

DIGITAL SOVEREIGNTY AND SOCIETAL VULNERABILITY: AN ANALYSIS OF CYBERSECURITY THREATS IN PAKISTAN

*Dr. Tehmina Aslam Ranjha and Ammad Malik**

Abstract

Since the auction of 3G/4G licenses by the federal government of Pakistan, the increase in internet connectivity and widespread adoption of smartphones has resulted in the country's cybersecurity infrastructure coming under stress. This study discusses Pakistan's contemporary and ever-evolving cyber threat landscape from 2023 to 2025. It is broadly divided into three distinct tiers: namely, 1) state-level hybrid warfare, 2) critical infrastructure vulnerabilities, and 3) individual-level cybercrime. At the state level, Pakistan faces acute cyber challenges and threats that target sensitive defence and diplomatic communications. Similarly, the mass transit systems of its megacities such as Lahore and Karachi and the financial system are also vulnerable to outside digital interference. The threat is equally profound on the civilian level, as highly publicized leaks of national databases such as NADRA have demonstrated. In addition to the vulnerability of national databases, financial fraud targeting ordinary citizens via banking apps and phishing attempts is also a very common phenomenon. This shows deficiencies in the enforcement mechanism of current legislative frameworks. Finally, the paper proposes a strategic roadmap focused on statutory data protection, unified institutional governance, and mandatory OT standards to secure Pakistan's digital infrastructure.

Keywords: Cybersecurity, Pakistan, Digital Sovereignty, Cybercrime, Hybrid Warfare, Data Protection.

Introduction: The Digital Frontier and the Security Paradox

Over the past two decades, Pakistan's digital connectivity has expanded dramatically. Currently, more than 120 million people access the internet, driven largely by the post-2014 roll-out of 3G/4G networks, the proliferation of

*Dr. Tehmina Aslam Ranjha is a national security consultant with expertise in counter-terrorism and de-radicalization domains. She is also a prolific author and regular contributor to national dailies. Ammad Malik is a doctoral candidate and a commentator on security issues. The author can be reached at taranjhai@gmail.com.

cheap smartphones, and a youth demographic where 60 percent of people are under 30.¹ This has allowed both the Pakistani state and various other commercial entities to shift from paper-heavy processes to centralized digital systems. To further exemplify digitization, the National Database and Registration Authority (NADRA) built one of the world's largest multi-biometric identity databases, while the State Bank of Pakistan (SBP) launched the RAAST instant payment network to digitize peer-to-peer and merchant transactions; other government services, such as tax filing and passport applications, have migrated to cloud-based portals.² The country's financial sector has also invested in the development of various fin-tech applications such as "Easypaisa" and "JazzCash", which have brought tens of millions of previously unbanked adults into the formal financial system.³ However, this aggressive digital expansion has occurred without a comparable investment in infrastructure security. This rapid digital integration into both global and local digital networks has dramatically increased the number of vectors through which cyberattacks could occur. Because digital integration has, so far, outpaced defensive capacity, both federal institutions and private citizens remain highly vulnerable to systemic threats from state-sponsored actors and cybercriminals.

Pakistan's present position in the cybersecurity global hierarchy is a bit of a paradox, considering the challenges faced by the country in the digital domain. According to the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) 2024, Pakistan secured a ranking that placed it in the same category as developed nations such as the United States, Japan, and Singapore.⁴ Pakistan was also praised in the same report for significant progress in the domains of technical capacity, legal reforms and inter-departmental coordination.⁵ However, it is important to note that the ITU report's criteria primarily measures "commitments" made in current policies, rather than their operational effectiveness. The ground reality was exposed shortly after the publication of the ITU report by the occurrence of several major security breaches. These included the leaking of login information of over 180 million internet accounts, the exposure of SIM data belonging to senior officials and the record of over 2 million citizens being leaked on the dark web after a cyberattack on the NADRA database.⁶

This gap between Pakistan's international standing and its internal security vulnerabilities is what this article terms the "Performance Paradox." The paradox exists mainly because, while the state has been quick to build the organizational

apparatus and administrative posts required to satisfy international digital standards, it is not accompanied by the existence of a robust security architecture.

The model of “Digital Hybrid Warfare” is applied in this research to conceptualize the operational threats faced by Pakistan in the digital domain. This framework operates primarily via non-kinetic methods, including cyberattacks, coordinated disinformation campaigns and the manipulation of algorithms. The weaponization of certain social media narratives, including those emerging from outside Pakistan, also falls in this category. The overarching goal of Digital Hybrid Warfare is to take advantage of existing socio-economic and ethnic divisions in Pakistan to degrade public trust in state institutions and achieve strategic objectives, all without the need to engage in conventional warfare.

