Received: 10 July 2024, Accepted: 05 August 2024

Cyber Insecurity in Pakistan: Unregulated Spaces and Policy Vacuum

Muhammad Usman Ghani[1] M.M. Afnan[2]

1. Student of BS Political Science, Department of Political Science and International Relations, University of Management and Technology, Lahore. Email:F2021126011@umt.edu.pk
2. BSIR, (Graduate) Department of Political Science and International Relations, University of Management and Technology Lahore.Email: mianafnan111@gmail.com

Abstract

This study looks at the changing issues of cybersecurity in Pakistan with emerging threats, the level of institutional preparedness, and policies in mind. Using both primary and secondary datasets, the study highlights critical concerns regarding gaps and cyber defense enforcement, regulatory enforcement, and inter-agency collaboration in Pakistan's digital framework. A thematic and statistical analysis reveals underlying patterns of cybercrime, cyber threats at the level of the state, and the socio-economic consequences of insufficient cybersecurity infrastructure. The study assesses the policies for cybersecurity in Pakistan compared to the international benchmarks of best practices, identifying the need for legislative cyber defense gaps, revised policy frameworks with enforcement needs, advanced capacity building, and upgraded technologies. The most important findings reveal the gaps that Pakistan has commenced steps towards building further resilience in cybersecurity. Pakistan's accelerated rate of digital adoption requires more step and proactive integrated-adaption frameworks. The study noted governance frameworks for national cybersecurity strategy and policy collaboration gaps need to be addressed with comprehensive: governance strengthening, stakeholder collaboration, and advanced digital ecosystems aligned with emerging cyber threats.

Keywords: Cybersecurity in Pakistan, cyber threats,digital sovereignty, AI-driven security,national security, cyber resilience.

1. Introduction

Cyber-insecurity means being weak and vulnerable to attacks online, and puts people, companies, and even countries at risk. Perhaps some of the most serious risk factors for attacks in cyberspace include unguarded networks, outdated software, ignorance, and unregulated systems. Cyber-insecurity, though, is the most serious problem in the digital world today. It is the most serious problem in the digital world today, as it causes distrust and reduces confidence in online systems. Cyber-insecurity also has the potential to cause serious economic, political, and social problems. Though some actions that fall under the umbrella of "cybercrimes" require more sophisticated means, most of the illegal actions that can be accomplished using computers, the internet, or, for that matter, any digital accessories constitute cybercrimes. These actions include but are not limited to: hacking, phishing, holding one's data for ransom, impersonation, digital financial fraud, cyberespionage, cyberterrorism, and the dissemination of digital material that is illegal or does not comply with the law. Similarly, unlike conventional crimes, cybercrimes are extremely easy to commit as geographical barriers do not constrain the perpetrator. This is in addition to being easy to commit as they can be carried out from any remote place, and the anonymity they enjoy in the online world.The increasing use of mobile phones, online shopping, and the internet is transforming Pakistan socially and digitally. More than 130 million Pakistanis have internet access as reported by PTA in 2024 which is also enabling people to work remotely. The government is helping to advance digital infrastructure through "Vision Digital Pakistan" which seeks to promote better connectivity and e-government. All of these changes could significantly enhance economic growth and innovation, along with social participation. However, the pace of technological growth and adoption of new technologies creates gaps in the security infrastructure, increasing the risk in cyberspace.

Cybersecurity is the use of technology methods and practices to protect systems and systems networks from digital attacks, unauthorized access, or destruction (NIST, 2018). On a national level, cybersecurity goes beyond a technical issue since it also concerns policy and governance, public relations, and national security. It requires not only sophisticated technological security systems, but also a strong legal body, complex institutional coordination, a rational public, and wide public recognition.

In Pakistan, cybersecurity has developed into a matter of both national security and governance. The increased use of digital services in the country makes it more susceptible to cyber threats from both sides of the border. Such threats aim at penetrating sensitive areas like banking, defense, healthcare, and national databases. Due to the lack of a comprehensive and enforceable cybersecurity policy, PECA of 2016, some of these systems remain vulnerable. Although the PECA of 2016 offers some legal means to address some of the cyber offenses through electronic means, it attracts negative attention for focusing on overregulation on content rather than the infrastructure, digital rights, and proactive mitigation of threats (Khan, 2023).

Pakistan's cyber gaps stem from a lack of policy attention, which is a gap in Pakistan's expanding digital ecosystem, is not matched with the growth of regulating policies. The cybersecurity duties of Pakistan are divided amongst a few different departments the FIA, PTA, and NACTA. Each of these departments works in siloes which makes the gaps worse. Because of this lack of coordination, these institutions are stuck responding to cyber-attacks instead of proactively implementing prevention policies. The absence of clear guidance and a regulatory framework for Pakistan's digital infrastructure makes the country's system vulnerable to exploitation, cyber threats and incursions.You can see the effects of this policy gap across multiple sectors. There is often inadequate cyber protection for critical infrastructure like energy grids and the financial systems. Digital forensics is a highly specialized field that, for a variety of reasons, law enforcement and judicial agencies are unable to investigate and prosecute cybercrimes. Cybersecurity awareness campaigns are almost nonexistent, especially in rural and underserved communities, so people are more likely to be targeted by scams, phishing, disinformation, and other digitally fraudulent activities. Moreover, the lack of robust privacy and data protection policies means that the personal data and information of citizens can be easily exploited by hostile foreign governments as well as their own regardless of whether the information is sensitive or not. Academic institutions and research universities are more vulnerable to losing their sensitive information, data, and other forms of intellectual property, yet the few programs that do exist are solely focused on cybersecurity, a field where more specialized research and training is highly important. Within the region, Pakistan is particularly worried about cyber aggression from its neighbors in South Asia, including the use of cyber warfare as part of hybrid warfare. Even the promising technology startup ecosystem is hindered by lack of specialized aid for cybersecurity entrepreneurship.

This research adopts a thorough perspective in addressing these interconnected problems. It will analyze the gaps and flaws that define the cyber insecurity of Pakistan to understand the existing cyber insecurity gaps and weaknesses in the country. By looking into the gaps in governance, civic engagement, cyber law enforcement, public participation, and geopolitical considerations, the research sets out to portray the ungoverned gaps of Pakistan’s cyber landscape. Recent occurrences of data breaches and other cyber-attacks will be analyzed as case studies to demonstrate the importance of addressing these issues and gaps.

The **objectives** of this research are to:

1. Identify and analyze the key governance, legal, and operational gaps in Pakistan’s cybersecurity framework.
2. Assess the implications of these gaps for national security, economic stability, and public trust.
3. Recommend practical, context-specific measures to strengthen Pakistan’s cybersecurity governance and resilience.

The scope of this research is national in focus but considers Pakistan’s position within the wider South Asian cybersecurity environment. It examines vulnerabilities and governance issues across both public and private sectors, including critical infrastructure, financial systems, educational institutions, and emerging technology enterprises. By linking sector-specific findings to broader policy and governance considerations, this study emphasizes that Pakistan’s cybersecurity challenges are not isolated problems but part of a systemic and interconnected risk environment.

2. Existing Cybersecurity-Related Laws and Regulations in Pakistan

Pakistan’s cybersecurity measures are based on a few pieces of laws and regulations. The most important of these is the Prevention of Electronic Crimes Act (PECA) 2016. PECA was created to deal with cybercrimes, such as unauthorized access to information systems and electronic fraud. Under PECA, the Federal Investigation Agency (FIA) is granted primary jurisdiction to investigate these cybercrimes. PECA also focuses on criminal offenses of hacking, identity theft, cyberstalking and the distribution of malicious software (Government of Pakistan, 2016). PECA is also supported by other regulations from Pakistan Telecommunication Authority (PTA) related to internet governance, domain registration, and compliance by service providers. The Cyber Crime Wing of the FIA acts as the operational enforcement body of PECA and is responsible for the investigation of registered complaints, cyber investigations, and prosecutions.

