CASS
LAHORE

# MASS DIGITALISATION AND CYBER SECURITY: THREATS AND WAY FORWARD FOR PAKISTAN

Naba Fatima

Centre for Aerospace and Security Studies, Lahore

# MASS DIGITALISATION AND CYBER SECURITY: THREATS AND WAY FORWARD FOR PAKISTAN

Naba Fatima

Centre for Aerospace and Security Studies, CASS Lahore

July, 2024

# ABSTRACT

This study examines the cyber security threats confronting the people of Pakistan at the grassroots level and their impact on national security. The primary object of this research is to indicate the role of cyber illiteracy, imported Information Communication Technologies, and cyber security policy gaps in exposing the masses to cyber threats. This paper finds that these indicators lead to financial frauds, identity thefts, malwares, and digital harassment. The large scale prevalence of these problems poses a threat to national security by creating social unrest and economic instability. It also assists malicious groups in spreading misinformation, propaganda, and paves the way for terrorist activities. Therefore, this paper recommends a holistic approach to revamp Pakistan's cyber infrastructure, invest in local IT sector, implement bottom-up digital literacy programmes, and incorporate Privacy Enhancing Technologies (PETs) in critical infrastructure. It concludes that by addressing these areas, Pakistan can consolidate its digital infrastructure and ensure its security in cyber domain.

**Keywords:** Cyber literacy, Indigenous Information Communication Technologies, Data Protection Laws, Cyber Protection

# TABLE OF CONTENTS

# List of Figures



# List of Tables

# 1. INTRODUCTION

Over the past two decades, public and private sectors have undergone consequential digitalisation in Pakistan[1]. With over 100 million internet subscribers, the use of digital tools has become widespread among the population[2]. However, this rapid digitalisation heavily relies on imported Information Communication Technology (ICT) which poses substantial risks to Pakistan's digital infrastructure through embedded malwares, backdoors, and compromised cyber chips[3]. To address cyber security issues, the National Cyber Security Policy 2021 and the National Security Policy 2022 were introduced. However, these policies lack an inclusive approach for the predominantly cyber-illiterate population of Pakistan which is being exploited by cyber-criminals and malicious groups.

This paper argues that Pakistan's rapid digital transformation has not been accompanied by sufficient cyber literacy which is leading the masses to financial fraud, privacy breaches, misinformation, and blackmail. Since the introduction of 3G/4G licences in 2013, the pace of digitalisation has accelerated due to the efficiency and affordability of internet access. Today, digitalisation is trigging changes in services sector which is expanding digital infrastructure across various domains and exposing the public to cyber world without sufficient knowledge of cyber safety.

---

[1] State Bank of Pakistan, "Digitization of Services in Pakistan," *State Bank of Pakistan Annual Report 2017-18*, 2018, https://www.sbp.org.pk/reports/annual/arFY18/Chapter-07.pdf.

[2] "Pakistan - Cybersecurity," International Trade Administration | Trade.gov, January 12, 2024, https://www.trade.gov/country-commercial-guides/pakistan-cybersecurity#:~:text=Like%20other%20markets%2C%20the%20cybersecurity,terrorism%2C%20vandalism%2C%20and%20pornography.

[3] Aadil Nakhoda, "Propelling the ICT Sector via Imports of IT Products," *The Express Tribune*, May 20, 2024, https://tribune.com.pk/story/2467349/propelling-the-ict-sector-via-imports-of-it-products.

The fluid nature of cyber technology, for instance, the anonymity offered by Dark Web and the rise of Artificial Intelligence in cybercrime has enabled minimally skilled individuals to engage in sophisticated malicious activities. Concurrently, cyber illiteracy has rendered the general population more vulnerable to these threats. Although the parliament of Pakistan has enacted the Prevention of Electric Crimes Act (PECA) of 2016[4], the absence of a data protection law allows service sector to request personal data including CNIC numbers which is then misused by cybercriminals[5].