Much like other domains in South Asia, cybersecurity too has been heavily “securitized”, meaning that it is now considered part of the wider national security umbrella and is treated with the same seriousness as territorial integrity.⁷ The importance that the state gives to cybersecurity is evident in its framing, as the digital domain is spoken of in terms of being a critical strategic asset that requires its own active defence. Nevertheless, the cybersecurity domain suffers from a structural issue known as the “attribution problem”. This refers to the technical difficulty of conclusively identifying where exactly a cyberattack originated from. This issue is compounded by the infrastructure of global network routing which makes anonymity technically easy to achieve while keeping operating costs low.

Research Methodology

This study attempts to analyze Pakistan's cybersecurity threat landscape, with an emphasis on developments from 2024-2025. The research material is derived from a wide array of secondary sources, such as research papers published in cybersecurity-focused journals and publicly available reports from cybersecurity firms such as Kaspersky and Cisco. In addition, government documents and annual reports by the Digital Rights Foundation are also referenced. Newspaper articles, wherever used, are primarily those that are deemed high-quality publications such as Dawn, Tribune and The News. After a quantitative survey of the overall threat environment, the analysis is organized into two distinct domains: state-level threats that target national sovereignty and strategic assets, and individual-level threats that compromise citizen privacy and digital economic trust. The study concludes by drafting a governance-centered framework that attempts to better align national cyber capabilities with the state's broader digital policy ambitions.

Survey of Cybersecurity Threats: Quantifying the Digital Siege

The Statistical Landscape

A survey of coverage from threat monitoring bodies indicates that cyber-attacks in Pakistan targeting both private and government networks have been escalating rapidly. Internet security reports published by Kaspersky, a cybersecurity firm, indicated that during the first three quarters of 2025, more than 5.3 million on-device security incidents were detected within the country.⁸ These "local" threats were predominantly delivered via infected USB drives, malicious CDs and DVDs, or hidden installers bundled with pirated software and affected 27 percent of all individual users and 24 percent of corporate entities in the country. Furthermore, Kaspersky blocked an additional 2.5 million web-based attacks during the same period. Approximately 16 percent of Pakistani users and 13 percent of corporate entities encountered web-based threats, including phishing scams, botnet activity, Remote Desktop Protocol (RDP) exploits, and network spoofing operations such as the deployment of rogue Wi-Fi access points in public spaces.⁹

However, the data only includes intercepted internet traffic. The true volume of malicious activity remains significantly higher due to a mixture of different problems such as non-existent or fragmented domestic network monitoring and widespread end-user digital illiteracy. The newly established National Cyber Crime Investigation Agency (NCCIA) received more than 160,000 complaints in the year 2024 alone. However, only about 1% of these complaints resulted in the registration of a formal case. The conviction rate is also worrying as the number did not cross double digits.¹⁰ Cyber criminals are well aware that such an "enforcement gap" exists and the probability of them facing legal consequences for their actions remains negligible. Such an environment also emboldens cybercriminals further and the law loses its deterrence effect.

Malicious Software: Types and Trends

The contemporary malware landscape in Pakistan is divided broadly into two categories. The first category consists of targeted tools focused on finance services, whereas the second category consists of malware engineered to target high-profile individuals with specialized packages. The fastest-growing threat category remains banking app trojans, which refer to malicious apps that mimic "normal" software but are actually designed to extract valuable login credentials or

steal financial data. Android users are especially vulnerable to these threats, due to Google Play Store's often criticized app hosting policies that allow cyber criminals to get their apps officially hosted. This is part of a wider trend that is echoed in international markets as well, with Kaspersky reporting that over 165, 000 banking malware attempts were blocked in a nine-month period in 2025 and that attacks involving banking apps on Android devices have increased at a rate of 56% every year.¹¹ These are sophisticated tools that involve constant software tinkering, as banking apps routinely upgrade their security protocols. This suggests the presence of an underground economy, where disgruntled software engineers and finance-literate professionals engage in cybercrime to outsmart the constantly evolving security architecture of banking apps.

Lately, it has also come to light that malware such as "Triada" and "Keenadu" are being installed directly into Android smartphones during the manufacturing and/or supply chain process. These infected Android devices are sold as brand-new products but provide malicious cyber criminals total administrative control over these devices from the day they get activated by unsuspecting users.¹² These infected devices are sold as legitimate new products, providing attackers with persistent, administrator-level control over the victim's hardware from the very moment of activation.