Pakistan still does not have a single coherent national strategy on cybersecurity as a single cohesive law or strategy that brings everything together does not exist (Ahmad, 2022). Khan (2023) comments about PECA’s content regulation focus as a more reactive than strategic approach to building cyber defense capabilities. While useful to oversight telecommunications, PTA regulations are insufficient to address proactive preparedness, incident response frameworks, or include protection requirements for critical infrastructure on a sector-specific level. Also, Dawn (2023) highlighted that the Cyber Crime Wing of the FIA is severely understaffed, overworked, and has a limited reach outside of major metropolitan areas.

There is a stark contrast between empirical data and effective cyber governance. The FIA’s annual report (2023) states that 100,000 complaints of cybercrimes were filed across the country in 2022, there were only a handful of convictions. The majority of the time, delays in processes, lack of technical know-how, and jurisdiction issues stalled speedy resolution. Pakistan’s position is further frustrated by ranking 94 out of 194 countries in the ITU’s Global Cybersecurity Index (2021). This indicates systemic and operational weaknesses in the national cybersecurity infrastructure.

The Ministry of Information Technology and Telecommunication (MoITT) did create drafts for a National Cybersecurity Policy as recently as 2021, but none of them are fully enacted, legally binding policies. A draft from 2021 includes plans for a National Computer Emergency Response Team (NCERT), improving inter-agency collaboration, and expanding cybersecurity educational programs (MoITT, 2021). Still, there are no clear timelines, budgetary apportionments, or oversight structures provided. It seems that, as of mid 2024, most programs are still stuck in the design stage as no overarching body has been given the authority to mandate compliance in multiple domains.

Pakistan's cybersecurity framework is governed in a reactive manner, as there is no overarching policy. For example, responses to large scale cyber incidents such as the 2022 Meezan Bank phishing attack or the NADRA data leak have been handled in a reactive, short-term manner with no long-term, structural change implemented afterward. This disjointed strategy creates legal ambiguity for organizations, as there is no framework outlining their obligations. For citizens, it causes confusion regarding their entitlements, as well as the processes available to them to seek legal relief.

The lack of a national policy is sharply highlighted through comparative evidence. Countries like Singapore and Estonia have implemented strict cybersecurity frameworks that assign sectorial obligations, set minimum standard of safeguarding, as well as create a unified structure for crisis response command (Singapore Cybersecurity Agency, 2022; Ministry of Economic Affairs and Communications, Estonia, 2021). This clearly shows the difference between their comprehensive strategies and Pakistan's mid, fragmented and draft stage approach.

- **Governance Fragmentation and Overlap Institutional Divide**

The lack of cohesive Pakistan cybersecurity policy is driven most chiefly, by the overlap of institutions. Numerous bodies have claimed to hold partial jurisdiction over cyber-governance, however, jurisdictions lack any meaningful collaboration frameworks. Cyber Crime Wing of the Foreign Interference Agency (FIA) PEC Act investigations do not have direct jurisdiction over the telecommunication sector, which lies under the Pakistan Telecommunication Authority (PTA). At the same time, the National Counter Terrorism Authority (NACTA), who is responsible for addressing cyberterrorism, does so in complete isolation from both FIA and PTA. There are other specialized units too that are isolated from the international governance. The Inter-Service Public Relations (ISPR) Cyber Cell concentrates on armed forces-related cyber threats, and interacts very limitedly, to civilian cyber governance frameworks.

These divisions create a slow response time to incidents. In interviews with agency heads done by the Digital Rights Foundation (2022), the interviewees indicated that the coordination in between agencies is often "dependant on personal contacts" as opposed to set guidelines. Because of these gaps in rules and guidelines, in many situations, cyberattacks have been allowed to escalate with no intervention or assistance.

An example of this fragmentation is the 2020 cyberattack on K-Electric. After the ransomware attack on billing and customer services, initial reporting went to PTA, which then referred the matter to FIA. Because of the lack of a centralized control system, response efforts were fragmented, and critical services were still disrupted several days later (The News International, 2020).The divided structure worsens the lack of response in dealing with the cyber security laws and incidents as well as enforcing the laws in Pakistan. Because of divided responsibility, there is lack of jurisdiction which makes prosecution of criminals harder, especially those outside the borders. In case the civil aviation authority needs to initiate the case, there is a chance that military agencies become the command authority. This created a long delay in response time, and in turn, there was lack of cooperation from the private sector because no one was certain about the reporting obligations.

The issue is made worse by the limitation of resources of different institutions. The FIA Cyber Crime Wing, for instance, has just a few hundred trained staff across the country, most of whom are not trained in advanced digital forensics (FIA, 2023). Likewise, the PTA lacks specialized incident response teams because, while they track network activity, they do not have the specialized units needed for high-level networks. Therefore, Pakistan’s approaches to cyber threats tend to be reactive attempts to minimize damage instead of proactive approaches to minimize risk.

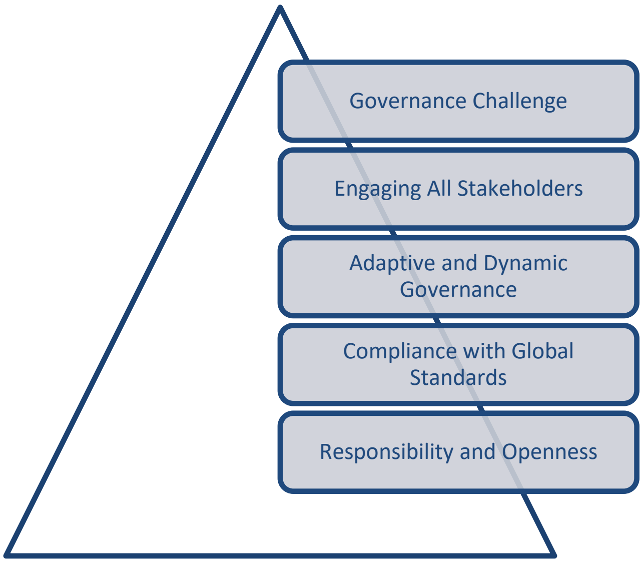
According to the World Bank (2022), cybercrime cost the economy of the country roughly USD 1 billion every year in lost business, data breaches, and damage to its reputation. Because there is not a centralized national plan, the businesses have to create their own cybersecurity systems, which is usually done without the necessary technical know-how or market standards.

Pakistan's cybersecurity setup now faces problems such as, legislative gaps, gaps within institutions, and reactionary enforcement to issues. PECA 2016, along with the PTA regulations and the FIA Cyber Crime Wing provide a basic enforcement framework, but does not create a cohesive, integrative national strategy. Without a cybersecurity unifying strategy, critical infrastructures, private businesses, and citizens are exposed to a wide range of threats. Responsibilities of the FIA, NACTA, PTA, and other relevant bodies with cybercrime concern intersect which adds to the chaos, making the information timely and reliable, slowing down action, and making the citizens distrust the system. Underreported cybercrime statistics and the lack of response to high profile incidents provide proof that without adequate governance, and enforceable jurisdictional cybersecurity laws, Pakistan will continue to face increased cyber risk.

3. Cybersecurity Governance Theory

The Cybersecurity Governance Theory offers a framework for understanding how countries, organizations, and other bodies formulate, execute, and govern protective policies on information systems and technology infrastructure. Further, it highlights that cybersecurity concerns, and challenges extend beyond technology and include governance issues, and requires accountability systems, governance frameworks, and collaboration from across different sectors. The Theory was developed in the late 2000's at the same time as the growing realization that cyber threats pose dangers to national security, the economy, and societyand go beyond the IT business.