Some of the most evident sectors in exasperating this issue are e-commerce, e-governance, e-banking, and digital media[6]. In e-commerce, consumers are using digital payment methods which are leading to data leak and financial thefts. Similarly, e-governance and e-banking initiatives are being exploited by cyber criminals for scams and blackmail. On digital media, socially marginalised groups and women are harassed, leading to social unrest. This study hypotheses that the gap between cyber threats and cyber security measures needs to be bridged to prevent social unrest and financial insecurity which are critical aspects of national security of Pakistan. Therefore, the paper recommends that to enhance Pakistan's cyber resilience and protect its digital future a combination of local ICT development, adoption of advanced privacy technologies, international collaboration, and stringent policy enforcement is required.

This study is categorised into eight sections, including an introduction and a conclusion. The second section provides a brief overview of digitalisation in Pakistan to

[4] Majlis-E-Shoora, *Prevention of Electronic Crimes Act Bill*, 2016, https://www.na.gov.pk/uploads/documents/1470910659_707.pdf.

[5] Sindhu Abbasi, "PAKISTAN&Rsquo;S WEB OF CYBER SCAMMERS," *DAWN.COM*, July 16, 2023, https://www.dawn.com/news/1764628#:~:text=Out%20of%20the%20respective%20totals,2021%20and%201%2C392%20in%202022.&text=cyber%20harassment%20complaints%2C%20but%20it,2021%20and%20500%20in%202022.

[6] State Bank of Pakistan, "Digitization of Services in Pakistan," *State Bank of Pakistan Annual Report 2017-18*, 2018, https://www.sbp.org.pk/reports/annual/arFY18/Chapter-07.pdf.

highlight major sectors prone to cyber threats. It then delineates four major cyber threats: financial frauds, malwares, identity theft, and digital harassment that are exasperating the vulnerabilities of the people of Pakistan. The fourth section analyses the rise of cyber-crime alongside increased digitalisation. This is followed by the impact of cyber insecurity of the people of Pakistan on the national security of Pakistan covering economic instability, digital dependence, espionage, terrorism, and propaganda. The paper then identifies policy gaps and issues in the current cyber-security measures taken by the government. Lastly, policy recommendations are provided with a conclusion to summarise the findings of the research.

## 2. DIGITALISATION IN PAKISTAN: A GLIMPSE

Digitalisation is a process of incorporating digital tools and technologies in daily life. It includes converting manual systems, processes, and information into digital formats to improve accessibility, efficiency, and connectedness[7]. The driving force of digitalisation is expansion of internet connectivity, availability of digital tools, and fiscal advantages[8]. Figure 1 shows a timeline of digitalisation process in Pakistan.

[7] Arifur Rahman et al., "Exploring Transformational Head Teachers' Practices of Digitalization in the Primary School," in *Advances in Educational Technologies and Instructional Design Book Series*, 2023, 76–106, https://doi.org/10.4018/979-8-3693-1826-3.ch007.

[8] Arifur Rahman et al., "Exploring Transformational Head Teachers' Practices of Digitalization in the Primary School," in *Advances in Educational Technologies and Instructional Design Book Series*, 2023, 76–106, https://doi.org/10.4018/979-8-3693-1826-3.ch007.