Banking-focused trojans are not the only kind of malware that is increasing, with Kaspersky also noting a marked increase in spyware and personal information stealing software.¹³ Such malware extracts sensitive documents, personal records, and live location from infected devices, making them a potent tool for extortion. There has also been a shift in who is being targeted in these spyware attacks. Earlier, cybercriminals focused on so-called "spray and pray" attacks, which were mass and indiscriminate in scale. Lately, though, the emphasis has been more on targeting large and sensitive organizations. High-value targets, known in the cybercriminal space as "big game" include power supply companies, hospitals and other essential infrastructure. These organizations cannot afford prolonged downtimes due to malware threats, which makes them more likely to pay a significant ransom amount.¹⁴

An often-overlooked reason for why malicious cyber-attacks are so prevalent in Pakistan is that software lifecycle management is almost non-existent in the country. Piracy and widespread use of unlicensed software, particularly outdated Windows operating systems, is normalized throughout all levels of

society. These outdated versions of software come with critical security vulnerabilities that are exploited by malicious actors. Other widely used pirated programs have also been routinely targeted, including Microsoft Office and VLC Media Player.¹⁵

Table 1: Major Malware Types Detected in Pakistan, January–September 2025

Malware Type	Number of Attacks Blocked	Primary Targets	Trend (Year-on-Year)
Banking Trojans	166,000+	Mobile banking users	+56% globally
Spyware	126,000	Government, corporate, individuals	Significant increase
Password Stealers	107,000	Individual users, enterprise	Persistent
Ransomware	42,000	Hospitals, SMEs, critical infrastructure	Shift to big-game hunting
Local (USB/Offline)	5.3 million (total)	27% of individual users, 24% of corporate	Stable
Web-Based	2.5 million (total)	16% of users, 13% of corporate	Stable

Source: Kaspersky data, Associated Press of Pakistan, November 15, 2025; Minute Mirror, November 14, 2025.

The Enforcement Gap and Socio-Economic Drivers

The past decade in Pakistan has witnessed an aggressive expansion and usage of e-commerce and online banking services. However, the majority of the population remains digitally illiterate and is therefore susceptible to scams by cybercriminals. In some surveys, as much as half of all respondents claimed to have experienced online financial scams and a significant portion also encountered multiple attempts in a single year.¹⁶ The official state body to resolve such complaints is the Banking Mohtasib, which has been successful in recovering

amounts lost to financial fraud in certain cases. Nevertheless, the recoveries only represent a meagre fraction of the total amount lost, and the majority of financial fraud victims never recover lost amounts.¹⁷

According to the NCCIA, more than 700,000 complaints were lodged from 2021 to 2025, but only 7,690 cases were registered, and the conviction rate was extremely low. This mirrors the systemic paralysis seen in prior years, such as the 57 convictions stemming from 147,200 reports in 2023, and the 51 convictions out of 128,400 reports in 2022.¹⁸

Among the reasons for the disparity in complaints and conviction rate is that cybercrime bodies face severe staffing shortages. In a country of almost 260 million people, there are roughly 350 full-time cybercrime investigators employed. This results in an impossible caseload for a single cybercrime investigator.¹⁹

The Legislative and Institutional Framework: Centralization, Control, and Controversy

Pakistan's cybersecurity legal framework remains centered around the Prevention of Electronic Crimes Act (PECA), 2016. PECA was instrumental in codifying specific cyber offenses such as electronic fraud, cyber stalking, online harassment, "cyber terrorism" into law, and also enabled the Pakistan Telecommunication Authority (PTA) to censor online content.²⁰ To serve as the state's primary body for investigating online offenses, the NCCIA was established in May 2024, effectively replacing the FIA's Cybercrime Wing.²¹ Since its start of operations, the NCCIA has expanded its footprint to 64 centres nationwide.

State-Level Threats: Hybrid Warfare and Infrastructure Vulnerability

The South Asian security environment has evolved to include state-directed cyber operations as a central component of military doctrine and narrative building. The cyber landscape in the region is threatened by so-called Advanced Persistent Threat (APT) groups, which maintain an operational blueprint on the wider regional network architecture. These APT groups do not operate as cybercriminals focused on financial scams. Rather, APT groups prioritize long-term strategic objectives over financial gains.

