changing nature of warfare, states must not only build technical defence but also consider inclusive and sustainable policies that respond to these hybrid threats. The National Cyber Security Policy of Pakistan (2021) was introduced as a policy document to secure cyber space; however, preliminary analysis suggests that significant conceptual, institutional, and operational deficiencies hinder effective implementation. This study addresses the urgent need to evaluate the threat recognition, practical relevance, and institutional capacity in countering cyber threats. This study further seeks to identify policy gaps in the cyber security governance infrastructure that undermine its effectiveness, along with exploring policy reforms to institutionalize a more inclusive and strategically robust cyber defense infrastructure. The following themes have been extracted using NVivo for content and thematic analysis from secondary and primary sources:

AGENDA SETTING AND THREAT IDENTIFICATION

Conceptual Ambiguity in Threat Recognition

The National Cyber Security Policy is a foundational document to achieve cyber security, with a vision to **"*have a secure, robust, and continually improving nationwide digital ecosystem ensuring accountable confidentiality, integrity, and availability of digital assets leading to socio-economic development and national security.*"** (Government of Pakistan National Cyber Security Policy 2021, 2021) Although the policy mentions the current cyber security landscape of Pakistan, the NCSP fails to identify cyber threats faced by Pakistan. Mirza and Akram (2022) in their research article, '*3 Cs of Cyber Space and Pakistan, '* maintains that states are currently facing three-dimensional threats in the realm of cyber space: cyber warfare, cyber crime, and cyber terrorism. The inability of the policy framework to identify cyber threats, especially cyber terrorism, exposes the lack of readiness in terms of legislation, policy and implementation to counter these threats.

Low Institutional Threat Perception

The identification and realization of cyber warfare and cyber terrorism as a threat is important to design and formulate counter-offensive strategies. The interviews conducted from government bodies and law enforcement agencies revealed that the NCSP fails to model or anticipate cyber threat capabilities of government institutions. The Cyber Security Director of PTA maintained that, '*Upon asking about the improvement mechanisms from government officials, they had no idea whether cyber security exist as a threat or not.'*

POLICY ADOPTION AND FORMULATION

Overlapping and Siloed Institutional Mandates

The National Cyber Security Policy 2021 formulated Cyber Governance Policy Committee (CGPC) for strategic oversight over national cyber security issues. In addition, Computer Emergency Response Teams (CERT) were formed at national level and sectoral level for coordination and implementation of all cyber security related matters. The Director Cyber Security of Ministry of Information and Technology, mentioned that the government needs to formulate a Cyber Security Authority since CERT does not have the mandate to enforce rules and regulations related to the policy.

The policy does not provide institutional mandates to ministries and divisions, considering their roles and responsibilities in implementing this policy, which stands as a major policy gap. Governmental ministries, including the Ministry of Interior, the Ministry of Planning and Development, Ministry of Law and Justice, which should have a clear mandate related to cyber securiy, have failed to establish cyber security departments or wings. National Response Center for Cyber Crime (N3RC), a law enforcement agency mandated to fight cyber crime in the country, does not consider other potential cyber threats, such as cyber terrorism. This situation does not only reflects poor operationalization of the policy but also stands as a challenge to cyber command unity which is crucial to manage and deter cyber threats.

Coordination Failures Among Agencies

Since the NCSP fails to mandate government agencies and bodies to work in their respective capacities on threats related to cyber space, there exists no coordination among governmental departments or institutions related to cyber security threat

identification and mitigation. The security experts from strategic study institution, such as Center for Aerospace and Security Studies (CASS), revealed that there exists 'significant' weak inter-agency coordination. The security expert from Pakistan Institute of Policy Studies (PIPS) maintained that there is a varied degree of mistrust among government entities. He further noted that government institutions and entities are not trusted by security agencies, which shows weak civil-military coordination. In issues such as cyber terrorism, the government institutions need to be trusted enough to ensure the effective implementation of policies and plans.