The key contributors to the Cybersecurity Governance Theory include Donner & Kent (2015), who explained the alignment of policies through the interrelation of national policies and global standards, Weissbrot& Galli (2017) who provided insights on the human rights aspects of cyber governance, and Baldwin & Cave (1999) whose prior work on regulation provided the basis for understanding cyber governance as part of the wider regulatory governance theory. More recently, Klimburg (2017) advanced the concept of 'cybersecurity ecosystems', making the case for the integration of the technical, legal, and institutional components in governance. All these scholars put forward the notion that good governance relies on a combination of top-down control through laws and policies, and bottom-up participation from the civil society, industry, and academia.


Governance Challenge
Engaging All Stakeholders
Adaptive and Dynamic Governance
Compliance with Global Standards
Responsibility and Openness

Developed By Authors

The theory is based on a few underlying assumptions:

Cyber Security as a Governance: ChallengeCybersecurity threats cannot be solved by technologic efforts only, there needs to be policies, laws, and governance frameworks to deal with cyber issues.Engaging All Stakeholders Governance is only effective with the inclusion of every government, private sector, international organization, and the general populace.Adaptive and Dynamic Governance Because cyber threats are changing, governance frameworks also need to be changed and have the capability to bounce back.Compliance with Global Standards Strategies instigated by nations to ensure security of their cyberspace should be in accordance with global policies and agreements aimed at dealing with cross-border cyber threats.Responsibility and Openness Sustainable cyber governance needs the public to have trust in the governance structure, in addition to defined roles, controls and oversight.

These assumptions broaden the discussion beyond "cybersecurity as a technical issue" to a comprehensive approach that blends legal, institutional, political, and social aspects.

This research looks at cybersecurity in Pakistan focusing on emerging governance gaps that have been under-studied. Applying Cybersecurity Governance Theory addresses the concern of the Technical-Policy Divide by framing cyber threats as IT risks and also as institutional and strategic crises. The cyber law PECA 2016, the National Cybersecurity Policy 2021, and other pertinent and subordinate laws have shaped Pakistan's current cybersecurity framework. Pakistan's cybersecurity framework PECA 2016 and National Cybersecurity Policy 2021 are based on the governance theory's assumptions. However, in addition to reliance on multi-stakeholder collaboration, the theory also lacks international norm alignment.

4. Protection of Critical Infrastructure in Pakistan

The critical infrastructures like power systems, banking systems, defense facilities, national databases, and health services are the backbone of Pakistan's security and economy. They are also of national importance. Along with the growing digitization of services, these systems are more vulnerable to cyber threats. Lack of strong sector-specific cybersecurity policies, a functioning national Computer Emergency Response Team (CERT), and a national cybersecurity strategy leaves these systems exposed to both state-sponsored and criminal cyberattacks. The lack Pakistan faces regarding cybersecurity for its critical infrastructures is not imaginary. Recent incidents highlight the governance, technical defenses, and incident response shortcomings and systemic vulnerabilities.

The smart meters, SCADA systems, and IoT devices are digitizing Pakistan's energy infrastructure, including smart grids, oil and gas pipelines, and hydropower facilities. These upgrades aid with operational efficiency, but like the National Electric Power Regulatory Authority (NEPRA) mentions in 2022, these improvements also make systems more vulnerable to cyber-attacks.

SCADA systems are especially useful to attackers since they manage important systems like electric and gas operations. A cyberattack on such systems could result in rotational blackouts, halting industrial operations and damaging delicate machinery. In 2020, K-Electric, the largest power utility in Pakistan, suffered a ransomware attack which disabled billing services for more than a week (The News International, 2020). Although no physical destruction was sustained, the attack demonstrated a failure in the redundancy and real-time monitoring of critical energy systems.

The oil and gas sector faces similar situations. A report by Digital Rights Foundation (2022) indicated that some oil pipeline monitoring systems have no firewalls, allowing threat actors searching for weak points to access them through the internet. Because of the area's ongoing geopolitical conflicts, such vulnerabilities may be taken advantage of by not only cybercriminals, but also by hostile state actors.

As the landscape of banking shifts to mobile banking and digital transactions, business makes them a key target for cyber criminals. Adoption of RTGS systems and interfacing with international financial messaging systems like SWIFT, has positioned banks not only to domestic, but also to multi-national cyber-crime syndicates.

BankIslami became the victim of Pakistan's first major SWIFT cyberattack in 2018, resulting in the loss of USD 6 million through international transfer fraud (State Bank of Pakistan [SBP], 2019). The attack was caused by compromised SWIFT terminals and exposed layers of poorly implemented endpoint security, gaps in staff training, and endpoint security. In 2022, phishing scams against clients of Meezan Bank showed that social engineering still poses the highest threat to banking credentials (CERT-PK, 2022).

After that incident, the State Bank of Pakistan issued new cybersecurity guidelines which included mandating penetration tests, multi-factor authentication, and mandatory incident reporting (SBP, 2022). Smaller banks without in-house dedicated cybersecurity teams still pose a problem, as lower tier banks have weak defenses and there remains no sector-wide, real-time threat intelligence sharing mechanism. Lessons from breaches are not systematically disseminated to all institutions.

- **Threats to National Databases and Defense Systems**

Cybersecurity threats to Pakistan's defense infrastructure have dire national security ramifications. Details of the military’s cyber defense capabilities are mostly classified, but there have been reports of foreign intelligence and hacker groups attempting to breach communication and surveillance system defenses (FireEye, 2021). Such breaches can threaten satellite imagery, control of weapons systems, troop movements, and more.Another area of concern includes national databases like the ones held with the NADRA, which have been noted as high value targets in the past. Media reports claim information about citizens held with NADRA was being sold in dark web forums in 2021. NADRA was claiming there was no breach of information. Experts claim the no mandatory security audits done from outside parties makes ensuring these databases safe unfeasible, therefore leaving room for speculation (Khan, 2022).

The overseeing bodies have also flagged the cybersecurity of e-governance systems like the FBR’s online tax filing, as FBR’s servers went offline for a short duration due to some online attacks which forced them to suspend services online, remotely extracting information (Dawn, 2021) as a e-governance system. These events emphasize the combination of military and non-military structures to have cyber-attacks tame controlled by having sophisticated monitoring systems and undertake exploration of ongoing weaknesses.

The health care system of Pakistan is seen as one of the fronts not being well protected in the new debates about cybersecurity. The information systems of Pakistan are increasingly being digitized with new systems like Tele health and various EHRs in Pakistan. EHR systems contain some of the most sensitive information about patients like health history, identification number, and their health insurance details.

In 2022, cybersecurity experts found gaps in the security of certain hospital management systems in Pakistan, which compromised patient data because of weak authentication methods (CERT-PK, 2022). A cybersecurity breach in this sector can lead to the compromise of patient privacy which can also put them in risk if essential systems like diagnostics, imaging, or surgical scheduling are tampered with.

One of the gaps in the Pakistan government's cybersecurity efforts is the lack of efficiency in the country's Computer Emergency Response Team also known as CERT. CERT-PK is part of Pakistan Telecommunication Authority [PTA] but functions as a purely advisory body, notifying stakeholders about prospective threats. It has a "tick box" approach and does not engage in proactive real-time problem solving, forensic analysis, and multi-sector collaboration (MoITT, 2021). On the other hand, Malaysia and South Korea has CERTs that work hand in hand with the government and private sector and helps them spring into action when cyber emergencies arise (APCERT, 2022). Because Pakistan does not have these proactive measures in place, cyberattacks, particularly targeting critical infrastructure, faces disorderly and slow responses. This is extremely risky for the energy and defense sectors where downtime, even for a minute, can severely impair operations and pose significant security risks.

In Pakistan, infrastructure systems are important for the economy, but they are exposed to numerous cyber security problems, such as ransomware in the energy sector, SWIFT hacks in the banking systems, espionage against the defense systems, and even healthcare systems that leak patient data. The absence of a fully operational national cyber security incident response team (CERT) immensely enhances the problem of incident response being reactive and compartmentalized. The response to sector-specific cyber threats remains reactive, and, even though there are some protective guidelines the response is very weak and compliance is not checked through independent audits. One of the biggest problems Pakistan faces is the cyber security lack of response plans, in which systems that are connected to each other, and cyber threats are capable of changing other systems. There are countless experts warning that national security alongside public wellbeing is in danger. The only way the critical infrastructure of Pakistan can be protected is through a well-defined cyber security policy which, alongside, integrates solid central frameworks to control the ever increasing and advanced cyber-attack threats.