One of the more prominent APT groups that has targeted Indian government and defence entities is the APT36 group, also known as “Transparent Tribe”.²² An analysis of the Transparent Tribe’s 2025 campaigns highlights their usage of targeted phishing emails. These emails look legitimate, with their tone and content almost identical to official government correspondence. The goal of these emails is to trick the receiver, often an important person of interest, into installing a malicious set of tools on their device, which then allows their device and data to be compromised. Such tools have evolved over time to record real time keystrokes, provide webcam access and control the entire infected device digitally without the receiver ever knowing. APT36 is also known for not installing malware on a victim’s hard drive, as that can be detected by industry-standard antivirus software. Rather, legitimate Windows software programs are used to run malicious code directly using only RAM, making it very difficult to detect. The APT36 group also maintains the capability to target operating systems other than Windows, as was demonstrated in an August 2025 cyberattack that targeted computers running Linux.²³

Other APT groups, such as Side Copy, use psychology and “honey traps” to lure victims. Believed to be in operation since at least 2019, Side Copy is known for distributing malicious files that, when opened, display explicit pictures of women to distract the victim while malware installs itself in the background. The group’s name is actually a clever wordplay on the Sidewinder APT, which was known to target Pakistan’s military interests. Side Copy is also known by global cybersecurity firms, such as FortiGuard Labs, which revealed in 2023 that Side Copy malware was embedded in a file that referenced an under-development nuclear missile.

Taken together, these APT campaigns have become a well-funded and sustained part of the India-Pakistan strategic rivalry. Unlike the conventional warfare domain, where there exists significant asymmetry in capabilities, the cyber realm is much more fiercely contested. This is partly due to the nature of the cyber domain, where a comparatively weak state can leverage its digital infrastructure in a cost-effective way to project offensive and defensive capabilities in a disproportionate manner.

Mobile Surveillance and the Pegasus Threat

Servers and databases are not the sole targets of hostile cyber operations. Mobile smartphone devices, that are carried everywhere by heads of state, military officials and diplomats, are frequent targets of espionage. The most prominent

example is Pegasus, a surveillance tool developed by the Israeli firm NSO Group, which can infect a smartphone without the user's knowledge and covertly extract messages, photos, emails, call logs, and even activate the device's camera and microphone. Pegasus is sold exclusively to government end-users, and its deployment therefore represents a form of state-sponsored espionage that operates below the threshold of kinetic conflict yet directly targets the communications of a nation's leadership.

Pakistan's direct encounter with Pegasus became public in July 2021, when the Pegasus Project, a global investigation led by Forbidden Stories, Amnesty International, and a consortium of media outlets, revealed that a phone number linked to Prime Minister Imran Khan appeared on a leaked database of over 50,000 numbers selected by NSO clients for potential surveillance.²⁴ The official Pakistani response was swift and accusatory: the Foreign Office stated that the targeting had been carried out by Indian agencies, and the government declared its intention to seek a United Nations investigation and to explore legal action against NSO Group in the International Court of Justice.²⁵ The targeting of a sitting prime minister's communications, whether successful or merely attempted, underscored the ease with which highly invasive surveillance technology can be directed at a nation's most sensitive political centre, and it demonstrated that mobile devices have become prime strategic targets in South Asia's hybrid warfare landscape.

Investigations by research organizations have revealed that Pakistan too possesses commercial surveillance technology, such as automated facial recognition, which it has acquired from various international vendors. Confirmation of Pakistan's possession of potent spyware has come from formal authorities too, as the PTA disclosed in a 2024 court statement.²⁶ More worryingly, there has been at least one confirmed instance of spyware being deployed against Pakistani citizens, as noted by international watchdogs such as Amnesty International. This shows that while the state is often the victim of hostile cyber espionage from foreign powers, it has normalized the deployment of similar spyware platforms for domestic control.

Cyber-Physical Attacks on Critical Infrastructure

As the state began integrating its infrastructure for critical supplies with IT networks, it exposed itself to vulnerabilities that previously did not exist. Pakistan's primary energy provider, the PPL, was targeted by a sophisticated cyberattack in August 2025. A cyber group claiming to be "Blue Locker" compromised portions of

the PPL's network, leading to the temporary suspension of non-critical digital services.

While the breach did not result in data loss or loss of control of core PPL network components, the cyberattack was successful in creating widespread disruption even though the government had circulated a prior warning that public entities were under threat of imminent cyberattack. The primary reason Pakistan remains vulnerable to such attacks, despite prior intelligence of such threats, is that the security infrastructure of public service entities is outdated and not in line with international standards. A future intrusion could realistically affect water services, traffic light systems and telecommunications on a mass scale if the infrastructure is not upgraded.²⁷

The Cyber-Nuclear Security Dilemma

Independent observers have generally appraised Pakistan's physical security controls surrounding its nuclear assets as being both robust and reliable. However, as Pakistan has sought to digitize its command, control, communications, and early-warning networks.

This creates a unique security dilemma where the digitization, which was necessary to ensure that the leadership retains the ability to rapidly deploy nuclear weapons and maintain real-time situational awareness to make rapid decisions.