POLICY IMPLEMENTATION AND EVALUATION

Inadequate Technical Workforce and Training

Technological deficiency in cyber security policy implementation often arises from factors such as outdated infrastructure, obsolete software, open source libraries, complex processes, and insufficient investment in appropriate cyber security technologies. Organizations and institutions are impacted from cyber threats when they fail to keep pace with the increasing vulnerabilities and rapidly evolving threats in cyber space. These gaps pave the way for security breaches which result in data losses, performance degradation, financial losses, reputation damages and legal liabilities. In addition, human resource issues lead to operational challenges and present broader issues. The ability to protect sensitive data, systems, and processes becomes impossible when sufficient manpower is not available.

Interviews conducted from government officials, including the Ministry of Interior, Ministry of Law and Justice, and Ministry of Planning and Development, revealed that there is no conceptual understanding of cyber security or cyber terrorism among government officials. The PTA official identified this gap and mentioned that there is a lack of capacity building among government officials and technical staff. Similarly, a strategic studies expert argued that, "*Government institutions do not have the technical expertise to materialize and implement these policies, and there is no effort to improve their technical gap."*

Budgetary and Legal Resource Constraints

The deficiency of financial resources directly impacts cyber security and risk management programs. Inadequate financial resources may have an effect on other cyber security functions or elements, including inadequate security infrastructure,

limited talent acquisition, outdated systems and technologies, reduced training and awareness programs, and limited investment in compliance and regulation. In this regard, the MoITT mentioned that, "*Human resource capacity building is taking place, but financial constraints are there related to cyber security solutions."* PTA official mentioned that, "*Cybersecurity solutions are expensive, so there is a need to aware government officials aware that they are the need of the time, and so the budget should be increased for that purpose."*

WHOLE OF SOCIETY IMPERATIVE

Minimal Involvement of Civil Society and Academia

In-depth interviews from think tanks, academia, and civil society revealed that stakeholder engagement was minimal during policy formulation, policy implementation, and the policy evaluation phase. Security expert from PIPS remarked that, "*Even the policies are not made and consulted in the parliament, so how can we expect private entities to be consulted. "* Similarly, the Director of CASS maintained that "*input from all stakeholders and SMEs is missing."* PTA Director Cyber Security mentioned that*, "* E*ngaging with civil society is a critical task on regulations since collaborating with them makes things tough."* Civil society organizations are essential in offering feedback on the state of cyber threats, particularly regarding matters like how cyberattacks affect safety, human rights, and vulnerable demographics. The policy expert from the Institute of Public Opinion Research (IPOR) was of the opinion that the input from civil society is almost non-existent, which hinders the effective implementation and evaluation of policies. Third-party evaluation is practiced at PTA, which involves only technical experts and companies for improvements in cyber security and no input from academia or civil society, which should be practices especially by the ministries during the policy formulation phase.

Underdeveloped Public-Private Partnerships

The Director of Cyber Security at MoITT mentioned that, "*We could not properly implement a public-private partnership related to cyber security as mentioned in NCSP. There is no investment in industry related to cyber security which could improve public-private partnership."* PTA conducts third-party audits from private contractors, which is commendable. Ministry of Law and Justice revealed that only telecom operators were consulted during PECA amendments, which define cyber

terrorism and cyber crime and served as a legislative framework for NCSP. The Ministry of Interior does not have any sort of collaboration or partnership with the private sector, and there is no evaluation mechanism.

CONCLUSION

This study critically examined the National Cyber Security Policy of Pakistan through the lens of the policy cycle model and the whole-of-society approach. Drawing on systematic content analysis, expert interviews and NVivo-based thematic analysis, the research unveiled significant conceptual, institutional and operational gaps that undermine the ability of policy documents to address emerging cyber threats.