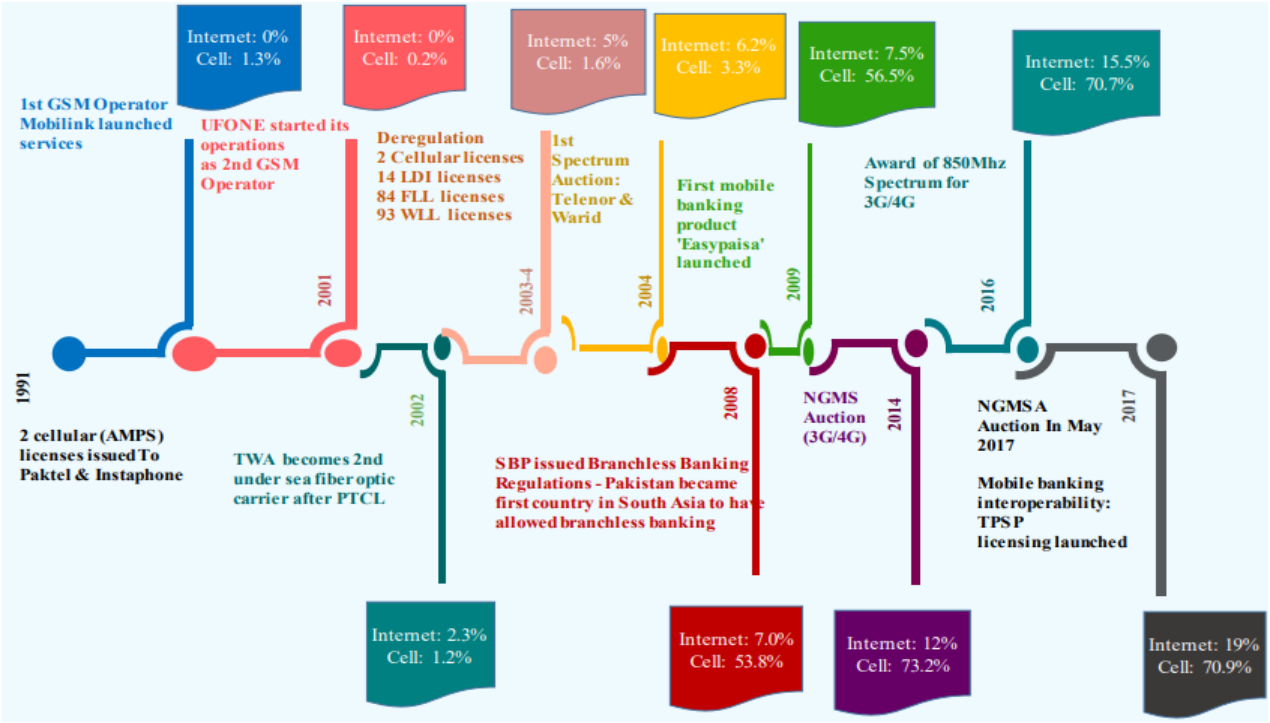


Figure 1: Timeline of Digitalisation in Pakistan[9]

The process of digitalisation began in Pakistan during 1980s with the governmental initiative to promote computer literacy and IT infrastructure. However, significant strides were made in 1990s with the embankment of internet connectivity and telecommunication[10]. In 1991, Pakistan took a constructive step towards digitalisation with the launch of its first GSM Operator Mobilink. At the same time two cellular (AMPS) licences were issues to Paktel and Instaphone[11]. After twenty years, in 2013 the introduction of 3G/4G licences increased the pace of digitalisation due to efficiency and

[9] State Bank of Pakistan, "Digitization of Services in Pakistan," *State Bank of Pakistan Annual Report 2017-18*, 2018, https://www.sbp.org.pk/reports/annual/arFY18/Chapter-07.pdf.

[10] Omar Qureshi, "The Transformative Role of Information Technology in Pakistan - Stratheia," Stratheia, February 29, 2024, https://stratheia.com/the-transformative-role-of-information-technology-in-pakistan/.

[11] State Bank of Pakistan, "Digitization of Services in Pakistan," *State Bank of Pakistan Annual Report 2017-18*, 2018, https://www.sbp.org.pk/reports/annual/arFY18/Chapter-07.pdf.

cheap accessibility of internet[12]. Today, digitalisation is trigging changes in the services sector which is leading to expansion of digital infrastructure in every domain. The shift is most evident in e-commerce, fintech, and e-government[13].

## 3. Cyber Threats and Vulnerabilities

In this digital era, one constant truth is that everyone will experience a security breach at some point[14]. This includes, encountering charges on credit cards, accidently downloading a virus, or having personal information stolen in a data breach. Despite concerted efforts by the government, significant cyber-security challenges persist in Pakistan. Following are some critical cyber threats that are affecting the personal and financial security of masses, exasperating cyber vulnerability of Pakistan.