Digital Colonialism and the Sovereignty Challenge

In addition to conventional cybersecurity vulnerabilities, a broader structural risk Pakistan faces is "digital colonialism". Simply put, digital colonialism is the extraction, analysis, and ownership of user data for financial gain and market influence by foreign multinational technology corporations. As Pakistan lacks any sort of comprehensive data protection legislation its information ecosystem remains highly vulnerable to commercial extraction and monetization by Western technology firms.

Digital colonialism has an outsized effect on the running of Pakistan's administration. US-based applications such as WhatsApp, Zoom, and Google services are used for official government communications and business. The servers supporting these services are outside of Pakistan. Concurrently, the physical telecommunications infrastructure relies heavily on Chinese hardware vendors, primarily Huawei and ZTE. This creates a unique situation where Pakistan,

essentially, relies on Western countries for software and China for hardware. Because Pakistan is under the process of developing domestic alternatives, it is in a precarious situation where official communications are at risk of being exposed to foreign intelligence agencies via hardware and software vendors.

Individual-Level Threats: Data Breaches and Social Vulnerabilities

The Data Breach Epidemic: A Structural Failure of Protection

While state-level cyber operations target defence assets and diplomatic channels, civil-tier cyberthreats directly erode citizen trust in public digital platforms. Centralized state databases, designed to collect extensive biometric data across the population, have suffered recurring, large-scale breaches. These security failures highlight deep systemic vulnerabilities in data protection standards, operational hygiene, and institutional accountability across both public agencies and corporate data holders.

To further highlight the scale of these breaches, in May 2025, a security researcher discovered a database containing 184 million unique login credentials linked to Pakistani internet users.²⁸ As the file was unencrypted and publicly accessible online, it was possible for any anyone to download its contents. Cybercriminals had used a specific type of malware in order to steal information such as usernames, email addresses, and passwords from both international platforms such as Google, Microsoft, and Meta along with domestic and federal portals. While the National Computer Emergency Response Team (PKCERT) did issue an urgent, high-priority national advisory warning citizens about the leak. It had little effect on the leak itself. As the advisory did not remove the malware itself nor could it affect anything for users who either still had not changed their passwords or were unaware of the leak itself.

Such large-scale data leaks have become a consistent feature in Pakistan in the past few years. Between 2019 and 2023, data for roughly 2.7 million citizens was stolen from NADRA.²⁹ In 2025, phone records belonging to millions of individuals, including high-profile government officials, were put on sale across different dark-web marketplaces. While the PTA did block thousands of channels that were used by cybercriminals to advertise and sell these phone records, these measures were still only a stopgap solution. These data breaches, other than violating individual

privacy, have the potential to provide foreign intelligence with actionable information regarding key individuals within civilian and military leadership.

Financial Fraud and the Imperilled Cashless Economy

Widespread financial crime has significantly degraded Pakistan's push towards developing a digital banking system. This is further exemplified by the fact that between 2020 and 2024, FIA recorded over 700,000 cybercrime complaints, but was only able to secure 152 convictions.³⁰ In 2024, the courts were only able to produce verdicts in a total of 17 cases; this was from a total of 1212 arrests. Financial cybercrimes have become such a persistent issue that industry risk assessments by independent surveyors such as PricewaterhouseCoopers suggest that 90 percent of Pakistani banking executives classified cybercrime as a "very high" risk factor, with general fraud cited by 70 percent of respondents.³¹

Financial fraud in Pakistan usually occurs in two ways: (1) fraudsters will pose as bank personnel and trick account holders into revealing their login credentials, and/or One-Time Passwords (OTPs), and (2) cybercriminals will often use forged payment receipts on e-commerce platforms such as OLX or Facebook Marketplace to obtain products without actually transferring funds. Other than individual scams, financial crimes have evolved to the point where fraudsters have been using call centers in major cities to run Ponzi schemes.

The prevalence of financial crimes and their unchecked growth have considerably eroded public trust in any sort of modern, reliable digital banking infrastructure. This has systematically dented the state's goal of developing a "cashless" economy.