The absence of threat identification in the policy language reflects a fundamental failure in the problem identification phase. This lack of conceptual clarity has weakened the agenda-setting and policy formulation process, resulting in a document that fails to align with evolving cyber threats within the broader national security landscape. The first major theme identified through NVivo analysis was '***Conceptual Ambiguity in Threat Recognition***.' The NCSP policy document and interview data revealed that a unanimous observation from experts at CASS, PIPS, and the Ministry of Law was that the policy does not mention major cyber threats in the problem identification phase of the policy cycle. This omission reflects a narrow understanding of cyber threats, and ambiguous definitions of important concepts such as cyber crime and cyber terrorism will hinder effective implementation, increasing the probability of undermining digital rights and civic engagement. The second theme mentions the ***'Low Institutional Threat Perception***', which explores that the government institutions and public sector officials fail to understand cyber threats, which hinder their ability to plan and implement counter policies and strategies.

The implementation phase of the NCSP is hindered by institutional fragmentation, overlapping mandates, and weak inter-agency coordination. The lack of unified command structures, capacity deficits among public officials, and limited budgetary support further dilute the effectiveness of the policy. Under this domain, NVivo analysis surfaced a dominant theme of ***'Institutional Fragmentation and Role Diffusion.***' Interviewees from MoITT, PTA, and the Ministry of Interior underscored overlapping mandates, siloed operations, and a lack of vertical integration among institutions. The node matrix analysis in NVivo observed frequent occurrences of terms such as 'mandate conflict' and inter-agency

mistrust', suggesting a systematic implementation failure. The second theme extracted under this domain was ***'Resource and Capacity Deficits'***, strongly evidenced from discussions with MoITT and PTA, who cited limited budgets, lack of skilled personnel, and insufficient legal tools as critical bottlenecks. Content frequency analysis showed that 'capacity', 'budget', and 'training' were among the most frequently cited terms in interviews. This adheres that the NCSP lacks the operational scaffolding necessary to implement effective cyber security measures.

Lastly, the content and thematic analysis revealed that the NCSP fails to adopt a Whole-of-Society Approach (WoSA). Civil society, think tanks, academia, and the private sector remain largely excluded from the policy process, and there is a lack of cyber awareness and community-level preparedness that hampers national cyber resilience and contradicts with global best practices that emphasize distributed responsibility and inclusion. NVivo coding revealed a strong theme of ***'Exclusionary Stakeholder Engagement.***' Respondents from PIPS, IPOR, and CIPS noted that civil society and academia were either excluded from the consultation process or only consulted in a post-facto manner. This violated the principles of WoSA, in which strategic resilience depends on civic and academic collaboration. A second theme, ***'Deficits in Cyber Awareness and Community Resilience,'*** was identified during the interview process with MoITT and PTA officials. Coding queries showed frequent mentions of 'lack of awareness,' 'training gaps, ' and 'cyber hygiene across the transcripts. Notably, no existing mechanism was found for engaging local communities or institutions for digital literacy programs or cyber preparedness drills.

In conclusion, the National Cyber Security Policy of Pakistan (2021), in its current form, fails to address the multidimensional threats. Bridging the gap between cyber security ecosystem and operational capability requires not only technical upgrades but also institutional realignment, cross-sector collaboration, and a sustained commitment to national cyber resilience.

POLICY RECOMMENDATIONS

Area	Recommendations	Rationale
Legal & Definitional Clarity	Clearly define cyber terrorism and distinguish it from cyber crime and activism, based on intent & motive, actor, target, means and impact.	PECA 2016 and NCSP 2021 currently lack a specific definition, which leads to overreach and violation of civil rights
	Propose the framing of the General Data Protection Act (GDPR) and the Data Protection and Privacy Act	To prevent data linkages of individuals and ensure data privacy, these acts are significant along with cyber security regulations.
Institutional Reform	Establish National Cyber Security Authority	Current roles are dispersed across MoITT, FIA, NACTA, without a unified chain of command.
	Enhance the authority and capacity of PKCERT with incident response and threat intelligence mandates.	PKCERT remains reactive and under-resourced; expanding its scope can improve early threat detection.
Policy Implementation	Develop a national-level Cyber Incident Response Protocol	Ensures coordinated and timely response to cyber terrorism incidents across all sectors.
	Mandate cyber audits of CII (critical information infrastructure)	This helps identify vulnerabilities in finance, telecom, power, and defense sectors.