5. Cybercrime & Digital Forensics in Pakistan

Cybercrime in Pakistan has changed from a simple act of defacing websites in the early 2000s to more complex financially and politically charged attacks. With more than 124 million broadband subscribers (PTA, 2023), the internet in Pakistan has created new avenues for cybercrime. Ransomware, phishing, identity theft, and online fraud are a few examples of the rise of cybercrime in Pakistan. The PECA law from 2016 does offer some means to tackle cybercrime, there are still gaps in the ability to investigate and successfully prosecute such crimes. Lack of trust in law enforcement agencies dealing with cybercrimes, coupled with gaps in forensic technology further complicate the issues.

Phishing, a type of cybercrime, has become a major issue in Pakistan and now targets users of online banking, e-commerce, and even government services. CERT-PK has reported a notable increase in phishing scams replicating Bank and Mobile services, targeting not only customers but even government aids such as the Ehsaas Cash Program (CERT-PK, 2022). Generally, these attacks trick users into providing sensitive information which allows the scammers to carry out unauthorized activities in the victim's account.

Over the years, ransomware incidents targeting both public and private organizations have risen. In 2020, K-Electric was hit with a ransomware attack by the NetWalker group, who demanded $3.8 million in Bitcoin for access to the systems (The News International, 2020). While the ransom was reportedly not paid, the attack highlighted operational disruptions and critical service provider vulnerabilities.Phishing financial fraud is evolving into more advanced forms, including sophisticated social engineering and card skimming. Operating in Karachi and Lahore, multiple ATM skimming networks were reported and taken down by the FIA Cyber Crime Wing in 2021 (FIA, 2021). These operations were often global in nature and utilized compromised card readers to collect customer information.

The incidents that do take place tend to go unreported, and Pakistan in specific suggests significantly lower numbers. Victims often decide not to report cases due to lack of trust in law enforcement, fear of reputational damage, or lack of knowledge of reporting systems (Digital Rights Foundation, 2022). It's significantly the case involving financial fraud, and then personal blackmail. Victims, mostly women especially, fear the social stigma that comes with involving authorities (Baloch & Hassan, 2020).

Unlike urban centers, rural regions hardly know about the complaint portal and helpline which the FIA Cyber Crime Wing set up. As highlighted by Haq (2021), more than 60% of participants in smaller towns did not know about any formal avenue to report online scams. This lack of reporting distorts the true picture of cybercrime in the country which makes it more difficult to policymakers to formulate tailored prevention and enforcement actions.

Cybercrime investigations require a well-defined infrastructure alongside digital forensics expertise (the process of collecting, preserving, analyzing, and presenting digital evidence in a law court). Although the regional forensic laboratories set up by the FIA Cyber Crime Wing are a step in the right direction, the scope and technology limitations for them are troubling. Numerous reports suggest that these facilities lack sophisticated tools for memory forensics, deep packet inspection, and even encrypted data analysis (Hussain & Aslam, 2022).Most forensic labs are operating with limited budgets, resulting in using older hardware and software tools. For example, a parliamentary committee report in 2022 noted that some regional offices continued to use older imaging devices that could not accept solid-state drives or cloud-based storage (National Assembly of Pakistan, 2022). In addition, the ability to conduct mobile device forensics, which is crucial for many cybercrime investigations, is limited to a few urban centers, leaving many parts of the country underserved.

The FIA Cyber Crime Wing of Lahore illustrates this problem with a case study: In the 2021 ransomware case, manual log review and device imaging took over three weeks to complete. In the course of that time, some volatile pieces of evidence were re-supplied due to system reboots (FIA internal report, as cited in Hussain & Aslam, 2022). So, the company's automated systems and tools which could have done the data analyses and identifications were decades behind and were not in place.Again, the lack of automation affects the chain-of-custody protocols. Defense lawyers could claim that the digital evidence had been altered and thus contaminated. Because of this, the defendant can easily state that this evidence was tampered with in some way and therefore should not be brought before the court. This has primarily led to an extremely low conviction of cybercrimes, with estimations at 10% (Baloch & Hassan, 2020).

The combination of rising cybercrime rates and chronic underreporting alongside a lack of digital forensics skill creates a constant cycle of risk. This, in combination with a lack of underreporting cybercrime, serves a heightened lack of investment for the problem. The scarcity of cyber forensics tools and the lack of personnel, cyber forensics tools and personnel, means that even the reported cyber forensics cases encounter a lot of delays due to lack of skilled personnel, which greatly reduces the chances of cybercriminal prosecution. Due to lack of punishment, cybercriminals lack deterrence which erodes trust in the cybercrime institutions.In addition to lack of a investment for the problem, there is also international security risks. In cases involving cyber espionage, attack on critical infrastructure, due to slow forensic cyber forensics times, there is always a lot data lost, missed chances to identify the data, and missed chances to engage in timely measure's countermeasures to the attack.

In Pakistan, cybercrime is getting worse both in scale and complexity. This is fueled by greater internet access and the increasing use of technology in daily activities. The major threats include phishing scams, ransomware attacks, and online and financial scams, though the real damage goes much deeper due to chronic underreporting. Law enforcement and investigative agencies face numerous assets, including outdated technology, manual extraction methods, and sparse regional coverage, which struggles to keep up with the digital forensic infrastructure. Investing in public awareness and automated forensic tools, as well as improving funding and inter-agency cooperation, can close such gaps.

6. Cybersecurity Awareness & Digital Literacy

Being careful and informed online, as well as having good digital skills, helps in protecting a nation from cyber threats. Even though the internet is more accessible in Pakistan and people are using the internet more, the level of awareness of online safety practices among the government employees, people living in the rural areas, and small businesses is extremely low (Shah & Khan, 2022). Not only does this lack of awareness result in undercutting the protection of people and organizations from cyberattacks, but it also contributes to the failure of achieving the intended goals of the nation's cybersecurity policies and strategies. This problem is made worse with the fact that Pakistan has one of the lowest digital literacy rates in the region, coupled with a lack of organized programs aimed at educating the population about cybersecurity (PTA, 2023).

The cyber vulnerabilities facing Pakistan are particularly acute in small and medium-sized enterprises (SMEs) partly due to a lack of formal training and an informal IT support system (Hussain et al, 2021). Like many small business owners, SMEs are generally unaware of basic digital safety measures such as two-factor authentication, phishing email detection, and secure data storage protocols. Consequently, they are easily targeted by ransomware and online fraud campaigns, suffering significant financial and reputational damage. Similar vulnerabilities are present in government offices, particularly at the district and municipal levels, as the staff work with little to no cybersecurity training, greatly heightening the chances of data breaches and interruption of services to the public (NR3C, 2022).

The problem is much worse in rural areas because of the lack of infrastructure and education. A lack of quality ICT infrastructure coupled with a lack of trained teachers means that rural people often do not have the necessary skills to detect and manage cyber risks (World Bank, 2021). People in such situations are much more vulnerable to digital fraud, misinformation, and social engineering scams, which could have widespread effects. For example, during election periods and public health campaigns, digitally uneducated people are unable to assess the accuracy of online information and, therefore, the distribution of manipulated content and fake news is rampant (Zubair & Ahmad, 2023).

There is a clear and direct link between lack of digital literacy and greater vulnerability to phishing, identity theft, and other cybercrimes, including cyber misinformation (Ahmad et al., 2020). Along with misguiding the public, misinformation also risks destabilizing social cohesion, disrupt social order, tamper with election results, and erode faith in democratic governance. Without adequate digital literacy, people are less able to check the credibility of a source, question the source of the content, or check the information against reliable databases. This lack of skills allows many people, both from within the country and outside, to freely spread misinformation that targets and harms the political, economic, or security interests of the nation.