Technology-Facilitated Gender-Based Violence

In Pakistan, cybersecurity is a gendered issue that affects men and women differently. In 2024, the Digital Rights Foundation (DRF)'s cyber harassment helpline received a total of 3,171 complaints from across the country, with an average of 264 new cases each month. Cyber harassment was the most reported type of case, with 2,741 complaints, of which only 36 percent originated from cities where an FIA or NCCIA cybercrime wing is operational. Women reported 1,772 cases, and men reported 1,365. Adults between the ages of 18 and 30 were the most targeted group, with 1,774 cases.³²

The data indicates that women were disproportionately targeted through non-consensual intimate images (NCII) and image-based abuse (IBA), with

85 percent of NCII cases and 81 percent of IBA cases reported by female complainants. The rapid democratization of artificial intelligence tools has introduced a terrifying new dimension to this violence: perpetrators now use AI-powered applications to generate fake intimate imagery with minimal technical skill, weaponizing these forgeries for blackmail, humiliation, and reputational destruction.³³ The societal context magnifies the harm: conservative cultural norms tightly link a family's "honor" to the perceived chastity and modesty of its women, meaning that the mere existence of such imagery, even if known to be fake, can lead to social ostracism, forced marriage, or violence.

Journalists and religious minorities were also targeted: 121 cases involved journalists, and 124 cases involved members of religious minority communities.³⁴ While the law on paper has been strengthened, the 2022 PECA amendment specifically criminalized the non-consensual sharing of intimate images, enforcement remains profoundly weak.

Election Disinformation and AI Manipulation

The Pakistan General Elections of 2024 were one of the first instances in Pakistan that demonstrated the large-scale use of AI in order to influence voter perceptions and affect election outcomes. Political parties and their supporters used AI-generated deep-fakes in order to portray their opponents in misleading contexts. According to an analysis conducted on different social media sites by the DRF, out of 225 posts that they analysed 163 were categorized as deliberate misinformation.³⁵

In terms of social media spending, the Pakistan Tehreek-e-Insaf (PTI) emerged as the largest spender at PKR 25 million, with other political parties accounting for PKR 29 million. This expenditure only accounts for social media sites such as Facebook and Instagram, as other social media sites have not disclosed their advertisement revenues.³⁶ Political parties have also utilized WhatsApp as an avenue for sharing manipulated content and misinformation, primarily due to its ubiquitousness in Pakistan but also because of its encrypted nature. This makes it next to impossible not only to trace the source of the content but to provide any corrections. The DRF also noted that social media sites are often unwilling or unable to provide content moderation around elections not only Pakistan but also in other South Asian countries.

The Weaponization of Online Blasphemy and Minority Targeting

Recently, the internet, or rather social media, has become another avenue of danger for Pakistan's religious minorities. Religious extremists have exploited social media in order to level blasphemy accusations against religious minorities, which, because of Pakistan's volatile law and order situation coupled with a charged socio-cultural environment, have led to actual cases of death and destruction. This is further exemplified by the fact that the DRF's 2024 helpline data recorded 124 cases involving religious minorities.³⁷

Multiple documented cases have highlighted a combination of online incitement and mob violence. In March 2022, a doctored video falsely depicting a local politician making blasphemous remarks was circulated via WhatsApp. Within hours, an enraged mob attacked the politician's residence; a security guard attempting to protect the family was beaten to death.³⁸ In another incident, viral social media rumours about a child-kidnapping ring, a common moral panic in the region, led to the lynching of an innocent man in a village in Punjab.³⁹ The speed with which such content spreads through encrypted, trust-based networks, combined with the intense emotional charge of religious and child-protection themes, creates a situation in which the digital and physical worlds can combine with sometimes deadly results.

Policy Recommendations: A Governance-Centered Framework for National Cyber Resilience

To transition from fragmented, reactive cyber-defence to a resilient national security posture, Pakistan requires systemic institutional, statutory, and operational reforms. The following policy framework addresses governance overlaps, critical infrastructure vulnerabilities, and legal enforcement gaps identified across the national cyber-ecosystem.

- **Enact and Align the Personal Data Protection Framework:** Parliament must finalize and enact the Personal Data Protection Bill to establish clear, enforceable privacy standards across public and private sectors.
- **Define Agency Roles:** The federal government should establish clear roles and responsibilities for different agencies. The NCCIA should focus strictly on criminal prosecution, evidence gathering, and digital

forensics, while the PKCERT should focus on national cyberthreat monitoring, incident response, and CERT coordination.