### 3.1 Financial Frauds

In Pakistan, with digitalisation, financial frauds have become a prevalent type of cyber threat to the people of Pakistan. Between 2016 and 2019, there has been a 71 percent increase in e-banking users from 24 million to 42 million. Meanwhile, according to the cyber wing of Federal Investigation Agency (FIA), in 2022, 100,000 cybercrime complaints were received amongst which 40 percent were of financial frauds[15]. It indicates the gap between digitalisation of banking sector and cyber safety measures. It

[12] Ministry of Planning, Development & Special Initiatives "P" block Pak-Secretariat, Islamabad, Pakistan., "Ministry of Planning, Development & Special Initiatives," n.d., https://www.pc.gov.pk/web/press/get_press/1129.

[13] State Bank of Pakistan, "Digitization of Services in Pakistan," *State Bank of Pakistan Annual Report 2017-18*, 2018, https://www.sbp.org.pk/reports/annual/arFY18/Chapter-07.pdf.

[14] Thomas Kranz, *Making Sense of Cybersecurity* (Manning, 2022), https://www.manning.com/books/making-sense-of-cybersecurity.

[15] Sindhu Abbasi, "PAKISTAN&Rsquo;S WEB OF CYBER SCAMMERS," *DAWN.COM*, July 16, 2023, https://www.dawn.com/news/1764628#:~:text=Out%20of%20the%20respective%20totals,2021%20and%201%2C392%20in%202022.&text=cyber%20harassment%20complaints%2C%20but%20it,2021%20and%20500%20in%202022.

has been observed that scammers in the guise of bank employees exploit the population's digital illiteracy and lack of data protection laws to manipulate individuals into revealing their sensitive information such as ATM pins and OTPs, leading to financial losses. These cyber criminals also get an access to personal data through social media groups selling compromised information from national database and social safety programs like National Database Regulatory Authority (NADRA) during cyber breaches. This systematic nature of data theft and the absence of digital literacy leave the public vulnerable to such frauds. Meanwhile, cybercriminals gain unauthorised access to the private businesses' sensitive information[16]. With increasing digitalisation, many companies rely heavily on their propriety information, including new product information, employment records, and sales figures. Once cybercriminals access this information, they engage in blackmail and fraud, targeting the business community.

Additionally, the ability to operate anonymously on the Dark Web allows cybercriminals to evade traditional law enforcement measures. Therefore, it becomes difficult to track their activities and infrastructure. For instance, a notable incident in 2018 happened in Pakistan where its banking system suffered a major breach[17]. It resulted in the theft and sale of customer's data from numerous debit cards on the Dark Web. This breach inflicted financial damage on the banking sector and compromised the personal security of customers. This incident highlighted systemic weakness in Pakistan's banking infrastructure. It also revealed lack of coordinated cyber security

[16] Anthony Bowie, *Policing Cyber Crime* (London: Bookboon, 2021), https://bookboon.com/premium/reader/policing-cyber-crime.

[17] Staff Report, "Hackers Steal Data From 'Almost All Pakistani Banks': FIA," Profit by Pakistan Today, November 6, 2018, https://profit.pakistantoday.com.pk/2018/11/06/nearly-every-banks-data-got-stolen-in-security-breach-says-fia-cybercrimes-director/.

efforts across financial institutions. The anonymity provided by the Dark Web and its cheap availability in Pakistan enables cybercriminals to loom scot-free.

Furthermore, the State Bank of Pakistan and the Federal Board of Revenue banned digital currencies in 2018; however, crypto market is still flourishing in Pakistan due to the absence of a legal framework[18]. The absence of legislative regulations leaves investors unprotected against fraud and scams, making them easy targets for cybercriminals. The ban of government and the decentralisation of crypto-currencies further complicate efforts to trace stolen assets. This lack of legal oversight facilitates money laundering and other illicit activities, undermining financial integrity of the crypto investors. The inadequate digital literacy among the population also increases the risk of exploitation, as individuals may fall prey to misleading schemes and frauds. Nevertheless, the deregulation of a substantial share of Pakistan's capital leads to its incorporation into the black economy.