Filling in these gaps requires cyber security awareness to be integrated in the education and training system vertically through all levels and phases of the education system, commencing from the primary level upwards. Some experts propose that primary and secondary education include basic digital literacy modules like password hygiene, safe browsing, privacy settings, and recognizing online scams (United Nations Educational, Scientific and Cultural Organization [UNESCO], 2021). Gaining these skills at a young age helps ensure that younger generations will have at least a foundational grasp of cyber security when they eventually join the workforce. Along with these skills, adult populations such as government officials and small business owners require mandatory training workshops and e-learning modules to address ever-changing foundational cyber security threats.In addition, campaigns at the community level and at the grassroots level also need to be activated to improve the gaps in knowledge at the community level. These campaigns should also include television, radio, social media, and publications in local and ethnic languages to reach a broader audience. In the case of rural areas, awareness sessions organized by NGOs as well as local government and telecommunication offices could greatly improve the outreach of such community campaigns. These campaigns must be tailored to local cultures or else they run the risk of losing interest and failing to be understood.

As this example shows, the government is very important when it comes to coordinating and financing these projects. Even though the PTA and NR3C have started public advisories and reporting systems, the consistency and scale of these efforts is nowhere near enough to address the ever-increasing threat landscape (PTA, 2023). There is still the possibility of a public-private partnership in which telecom companies, technology companies, and NGOs come together to market and have an impact on a wider scale. International development partners could also be invited to fund pilot testing programs that incorporate cybersecurity into the training of development and poverty alleviation programs.

Raising and improving awareness on cybersecurity and digital literacy goes far beyond just a technical problem. It is a social problem. Through these responsibilities, Pakistan would be able to minimize cybercrimes, strengthen the country’s protections against misinformation campaigns, and cultivate responsible digital practices. In this day and age, the cybersecurity practices of every individual, including city-dwelling businessmen and country-dwelling agriculturists, impact national security, economic health, and the resilience of democracy. Not taking action, as is the case now, would result in a loss of value, and degradation of public trust in initiatives meant to enable a digital economy.

7. State Surveillance vs. Citizen Privacy

In Pakistan, there is a conflict between state surveillance and citizen privacy, concerning the balance of security and human rights. In the last ten years, Pakistan’s law enforcement and intelligence agencies have gained the ability to monitor people’s digital communication through the use of advanced surveillance technologies, like spyware, geofencing, and data monitoring systems (Khan, 2022). Even though these tools are deemed necessary for counterterrorism, cyber, and public safety, the lack of proper governance puts privacy, civil liberties, and possible abuse of authority at risk.

Research and exposed files indicate that Pakistan might have tried to obtain advanced spyware similar to Pegasus that can hack smartphones, read encrypted messages, and turn on microphones on devices without the user knowing (Amnesty International, 2021). These features enable state agencies to circumvent legal frameworks, which would normally be required to keep them under scrutiny, and conduct surveillance on politically opposing figures, journalists, activists, and the general public. Moreover, geofencing, the technology which sets virtual borders for mobile devices to be tracked, has been reported to be used during the pandemic both in the security operations and public health tracking (Nabi, 2022). Though useful for dealing with crowds in certain situations such as the rapid response to emergencies, the unchecked use of geofencing could lead to the establishment of systems for constant surveillance.

The legal grounds allowing for such surveillance is mostly based on Prevention of Electronic Crimes Act (PECA) 2016. Though PECA was meant for dealing with cyber-crime, some of its clausesespecially 29, 30 and 32grant certain powers to commanding user data from service providers, using wiretaps on conversations, and intercepting communications without telecommunications companies (Digital Rights Foundation, 2022). Even though the Act claims these provisions must be used for the “interest of national security” or “public order,” these are vague and open-ended terms which can be used to justify almost anything. In addition, the lack of clear processes for requesting surveillance and the absence of an independent agency to oversee these matters intensifies the suspicion that PECA provisions can beand have beenused for political purposes instead of operations meant to protect the state.

Pakistan’s legal structure is missing many things, however the lack of an effective law on data protection is most notable. A Personal Data Protection Bill has been attempted many times since 2018, yet it is still waiting for acceptance within Parliament (MoITT, 2023). The attempts to resolve the issue has shown some degree of progress, like granting consent to data holders to share the information, restriction on data sharing for a set period of time, and penalties for sharing data without permission. Rights protection groups however, have voiced their disapproval on some parts of the bill, which allows government bodies to exempt themselves from compliance due to security reasons, which removes protections for people from government intrusion (Baloch & Qureshi, 2021).The current surveillance methods being used in Pakistan raise severe human rights concerns. As pointed out by the UN Human Rights Council (2021), privacy stands out on its own as a right, but also acts as a gateway to various other rights like freedom of expression, freedom of association, and the right to a trial. The phenomenon of unchecked surveillance leading to a chilling, or self-censorship effect, has been documented in Pakistan among journalists, human rights activists, and everyday citizens fearful of discussing politics online (Freedom Network, 2022).

Other countries have set more advanced regulations which serve to highlight Pakistan's shortcomings. The General Data Protection Regulation (GDPR) in the European Union places severe restrictions on private and public data collection, requiring legal and user approval of surveillance. The Privacy Act and PIPEDA also places strong accountability rules on federal agencies and corporations in the handling of private information (Office of the Privacy Commissioner of Canada, 2020). Pakistan’s current legal framework on state surveillance lacks justification as well as the scope and scale of surveillance being conducted.

Striking a balance between privacy rights and national security considers legal changes, responsibility, and involvement from society. Trust needs to be established as the government must consider the swift passing of a Data Protection Act while the private sector must also view it as a priority. There are also non-negotiables as there need to be allowances for national security. There has to be comprehensive independent data protection authorities as there must be audits on the overreaching scrutiny and also on the transparency reports. There needs to be defined limits as there also needs to be an independent review ballot of the request surveillance and transparency.

Authority that protects regional data and oversees request needs to be independent. Democracy and other civil societies need to bridge the gap, as private security and extensive overreaching needs to protect everyone. There also needs to be comprehensive media coverage so there can be coverage that needs to be addressed so revisions can be completely addressed. So on the road to comprehensive change to data rights, there needs to be defined changes to protect everyone. There also needs to be limits imposed so that there also be coverage that has defined limits.

In today’s world, where information can be both beneficial and a potential risk, especially for a country like Pakistan, the main issue is formulating a plan that protects its citizens from unnecessary government spying and cybersecurity dangers at the same time. The lack of well-defined borders brings a risk of surveillance evolving from a focused security measure into a tool for oppression, which can lead to the breach of trust in democratic systems and, in the end, undermine the society it is intended to safeguard. Pakistan’s digital resilience in the future will necessarily rely on achieving this finely tuned equilibrium between security needs and encroachment on constitutional freedoms.

8. Cybersecurity in Educational Institutions

Schools and universities in Pakistan are using digital platforms for managing academic activities, conducting research, and communicating, and are streamlined using academic management software. This automation reduces work overload, saves time, and improves efficiency, but comes with risks for cybercrimes. Due to the critical user information like student details, payment records, and exam results, cybercriminals are more inclined to strike educational institutions for personal gain (Shah, 2021). In addition, many universities also maintain large intellectual property and sensitive information research repository databases from collaborative projects, including those in defense, engineering, and medical sciences.