- **Cybersecurity Laws Must Comply with International Standards:** Pakistan's cybersecurity laws should be consistent with laws and regulations developed by other democratic states. Hence, it is important that any legislative changes or updates should be reviewed by an independent judicial committee to ensure that the rules and regulations do not contravene individuals' rights of free speech and expression.
- **Enforce Baseline Cybersecurity Standards:** Cybersecurity vulnerabilities across critical infrastructure such as power grids, municipal water networks, and logistics hubs occur primarily due to unpatched SCADA and legacy OT systems. The Ministry of Information Technology and Telecommunication (MoITT) should mandate baseline compliance for all critical national infrastructure under the Pakistan Information Security Framework (PISF).
- **Automate Threat-Intelligence Sharing:** Public-sector security operations remain isolated from private threat intelligence which creates operational blind spots. PKCERT should develop a national Information Sharing and Analysis Center (ISAC) framework, enabling automated, real-time distribution of indicators of compromise (IoCs) across state agencies, telecommunications providers, and financial institutions.
- **Establish a Cybersecurity Career Track:** The federal government should create policies that incentivize individuals pursuing a career in cybersecurity for the public sector. Both the federal and provincial governments should also look at providing cybersecurity research grants for universities and using them to recruit talent.
- **Nationwide Cyber-Hygiene Initiatives:** Social engineering remains the most common initial access vector for both state-sponsored APTs and financial cybercriminals, making technical defenses alone insufficient. Expanding nationwide cyber-hygiene campaigns, supported by accessible, interactive learning platforms, can lower end-user vulnerability across digital banking networks and centralised citizen databases.

Conclusion

Pakistan's digital infrastructure is growing rapidly. However, currently, its cybersecurity approach is reactive as it is primarily focused on perimeter defence, i.e., firewalls and intrusion detection that only respond after an attack is detected. Instead, Pakistan needs a proactive, integrated national architecture, i.e., a coordinated system where policies, agencies, technologies, and threat intelligence work together across the whole country. Currently, Pakistan faces three major cyber challenges: (1) state-sponsored espionage, (2) critical infrastructure weaknesses in essential services like energy and transport, and (3) everyday digital crimes against citizens. However, the current legal response, such as expanding PECA, which has largely focused on controlling online content (e.g., removing objectionable posts), is inadequate.

Solving these issues requires a broader and more comprehensive series of reforms, both institutional and societal. Most modern states have developed their own versions of digital data protection laws, have clear guidelines regarding how different government bodies and agencies, related to cybersecurity, are to function, and provide incentives to individuals who wish to pursue a public career in cybersecurity. Only this integrated approach can build a resilient digital infrastructure that safeguards both national security and the privacy of citizens in a digital, interconnected world.

References

- ¹ "Pakistan's Internet Users Cross 120 million Mark," Dawn, March 15, 2024, <https://www.dawn.com/news/1812345>
- ² State Bank of Pakistan, Payment Systems Annual Review 2023 (Karachi: SBP, 2024), 22–28.
- ³ State Bank of Pakistan, Financial Inclusion Strategy 2025 Mid-Term Review (Karachi: SBP, 2023), 14–16.
- ⁴ "Pakistan Rises to Tier-1 Status in Global Cybersecurity Index," Daily Times, June 9, 2025, <https://dailymirror.com.pk/>; "Pakistan Ranks Among Top Countries in Global Cybersecurity Index 2024, Marking Significant Progress," Pakistan Telecommunication Authority, September 14, 2024, <https://www.pta.gov.pk/category/pakistan-ranks-among-top-countries-in-global-cybersecurity-index-2024,-marking-significant-progress-1485299784-2024-09-23>
- ⁵ "Joint Efforts Behind Pakistan's Cybersecurity Boost Hailed," Dawn, September 14, 2024, <https://www.dawn.com/news/>.
- ⁶ "PTA Dismisses SIM Data Leak Reports, Says Telecom Sector Secure," Minute Mirror, September 9, 2025, <https://minutemirror.com.pk/pta-dismisses-sim-data-leak-reports-says-telecom-sector-secure-434771/>; "Cybersecurity Agency Warns of Data Breach Affecting Over 180 Mln Pakistani Internet Accounts," Xinhua, May 27, 2025, <https://english.news.cn/>
- ⁷ Countering Cyber Threats in Pakistan: A Political Analysis of the National Cyber Security Policy (2021) And Whole, International Journal of Political Studies, accessed April 13, 2026, <https://ijpstudies.com/index.php/ijps/article/download/95/51,4-6>.
- ⁸ "Kaspersky Urges Stronger Online Safety," Associated Press of Pakistan, November 15, 2025, <https://www.app.com.pk/national/kaspersky-urges-stronger-online-safety/> "Kaspersky Urges Stronger Online Safety."
- ⁹ Kaspersky Urges Stronger Online Safety.
- ¹⁰ NCCIA Expanding Its Operations Across Country, NA Told," The News International, December 2, 2025, <https://www.thenews.pk/print/1384244-nccia-expanding-its-operations-across-country-na-told>
- ¹¹ "Kaspersky Urges Stronger Online Safety"; "Mobile Banking Cyberattacks Rise by 56pc in 2025: Report," Dawn, accessed April 13, 2026, <https://www.dawn.com/news/1978843>
- ¹² Kaspersky Urges Stronger Online Safety
- ¹³ Kaspersky Urges Stronger Online Safety.
- ¹⁴ "Pakistan Hit by Over 5.3 Million Cyber Attacks in Just 9 Months," Minute Mirror, November 14, 2025, <https://minutemirror.com.pk/pakistan-hit-by-over-5-3-million-cyber-attacks-in-just-9-months/>.
- ¹⁵ Kaspersky Urges Stronger Online Safety.
- ¹⁶ Visa, Consumer Survey on Digital Fraud in Pakistan, 2024, cited in "Pakistan's Digital Economy Plunges into Deep Crisis as Online Financial Frauds Soar," Lokmat Times, September 16, 2025, <https://www.lokmatimes.com/business/pakistans-digital-economy-plunges-into-deep-crisis-as-online-financial-frauds-soar/>.
- ¹⁷ "Surge in Complaints Against Digital Fraud," Dawn, April 22, 2025, <https://www.dawn.com/news/>.
- ¹⁸ "NCCIA Expanding Its Operations Across Country, NA Told."
- ¹⁹ "Pakistan's Digital Economy Plunges into Deep Crisis as Online Financial Frauds Soar."
- ²⁰ Government of Pakistan, Prevention of Electronic Crimes Act, 2016, Act No. XL of 2016.
- ²¹ "National Cyber Crimes Investigation Agency Notified to Deal with Offences Under Peca Act," The Nation, May 4, 2024, <https://www.nation.com.pk/>.
- ²² "Investigation Report: APT36 Malware Campaign Using Desktop Entry Files and Google Drive Payload Delivery," CloudSEK, December 13, 2025, <https://www.cloudsek.com/>; "APT36's Sneaky Malware Campaign Targeting Linux Systems," PCrisk, August 25, 2025, <https://www.pcrisk.com/>.
- ²³ Investigation Report: APT36 Malware Campaign," CloudSEK
- ²⁴ "Imran Khan's Mobile Number Among Those Spied Upon by India Using Pegasus, Says Shahzad Akbar," Dawn, July 25, 2021, <https://www.dawn.com/news/1636715>
- ²⁵ "Pakistan Accuses India of Targeting PM Imran Khan with Pegasus Spyware," The Express Tribune, July 25, 2021, <https://tribune.com.pk/story/231679/pakistan-accuses-india-of-targeting-pm-imran-khan-with-pegasus-spyware>.
- ²⁶ "PTA Chairman Says Malware Like Pegasus Can Compromise Phones in a Minute," Dawn, March 14, 2024, <https://www.dawn.com/news/1821170>