Public-Private Partnership	Create formal PPP mechanisms in NCSP.	Enhances threat information sharing and coordination with ISPs, banks, and tech companies.
	Encourage private sector compliance with national cyber security standards	Aligns private sector practices with national security interests.
Monitoring and Evaluation	Establish an independent oversight body for audits and compliance	Introduces transparency and adaptive governance.
	Publish Annual National Cyber Threat Reports	Informs policy reform and public awareness through open data on incidents and vulnerabilities.
Whole of Society Approach	Develop national digital literacy and cyber resilience programs	Empowers citizens to recognize cyber threats and resist online radicalization.
	Institutionalize the role of academia, civil society and media for policy consultation and implementation	Expands societal ownership and democratic legitimacy of cyber policy.

REFRENCES

Adeel, A & Shan, R. (2020). Global Cyber Terrorism: Pakistan's Cyber Security in Perspective. *Pakistan Journal of Terrorism Research*, *2*(1). http://pjtr.nacta.gov.pk/index.php/Journals/article/view/102

Ahmad, S. (2022). Cyber Security Threat and Pakistan's Preparedness: An Analysis of National Cyber Security Policy 2021. *Pakistan Journal of Humanities and Social Sciences Research*, *5*(1), 25–40. https://doi.org/10.37605/pjhssr.v5i1.381

Ali, S. A., & Mehmood, N. (2025). *View of Conceptualising Cyber Deterrence and Policy Options for Pakistan*. Thesvi.org. https://thesvi.org/ojs/index.php/ojs/article/view/319/170

Babar, I., Mirza, M., & Hasnain Qaisrani, I. (2021). Evaluating the Nature of Cyber Warfare between Pakistan and India. *Webology*, *18*(6), 2021. https://shs.hal.science/halshs-03788162/document

Bernadette Hlubik Schell, & Martin, C. (2005). *Cybercrime : a reference handbook*. Santa Barbara, Calif.

Calabrés, S. (2023, March). *Cybersecurity and hybrid warfare: Expanding the spectrum.* Global Affairs and Strategic Studies. https://en.unav.edu/web/global-affairs/ciberseguridad-y-guerra-hibrida-la-ampliacion-del-espectro

Iqbal, Z. (2021). Terrorism in Cyber Space: A Case Study of Terrorist Organizations Operating in Pakistan. *4th Bosphorus International Conference on Cyber Security, Cyber Politics, and Social Sciences*. https://www.researchgate.net/publication/358125095_Terrorism_in_Cyber_Space_A_Case_Study_of_Terrorist_Organizations_Operating_in_Pakistan?utm_source=chatgpt.com

Jaspal, Z. (2020, April 8). *Pakistan's National Security Hybrid Warfare Challenges & Countermeasures*. https://www.researchgate.net/publication/340514708_Pakistan

Kemp, S. (2024, February 23). *Digital 2024: Pakistan*. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2024-pakistan

Mirza, M. N., & Akram, M. S. (2022). 3-Cs of Cyberspace and Pakistan: Cybercrime, Cyber-Terrorism, and Cyber Warfare. *Strategic Studies*, *42*(1), 62–80. https://doi.org/10.53532/ss.042.01.00134

Nye, J. (2010). *Cyber Power*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/cyber-power

Profit. (2024, November 19). *Cyberattacks surge by 114% in Pakistan's financial sector in 2024*. Profit by Pakistan Today. https://profit.pakistantoday.com.pk/2024/11/19/cyberattacks-surge-by-114-in-pakistans-financial-sector-in-2024/

Riaz, M. (2019). *Cyber Threat Landscape and Readiness Challenge of Pakistan*. https://www.issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf

Smith, J. (2022, February 22). *Forget a Whole-of-Government Cybersecurity Strategy—It's Time for a Whole-of-Nation Approach*. Modern War Institute. https://mwi.westpoint.edu/forget-a-whole-of-government-cybersecurity-strategy-its-time-for-a-whole-of-nation-approach/