In 2020, there was a reported data breach of Punjab University and Virtual University where students' records were exposed on the dark web forums (Cybersecurity Association of Pakistan [CAP], 2021). UMT (University of Management and Technology) has been a leader in the promotion of AI education, research, and implementation in Pakistan. UMT has prepared students for the future AI-integrated workforce through academic activities, collaborations with the industry, and even student-led initiatives. A key milestone in these efforts was the Techverse mega three-day event aimed at bridging the academic and industrial gaps. This event was aimed at experts, students, and professionals to collaborate, discuss the practicability of AI in the industry, forge partnerships, and work towards the solutions of the problems. The same trend can be observed in Pakistan, where many campuses lack advanced tools and regular vulnerability assessments.

Research labs linked to Pakistani universities are also in jeopardy, especially those working on high-value or dual-use technologies. Weak cyber security systems give state and non-state actors the ability to exploit research data for commercial or strategic advantage. Cybersecurity analysts reported phishing attacks against faculty members working on health sciences during the COVID-19 pandemic with the aim of stealing vaccine data (Nabi, 2021). Such attacks not only undermine academic integrity but also weaken the country's global standing in the field of science and technology.

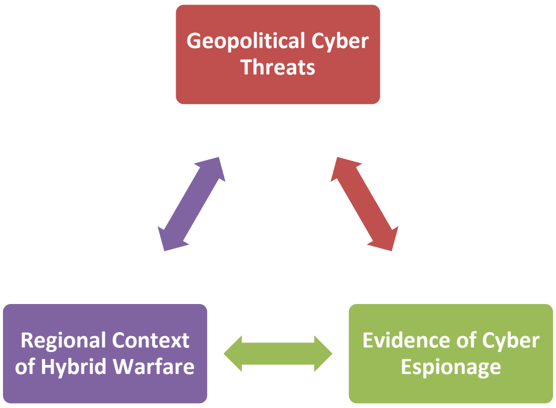
A lack of specialized cybersecurity education in Pakistan's academic landscape, coupled with a lack of funding for research, has greatly widened the gap in the nation's cybersecurity defenses. A handful of universities, like the National University of Sciences and Technology (NUST) and COMSATS, offer information security courses, but there are very few, if any, dedicated undergraduate or graduate programs in cybersecurity (HEC, 2022). In addition, funding for research in the field of cybersecurity, when compared to other STEM fields, is exceptionally low. This inability to develop homegrown security technologies and expertise hinders the country's ability to develop a talented workforce that can deal with changing cyber threats.

Collaboration between industries and academies is still developing. In more advanced countries with established cyber defense systems, collaborations that involve universities, tech firms, and government agencies have been vital in driving innovation, providing intelligence on industry threats, and developing professionals in the field (OECD, 2020). In Pakistan, some private sector initiatives, like the Ignite National Technology Fund's incubation center support, do show promise. However, they do not align with the requirements of cybersecurity education and applied research. Due to the lack of organized internship-based work, joint research projects, and established knowledge transfer systems between industry and academia, most graduates leaving universities are not equipped with experience in active cyber defense.

To solve these issues, a combination of different methods is needed. Educators should enforce minimum cybersecurity hygiene, such as requiring multi-factor authentication, regular penetration tests, and encrypted backups of academic databases to secure sensitive academic information. The Higher Education Commission could act as a leading figure by enforcing minimum cybersecurity compliance standards with grant allocations specifically directed toward cyber research projects. Simultaneously, industry-academia collaborations through hackathons, sponsored labs, and joint research and development programs would improve cyber defense capabilities and enhance graduate employability.

Pakistan’s Regional Cyber Defense Capabilities

The cybersecurity situation in Pakistan can only be understood in light of the world politics surrounding the country. It is located in a region characterized by deep-rooted conflicts, cross-border terrorism, and a digitally advanced theater of war. Cyber hostilities from India, Afghanistan-based actors, and other regional foes have progressed from basic website defacement to advanced espionage and hybrid warfare (Mustafa & Khan, 2022).


Geopolitical Cyber Threats
Regional Context of Hybrid Warfare
Evidence of Cyber Espionage

Developed By Authors

The most advanced and relentless cyber threats to Pakistan stem from groups associated with India. Cybersecurity firms like Recorded Future and Group-IB have attributed APT36 (Mythic Leopard or Transparent Tribe) to longstanding campaigns aimed at penetrating the Pakistani government and its defense and diplomatic institutions as advanced and persistent attacks (Recorded Future, 2021). These campaigns frequently consist of spear phishing emails with harmful appendices meant to exfiltrate sensitive files, track communications, and infiltrate institutions focused on sensitive military technology.

Non-state actors from Afghanistan have also been implicated in cyber intrusions aimed at Pakistan’s border security and government systems, especially during periods of heightened tensions (Shahzad, 2021). These activities are minimized and opportunistic, exploiting weaknesses in public-facing government systems and limited, yet disruptive capabilities like DDoS attacks on Pakistani government portals.

Pakistan’s relationship with China has both pros and cons, particularly as China seemingly ramps up its cyber presence in the region. China has economically partnered with Pakistan and provides technological support under the China-Pakistan Economic Corridor (CPEC) initiative. Yet, China’s extensive cyber espionage capabilities on its own and abroad prove that Pakistan must guard its networks even from allies in order to protect sensitive data.

In the past decade, there have been multiple documented incidents of cyber espionage targeting Pakistan. Amnesty International’s 2020 report confirmed the use of spyware tools on Pakistani journalists and political activists, indicating that either the state or its proxies were potentially involved (Amnesty International, 2020). Also, the cyber security company Malwarebytes published a report about an ongoing effort to target Pakistan military officials with malware that was embedded in Android apps, which claimed to be secure communication tools (Malwarebytes, 2021).

Such operations as the ones described demonstrate the use of fluently spoken local languages, cultures, and social engineering to exploit the success rate of intrusions. The collected data from these operations can be leveraged to influence operations and for intelligence-gathering in both peacetime and conflict scenarios.

The combination of conventional military strategies, cyber operations, disinformation, and other forms of irregular tactics is referred to as hybrid warfare. In South Asia, this is has become one of the defining characteristic features of its security landscape (Rizvi, 2022). In regions such as Pakistan, the cyber dimension of hybrid warfare is often coupled with kinetic and psychological operations. A case in point is the 2019 Pulwama-Balakot crisis where cybersecurity experts recorded disinformation campaigns aimed at Pakistani defense officials and citizens as well as phishing attacks during the crisis. These campaigns were aimed at fostering public distrust towards state institutions as well as interstate relations and spying (FireEye, 2019).

A similar situation is observed where lower-level social media accounts amplify narratives portraying Pakistan’s military as the perpetrator of sectarian violence, lied about military administration, and fabricated countless stories about governance failure. Hybrid Warfare is aimed with the intent of disrupting social harmony, deepen polarization, and weaken domestic morale.

Pakistan lags behind its neighbors India, Iran, and China in cyber defense and technology integration. India’s cyber defense and offensive capabilities are advanced. Their National Critical Information Infrastructure Protection Centre (NCIIPC) and Defence Cyber Agency provide a structured framework for cyber readiness (Bansal, 2021). Iran has equally strong, albeit heavily sanctioned, cyber capabilities supporting domestic control and international cyber conflict, including against Israel and Saudi Arabia (Clarke & Knake, 2020). China is one of the strongest cyber powers in the world, distinguished by advanced APT units and extensive domestic R&D in the field of cybersecurity. China is also home to well-known threat actor groups, APT10 and APT41, recognized for their international espionage activities (Muncaster, 2021).

Pakistan is actively working on bridging these gaps which includes establishing the Cyber Security Centre under the Pakistan Air Force's Centre of Artificial Intelligence and Computing (CENTAIC) and more recently drafting the National Cyber Security Policy (2021). However, the lack of collaboration between various offices like Federal Investigation Agency (FIA) and the Pakistan Telecommunication Authority (PTA) or National Counter

Terrorism Authority (NACTA) which operate independently, still makes it difficult to form a unified strategy on Pakistan’s cyber defense systems (Khan & Rehman, 2022).In addition, the lack of a fully operational national Computer Emergency Response Team (CERT) hinders Pakistan’s capability to swiftly monitor, analyze, and respond to potential threats from other countries. Compared to India’s CERT-In or Iran’s Maher CERT, Pakistan's capability to respond to cyber incidents is mostly passive. The response is an action taken without or after the event occurs instead of anticipating the event and taking steps proactively. The response to cyber incidents is mostly without collaboration between the private and public sectors and inadequate sharing of threat intelligence.