### 3.2 Malwares

Malware is another financial cyber threat posing serious challenges and exploiting the vulnerabilities of masses. Malware is a cyber-security threat, wherein software designed to get unauthorised access to a system is used by hackers for a variety of purposes, including jamming the networking system of an organisation and demanding ransom. Since the ICT structure of Pakistan is imported it is easy to adulterate it by foreign cyber criminals. For instance, the Institute of Space Technology (IST) fell to a

[18] Muhammad Arif Saeed and Muhammad Hassan Sial, "Issues of Legislation of Cryptocurrency in Pakistan: An Analysis," *ANNALS OF SOCIAL SCIENCES AND PERSPECTIVE* 4, no. 2 (December 29, 2023): 429–43, https://doi.org/10.52700/assap.v4i2.292.

malware by the hacking group Medusa[19]. Hackers accessed contact details and identification numbers of students and faculty and demanded ransom of $500,000. Malwares are a step ahead from individual security threat to institutional security threats as they have bigger targets. Currently, a large number of small and medium businesses go burst within six months after disruption due malware attacks. These businesses do not invest in cyber security solutions due to strained budget, causing financial loses[20].

The current situation of malwares is alarming in Pakistan. According to Kaspersky Managed Detection and Response (MDR) team, malwares have surged to 300 percent in the first quarter of 2024 compared to the same period in 2023[21]. According to the report, government sector is most vulnerable to malwares with 22.9 percent of all the detected attacks. After that, IT companies faced 15.4 percent of the attack, highlighting vulnerable digital infrastructure of Pakistan due to imported equipment. The financial and industrial sector also suffered at the rate of 14.9 percent and 11.8 percent respectively. It indicates the gap between digitalisation in every sector of Pakistan and the vulnerability of its digital infrastructure.

The unchecked availability of AI and Large Language Models (LLMs) is an escalating threat to the cyber-security of the people of Pakistan. In 2023, globally, 3000 Dark Web posts highlighted malicious chatbot versions, exploring projects like XXXGPT and

[19] Abdullah Shahid, "Hacking Group Medusa Attacks a Public University in Islamabad: Student and Staff's Personal Data up for Ransom," TECHJUICE, March 2024, https://www.techjuice.pk/hacking-group-medusa-attacks-a-public-university-in-islamabad-student-and-staffs-personal-data-up-for-ransom/.

[20] Jonathan Reuvid, ed., *Be Cyber Secure: Tales, Tools and Threats* (Legend Business, Jonathan Reuvid and Individual Contributors, 2019), https://www.ubpopenbooks.com/index.php/ubp/catalog/view/3/2/8.

[21] Correspondent, "Spyware Attacks Increased by 300 in Pakistan," *The Express Tribune*, May 10, 2024, https://tribune.com.pk/story/2466023/spyware-attacks-increased-by-300-in-pakistan.

FraudGPT[22]. It indicates that cyber-criminals are trying to use AI to find out new methods and technologies to bypass security checks. One alarming application of AI includes GPT models that are being used to develop polymorphic malware capable of altering its code while maintaining core functionality. This adaptability makes detection of malware challenging as it evades standard security checks. Therefore, it a major threat for common users as they are not digitally literate to understand evolving nature of AI in cyber-attacks and may fell victim to new form of cyber-attacks like downloading AI generated bugs and viruses, bypassing security check installed in their mobiles and PCs. It could lead to personal data theft that could be used for financial frauds, harassment, and ransom demand.

### 3.3 Identity Thefts

Identity theft is another serious cyber threat to the people of Pakistan. Pakistan has experienced numerous incidents of data theft from public institutions including National Database and Registration Authority (NADRA) and Benazir Income Support Programme (BISP) which compromised the security of masses. In 2021, Federal Investigation Agency revealed that NADRA's biometric data had been compromised during SIM verification process. It led to proliferation of fake SIMs with 13,000 seized in Faisalabad alone[23]. The investigation find out that most of the targets were elderly people and women and their cyber illiteracy exacerbates the situation. Although, Pakistan has criminalised illegal SIM sale and fines are imposed on mobile operator, the thumbprints are still being sold after data breach. This identity theft could be used social security

[22] Alessandro Mascellino, "ChatGPT Cybercrime Surge Revealed in 3000 Dark Web Posts," *Infosecurity Magazine*, June 19, 2024, https://www.infosecurity-magazine.com/news/chatgpt-cybercrime-revealed-dark/.