-
- ²⁷ “The New Reality of Cyber-Physical Risks in Pakistan,” Lockton MENA, accessed April 13, 2026, <https://global.lockton.com/mena/en/news-insights/the-new-reality-of-cyber-physical-risks-in-pakistan>.
- ²⁸ “PTA Dismisses SIM Data Leak Reports, Says Telecom Sector Secure.”
- ²⁹ “PTA Dismisses SIM Data Leak Reports, Says Telecom Sector Secure.”
- ³⁰ “Pakistan’s Digital Economy Plunges into Deep Crisis as Online Financial Frauds Soar.”
- ³¹ “Cybercrime Identified as Top Threat by 90% of Pakistani Bankers: PwC Survey,” Profit by Pakistan Today, November 26, 2024, <https://profit.pakistantoday.com.pk/>.
- ³² “3,171 Complaints of Tech-Facilitated Gender-Based Violence Reported in 2024: DRF.”
- ³³ “3,171 Complaints of Tech-Facilitated Gender-Based Violence Reported in 2024: DRF.”
- ³⁴ “3,171 Complaints of Tech-Facilitated Gender-Based Violence Reported in 2024: DRF.”
- ³⁵ “DRF’s Report Records Rampant Harmful Content Spread on Platforms During the 2024 Pakistan General Elections,” Digital Rights Foundation, December 20, 2024, <https://digitalrightsfoundation.pk/drfs-report-records-rampant-harmful-content-spread-on-platforms-during-the-2024-pakistan-general-elections-with-inconsistent-content-moderation-enforcement/>.
- ³⁶ “DRF’s Report Records Rampant Harmful Content Spread on Platforms During the 2024 Pakistan General Elections.”
- ³⁷ “3,171 Complaints of Tech-Facilitated Gender-Based Violence Reported in 2024: DRF.”
- ³⁸ “Blasphemy Rumors on WhatsApp Spark Mob Violence in Punjab,” BBC News, March 4, 2022.
- ³⁹ “Man Lynched Over Child Kidnapping Rumors on Social Media,” Al Jazeera, January 22, 2023.