9. Finding and Analysis

Governance of Cybersecurity in Pakistan takes place in multiple institutions, each functioning with a specific goal and mandate but lacking significantly in multiple capacities. Under the PECA Act of 2016, the Federal Investigation Agency, through the Cyber Crimes Wing, still remains the foremost organization in charge of investigating cyber-crimes. Many studies have shown that just in the year of 2022 alone, the FIA received upwards of 100,000 registered cybercrime complaints, and the range of these complaints varied, including but not limited to, financial crimes and harassment (Dawn, 2022). There is, however, a struggle with outdated equipment and a diluted workforce, which is why it is often said that these institutions have a lack of technical capacity. There is also a lack of prosecution with the number of convictions which is troubling in its own regard, and it also highlights the lack of correlation that information and documentation have with prosecution (Khan & Ahmad, 2021).

Among other things, the Pakistan Telecommunication Authority (PTA) is primarily responsible for the regulation of digital content and telecom operators, as well as the regulation of the telecom data that is in transit. Expressing the aggressive regulatory attitude, the PTA blocked 1.3 million URLs between the years 2016 to 2021 (PTA, 2021). Despite these efforts, the authority has received backlash due to the inability to focus on cyber defense, as well as the inability to block encrypted VPN traffic that emphasizes the systemic issues in the country’s cyber defense laws (Hussain, 2020).

The National Counter Terrorism Authority (NACTA) has a certain degree of involvement when it comes to online extremist propaganda. As the 'Cyber Counter Terrorism and Investigation Report,' suggests, it has ties with the FIA when it comes to the monitoring of terror financing and the recruitment of extremists within the cyberspace (NACTA, 2021). Regardless, the chronic underfunding and bureaucratic obstacles on NACTA’s capacity to create a digital unit are unlimited. Less than a quarter percent of NACTA’s annual budgets, which are significantly less than 1% global cyber defense expenses, are allotted for operational activities (Ahmed, 2022).

Pakistan’s nascent Computer Emergency Response Team (CERT) has been mentioned in the National Cyber Security Policy 2021, but it has been described as ‘underdeveloped.’ When compared with India and Iran, Pakistan does not possess a functioning National CERT in charge of responding to incidents and sending real-time alerts. Its operationalization has been delayed due to the lack of specialized technical skills and the absence of a consolidated cyber threat intelligence platform (Shah, 2022).

The National Database and Registration Authority has blamed breaches on foreign hackers, claiming sensitive biometric data on over 220 million citizens has been compromised. Such concerns were raised, for instance, when NADRA sponsored records were found surfacing on the dark web in 2021. From what we can tell, e-governance NADRA has become indispensable in. They lack infrastructure audits or transparent methods. This, combined with aging information technology systems, automates the likelihood of insider and espionage threats much worse. This centers around external defense capabilities (Ali & Rauf, 2022). For instance, provincial police act as the lowest, front-line responders to reports of electronic fraud or harassment. Regrettably, this lack of technological resources is commonplace throughout police systems, and branches of the FIA have to do the legwork and more technical parts of an investigation. In 2022, The Punjab Police supposedly were responsible for receiving 25 thousand reports of electronic harassment, with less than a five percent solution and service margin. This more forensics needed were police resources, as the lack of training personnel needed to issue forensic scans is also very limited (The Punjab Police, 2022).

Table: Comparative Overview of Cybersecurity-Related Institutions in Pakistan developed by Authors

Institution	Core Function	Cybersecurity Role	Strengths	Challenges
FIA (Federal Investigation Agency)	Investigates crimes, including cybercrime, human trafficking, and terrorism	Operates Cybercrime Wing under PECA 2016; runs forensic labs	Nationwide investigation powers; experience in law enforcement	Underfunded, lack of modern tools, low manpower for cyber cases
PTA (Pakistan Telecommunication Authority)	Regulates telecom, internet, and digital services	Enforces internet regulations, data protection, and content monitoring	Strong regulatory mandate; growing ICT budget	Criticized for censorship; lacks advanced cyber defense capacity
NACTA (National	National	Integrates cyber	National	Bureaucratic

Institution	Core Function	Cybersecurity Role	Strengths	Challenges
Counter Terrorism Authority)	counterterrorism policy and coordination	dimensions of terrorism (cyber-terrorism, propaganda)	scope, high-level policy role	delays, limited direct operational capacity
CERT (Computer Emergency Response Team – NR3C / National CERT)	Responds to cyber incidents and vulnerabilities	Detects, responds to, and mitigates cyberattacks	Technical expertise; links with international CERTs	Still evolving, lacks independent budget and large-scale infrastructure
NADRA (National Database & Registration Authority)	Manages citizen identity database and digital ID	Protects biometric and national database against cyberattacks	Advanced IT infrastructure, biometric expertise	Target of frequent hacking attempts, needs stronger encryption/security
Police (National / Provincial)	General law enforcement and public safety	Local cybercrime reporting, first-response, coordination with FIA	Nationwide reach, grassroots accessibility	Low technical expertise, lack of training and digital forensics tools

10. Conclusion & Recommendations

Cybersecurity in Pakistan is still developing, and faces challenges like not having enough policies in place, limited funding, and a lack of awareness among the general public. Although the attacks on cyber infrastructure, and other like state-sponsored and ransomware attacks, are becoming more advanced, there is still a lack of strategic and proactive policy responses. Without a fully developed National Cybersecurity Framework, there are many gaps in coordination, incident reporting, and resilience-building within government and private organizations. The existing cyber laws PECA 2016, focuses on prosecution and lacks a focus on proactive risk management.One of the growing weaknesses today is the absence of a single system for responding to incidents. In the absence of a fully operational nationwide Computer Emergency Response Team (CERT), Pakistan’s cybersecurity incident detection, response, and recovery capabilities are significantly limited. In addition, the country has not adopted a comprehensive data protection law which aligns with global practices, thus exposing citizens' data to breach, misuse, and unauthorized transfers. Moreover, the general public's knowledge regarding the basics of cybersecurity is minimal, which poses a greater risk of phishing, identity fraud, and disinformation.

Policy recommendations

- **Improving Institutional Capacity and Budgeting**

Cybersecurity governance in Pakistan is struggling with fragmented mandates. FIA's Cybercrime Wing has a lack of technical proficiency, and other institutions such as NACTA and the Police are understaffed. It is recommended that the government increase the budget for cybersecurity institutions and accountability for how the funds are spent. Khan (2023) suggests that budgets for FIA, Police, CERT, and NACTA would allow for the hiring of experienced professionals, the acquisition of contemporary digital forensics equipment, and 24/7 operational readiness.

- **Creation of a National Cybersecurity Authority**

Difficulties in coordination result from overlapping responsibilities of the Police, PTA, FIA, CERT and NADRA. A National Cybersecurity Authority should be formed to streamline the legal and operational skeleton of these government branches. This body would be in charge of national threat data collecting, synchronizing, and coordinating policies to inter- and intra-agency communication and minimize overlap.

- **Formulating a Law for Data Protection and Privacy**

Biometric data in NADRA's control is sensitive and could lead to data misuse and breaches because of loose legal restrictions. Pakistan needs to enact a data protection law based on the EU's GDPR. Such a law must have clear lines of accountability, consent requirements, and a siloed data protection body. Trust on the government would be improved, provision of data subject to protection would be cross national, and the citizens' digital identity would be protected.