[23] Javed Hussain, "Nadra'S Biometric Data Has Been Compromised, FIA Official Tells NA Body," *DAWN.COM*, November 25, 2021, https://www.dawn.com/news/1660199.

frauds in which government benefits could be received without the actual person's knowledge, loan frauds in which loans from banks or people could be taken, and criminal activities like providing stolen identity information when apprehended which could lead to false record against victims, etc.

### 3.4 Digital Harassment

Digital harassment is a growing cyber threat, especially for women and marginalised communities of Pakistan. Rapid increase of internet literacy and cyber illiteracy among women led to digital harassment, which often go unreported. Similarly, disinformation and fake news about a community member of a minority group is used for propaganda and digital harassment of the whole community[24]. For cyber harassment, fake news and misinformation are spread through bots and fake profiles which distort public perception. According to Digital Rights Foundation, 40 percent of Pakistani women using web have experienced harassment on social media[25]. It also highlights that 72 percent of female social media users are unaware of legal protection against cyber harassment. It shows that there is a huge gap between digitalisation and cyber literacy which is exposing a huge population to cyber harassment.

The theory of 'six degrees of separation' suggests that individuals across the globe are connected through a short chain of acquaintances[26]. This concept underscores the power of digital connectivity in spreading propaganda and harassment, making it potent for targeting individuals. Marginalised communities, especially religious minorities in Pakistan also have to face censorship, surveillance, violence and online harassment

[24] Digital Rights Foundation, "Religious Minorities in Online Spaces," *Digital Rights Foundation*, 2021, https://digitalrightsfoundation.pk/wp-content/uploads/2021/05/Religious-Minorities.pdf.

[25] Farooq Feroze, "Lack of Digital Media Literacy and Cyber Crimes," Pakistan Observer, 2023, https://pakobserver.net/lack-of-digital-media-literacy-and-cyber-crimes-by-farooq-feroze/.

[26] Paul Day, *CyberAttack* (London: CyberTech Publishing, 2016), 180.

that is being triggered on digital platforms and extended to real world like the Tahir Ahmed Naseem case, wherein victimisation followed a video shared on social media[27]. Such incidents indicate that online platforms become crucial extension of public space, reflecting societal attitudes, leading to social unrest and ostracise communities.

## 4. Analysing the Trajectory of Cyber Threats and Vulnerabilities with Digitalisation

The increasing digitalisation in Pakistan has left its population highly susceptible to various cyber threats, including financial frauds, malware attacks, identity thefts, and digital harassment. The Bureau of Statistics Punjab released a report in 2023, highlighting reported cyber-crimes from 2018 to 2021 in Pakistan[28]. The report indicates a five-fold increase in cyber complaints from 16,122 in 2018 to 1,15, 800 in 2021 exposing the vulnerability of the people of Pakistan due to rapid digitalisation and prevalent digital literacy.

The report shows that financial frauds surged from 2,358 to 32,604 in four years, delineating huge financial loss to the people of Pakistan. The cases of identity theft have increased from 114 to 1,334 and harassment cases have grown from 1,112 to 7,632 revealing a severe gap between the expanding use of digital platforms and the insufficient cyber-security measures. Notably, child pornography rose from 1 compliant in 2018 to 113 in 2021 attracting international attention. These alarming trends highlight the urgent need for improved digital literacy, robust cyber infrastructure, and stronger regulatory frameworks to protect individuals from cyber threats and ensure national

[27] Digital Rights Foundation, "Religious Minorities in Online Spaces," *Digital Rights Foundation*, 2021, https://digitalrightsfoundation.pk/wp-content/uploads/2021/05/Religious-Minorities.pdf.