- **Promoting Academic-Industry Collaboration and Public Awareness**

Cyber-crimes in Pakistan are facilitated by poor digital literacy. There is a need for television, school, and the internet-based campaigns to improve understanding of the digital space. At the same time, Government and Universities should collaborate to create an academic industry partnership that would help develop local skills in digital forensics, artificial intelligence driven cyber defense, and sharing of cyber threat intelligence. This would isolate the country from foreign dependency in providing the country a sustainable strong cyber defense workforce.

References

Ahmad, S. (2022). Cybersecurity policy in Pakistan: Challenges and opportunities. Journal of Information Security Studies, 14(2), 45–58.

Ahmad, S., Khan, R., & Malik, A. (2020). Cybercrime and the challenge of digital literacy in Pakistan. Journal of Information Security Studies, 12(2), 45–59.

Amnesty International. (2020). Cyber surveillance of journalists and activists in Pakistan. Amnesty International.

Amnesty International. (2021). Uncovering the Pegasus project: How spyware targets activists and journalists. Amnesty Tech.

APCERT. (2022). Asia Pacific Computer Emergency Response Team annual report 2022. APCERT.

Baloch, I., & Qureshi, S. (2021). The need for comprehensive data protection laws in Pakistan. Pakistan Journal of Law and Society, 4(2), 55–69.

Baloch, S., & Hassan, T. (2020). Cybercrime prosecution challenges in Pakistan. Pakistan Journal of Criminology, 12(3), 45–60.

Bansal, S. (2021). India’s evolving cyber capabilities. Strategic Analysis Journal, 45(3), 221–238.

Bytes for All. (2021). Cyber harassment helpline annual report 2021. Islamabad: Bytes for All.

CERT-PK. (2022). Cybersecurity advisory reports 2022. Islamabad: Pakistan Telecommunication Authority.

CERT-PK. (2022). Cybersecurity incident report 2022. Islamabad: Pakistan Telecommunication Authority.

Clarke, R. A., & Knake, R. (2020). The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats. Penguin.

Cybersecurity Association of Pakistan. (2021). Annual cyber threat landscape report. CAP.

Dawn. (2021, August 15). FBR servers hacked, online services suspended. Dawn News.

Dawn. (2023, May 5). FIA struggles with rising cybercrime complaints. Dawn News.

Digital Rights Foundation. (2022). PECA and its impact on digital rights in Pakistan. DRF Reports.

Digital Rights Foundation. (2022). Policy brief: Cybersecurity governance in Pakistan. Lahore: DRF.

Digital Rights Foundation. (2022). Policy brief on cybercrime reporting in Pakistan. Lahore: DRF.

Europol. (2021). Internet organized crime threat assessment 2021. The Hague: Europol.

Express Tribune. (2021, October 5). NADRA data allegedly up for sale on dark web. Express Tribune.

Federal Investigation Agency. (2023). Annual report 2022–23. FIA Cyber Crime Wing.

FIA. (2021). Annual performance report 2021. Federal Investigation Agency, Cyber Crime Wing.

FireEye. (2019). Cyber threat intelligence: South Asia. FireEye Threat Research.

FireEye. (2021). Cyber threat intelligence report: South Asia. FireEye.

Freedom Network. (2022). Annual press freedom report: Pakistan.

Government of Pakistan. (2016). Prevention of Electronic Crimes Act, 2016. Islamabad: National Assembly of Pakistan.

Higher Education Commission. (2022). Curriculum review for computing disciplines. Government of Pakistan.

Haq, R. (2021). Public perception of cybercrime reporting in rural Pakistan. Journal of Rural Studies, 38(4), 112–125.

Hussain, M., & Aslam, S. (2022). Digital forensic capabilities in Pakistan's law enforcement. International Journal of Cybersecurity Policy, 6(2), 78–94.

Hussain, M., Raza, H., & Ahmed, T. (2021). Digital readiness and cybersecurity awareness in Pakistan's SMEs. Pakistan Journal of Commerce and Social Sciences, 15(1), 112–127.

International Telecommunication Union. (2021). Global cybersecurity index 2021. ITU.

Jisc. (2020). Cyber security posture of higher education institutions. Jisc Reports.

Khan, A. (2022). State surveillance in Pakistan: Legal frameworks and challenges. Journal of Security Studies, 15(1), 33–49.

Khan, A., & Rehman, F. (2022). Institutional fragmentation in Pakistan's cybersecurity governance. Pakistan Journal of Security Studies, 8(1), 55–72.

Khan, M. A. (2022). Cybersecurity challenges in Pakistan's public sector. Journal of South Asian Security Studies, 4(1), 34–49.

Khan, M. A. (2023). Regulating cyberspace in Pakistan: Policy and practice. Asian Journal of Public Policy, 15(1), 88–104.

Malwarebytes. (2021). Transparent Tribe targets Pakistani military with new Android spyware. Malwarebytes Labs.

Ministry of Information Technology and Telecommunication. (2021). National cybersecurity policy (draft). MoITT, Islamabad.

Ministry of Information Technology and Telecommunication. (2023). Draft Personal Data Protection Bill. Government of Pakistan.

Muncaster, P. (2021). China's cyber espionage strategy and capabilities. Infosecurity Magazine.

Mustafa, Z., & Khan, M. (2022). Geopolitics of cyber warfare in South Asia. Asian Security Review, 12(4), 99–118.

Nabi, M. (2021). Cyber threats to academic research during the COVID-19 pandemic. Asian Journal of Cybersecurity, 5(2), 41–53.

Nabi, M. (2022). Geofencing and mass surveillance in Pakistan: Emerging concerns. South Asian Journal of Technology Policy, 7(3), 88–102.

National Assembly of Pakistan. (2022). Standing Committee on Information Technology and Telecommunication: Report on cybersecurity infrastructure. Islamabad.

National Response Centre for Cyber Crime. (2022). Annual cybercrime report. Federal Investigation Agency.

NEPRA. (2022). State of the industry report 2022. National Electric Power Regulatory Authority.

OECD. (2020). Fostering industry-academia partnerships for innovation. OECD Policy Brief.

Office of the Privacy Commissioner of Canada. (2020). Privacy laws in Canada. Government of Canada.

Pakistan Telecommunication Authority. (2023). Cybersecurity initiatives in Pakistan. PTA Publications.

Pakistan Telecommunication Authority. (2023). Telecom indicators. Islamabad: PTA.

Recorded Future. (2021). Transparent Tribe's ongoing operations. Recorded Future Insikt Group.

Rizvi, H. (2022). Hybrid warfare in South Asia: Challenges and responses. Journal of Defence & Strategic Studies, 15(2), 75–94.

SBP. (2019). Report on BankIslami cyber incident. State Bank of Pakistan.

SBP. (2022). Guidelines on cybersecurity controls for financial institutions. State Bank of Pakistan.

Shah, A. (2021). Data privacy concerns in Pakistan's academic sector. Journal of Information Security Studies, 9(1), 23–38.

Shah, N., & Khan, F. (2022). Digital inclusion and cybersecurity in developing economies. Asian Journal of Digital Development, 9(4), 233–248.

Shahzad, U. (2021). Cyber threats from Afghanistan-based actors. South Asian Cybersecurity Review, 6(3), 31–44.

Singapore Cybersecurity Agency. (2022). Singapore cybersecurity strategy 2022. Singapore: CSA.

The News International. (2020, September 10). K-Electric hit by ransomware attack. The News.

United Nations Educational, Scientific and Cultural Organization. (2021). Digital literacy in education: Policy guidelines. UNESCO.

United Nations Human Rights Council. (2021). Right to privacy in the digital age. UNHRC Report.

World Bank. (2021). Bridging the digital divide in Pakistan. World Bank Group.

World Bank. (2022). Cybersecurity and the digital economy in South Asia. Washington, DC: World Bank.

Zubair, M., & Ahmad, N. (2023). Disinformation and digital illiteracy in Pakistan: A case study of rural communities. Journal of Media and Communication Studies, 15(3), 189–205