[28] "Cyber Crimes as Reported by Category, Pakistan (Numbers) - Cyber Crimes as Reported by Category, Pakistan (Numbers).Csv - Open Data Pakistan," n.d., https://opendata.com.pk/dataset/cyber-crimes-as-reported-by-category-pakistan-numbers/resource/fd18c91d-5334-49c0-b025-0ed151105ccb.

security in an increasing digital world. Table 1 provides a glimpse of numerical data on various cyber-crimes in Pakistan to understand the intensity and expansion of cyber-crime in every public sector of Pakistan in different forms.

| Crime Category | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|
| Total Complaints | 16122 | 54832 | 118011 | 115800 |
| Financial Frauds | 2358 | 11905 | 27720 | 32604 |
| Fake Profile | 5005 | 7140 | 7774 | 3926 |
| Hacking | 1171 | 5837 | 11833 | 9672 |
| Harassment | 1112 | 5120 | 8579 | 7632 |
| Defamation | 713 | 3641 | 7871 | 10283 |
| Unauthorised Access | 1339 | 3957 | 6137 | 3397 |
| Blackmailing | 450 | 2381 | 5099 | 5130 |
| Online Shopping | 264 | 1284 | 2546 | 1729 |
| Stalking | 393 | 981 | 1679 | 1861 |
| Blasphemous Content | 133 | 1126 | 1786 | 483 |
| Identity Theft | 114 | 780 | 1309 | 1334 |
| Anti-Religion | 68 | 641 | 1182 | 253 |
| Online Banking Fraud | 65 | 341 | 366 | 619 |
| Illegal SIMs | 15 | 144 | 170 | 531 |
| Child Pornography | 1 | 19 | 101 | 113 |
| Ransomware | 1 | 11 | 48 | 64 |

Table 1: Cyber Crime in Pakistan [29]

[29] "Cyber Crimes as Reported by Category, Pakistan (Numbers) - Cyber Crimes as Reported by Category, Pakistan (Numbers).Csv - Open Data Pakistan," n.d., https://opendata.com.pk/dataset/cyber-crimes-as-reported-by-category-pakistan-numbers/resource/fd18c91d-5334-49c0-b025-0ed151105ccb.

# 5. IMPACT OF CYBER THREATS ON NATIONAL SECURITY OF PAKISTAN

The combination of financial frauds, malware attacks, identity thefts and digital harassment compromise personal security and financial stability of the people of Pakistan. These cyber security threats at individual level poses the potential to risk the national security of Pakistan as discussed below.

## 5.1 Economic Instability and Trust Erosion

Economic security is a primary goal for achieving national security as encapsulated in National Security Policy 2022[30]. In its policy guideline, NSP suggests to ensure a prosperous and growth-oriented Pakistan through trade, investment, and connectivity initiatives. To achieve this target, Pakistan needs to ensure a secure financial digital setup to meet the global standards. However, consistent incidents of financial frauds and cyber-attacks on baking system undermine the trust of foreign investors and local business community of Pakistan. The exploitation of population's digital illiteracy and the scale of compromised data leaks lead to significant financial losses for individuals and business. As their scale is increasing, these financial frauds pose the threat to undermine the economic stability of the country through trust erosion of investors and creation of economic difficulties of individuals at large-scale leading to deterioration of individuals on state's institution and governance system. This lack of trust hinders individuals' use of digital modes of payments, thus reducing regulation of digital economy which is a necessity for economic security. It also undermines state's political and societal security.

[30] National Security Division, National Security Policy of Pakistan 2022-2026, 2022.

### 5.2 Digital Dependence and Social Unrest

Malware attacks on social sectors and public institutions indicate vulnerabilities in the ICT infrastructure of Pakistan, which is primarily dependent on imported products. This digital dependence has the capability to compromise critical systems and essential services from healthcare to education, causing social unrest in Pakistan. Lack of indigenous digital structure could also halt government operations and emergency services, creating chaos and insecurity. For instance, Japan experienced blackouts caused by malware attacks on its power system due to vulnerabilities in internet and control system equipment[31]. Pakistan's ICT system is also vulnerable to malwares and it could create a state of emergency in case of malware attack on public institutions and services shaking national security by creating emergencies. They could create national emergency by disrupting medical services putting a large number of population at risk. Similarly, by disrupting water supply system and electricity grids, the whole operational setup of Pakistan could be paralysed creating a national emergency. Today, national security is not limited to traditional security checks but its domain has widened to non-traditional arena like human security. The ability of Malwares to penetrate into health and educational institutions could threaten human security by gaining access to individual's digital equipment associated with such institutions.

### 5.3 Espionage and Terrorism

The incidents of data leak from institutions like NADRA had resulted in proliferation of fake SIMs and risked the personal identity of people. Similar to the warning issued by

[31] "An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures : NEC Technical Journal | NEC," NEC, n.d., https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html.

Keith Alexander, former head of the National Security Agency (NSA), who highlighted that cyber threats extend across critical sectors, from banks to power grids and military intelligence networks, the need for institutions to evolve beyond counterterrorism missions is paramount[32]. Such data breaches can be exploited by militant organisations for espionage and terrorism.

Fake SIMs and identity theft could be used by malicious entities to evade surveillance and communicate securely without detection. Therefore, incidents of identity theft by data leak not only put individuals at risk but also put national security at stake. For instance, in 2019 the Counter Terrorism Department (CTD) reported that a gang of seven people was arrested in identity theft for the illegal activation of mobile phone SIMs which was used for terrorist activities[33]. Pakistan is challenged by terrorist activities which have surged after US withdrawal from Afghanistan. External non-state actors are also active to sabotage CPEC. Therefore, such data breaches could be exploited by these factions threatening national security.

### 5.4 Societal Unrest

Uncontrolled digital harassment, particularly against women and minority groups leads to societal tension. For instance, according to International Federation of Journalists, female journalists in Pakistan reported that they are facing increasing level of online harassment, including trolling, cyber-bullying, intimidation and doxing which keep them under pressure and have psychological impact that affects their performance

[32] Shane Harris, *The Rise of Cyber Warfare* (New York: Atlantic Monthly Press, 2014), 83.

[33] Sajid.Rauf, "How a Gang Duped the Biometric System to Get SIM Cards for Criminals," *The Express Tribune*, April 24, 2019, https://tribune.com.pk/story/1957732/gang-duped-biometric-system-get-sim-cards-criminals.

professionally[34]. Stigmatisation and prejudice against victims through social media campaigns also halt their social growth and security. It leads to gender and social polarisation as different sections of society perceive harassment differently due to illiteracy and backwardness. At a large scale, it endangers human security, particularly young women who hold a major proportion of Pakistan's population. The use of fake news and misinformation to harass marginalised communities also serve broader agenda of propaganda and social manipulation. For instance, in 2020 a large social media campaign was initiated against Shias which put the community in terror and rifted sectarian violence[35]. Anti-state groups exploit this situation to sow discord, spread disinformation, and influence public opinion which is against national interests.

## 6. GOVERNMENTAL POLICIES AND INITIATIVES' ANALYSIS

Amid rapid digitalisation and escalating cyber threats, cyber protection has become a paramount concern for the government of Pakistan. For this, legislative measures to regulate the cyber domain began with the Pakistan Telecommunication (Re-Organisation) Act 1996 and the Electronic Transaction Ordinance 2002. These foundational steps were followed by the Prevention of Electronic Crimes Act in 2016 which aimed to counter the increasing cybercrimes. While these legislative measures represent proactive effort, they lack a comprehensive approach to cover the evolving nature of cyber threats like financial frauds, identity theft, digital harassment and

[34] "Harassment of Women Journalists in Pakistan: Perspectives, Politics &Amp; Action / IFJ," August 18, 2022, https://www.ifj.org/media-centre/blog/detail/category/labour-rights/article/pakistan-harassment-of-women-journalists-perspectives-politics-action.

[35] Shah Meer Baloch and Hannah Ellis-Petersen, "Pakistani Shias Live in Terror as Sectarian Violence Increases," *The Guardian*, October 21, 2020, https://www.theguardian.com/world/2020/oct/21/pakistani-shias-live-in-terror-as-sectarian-violence-increases.

malware proliferation. Furthermore, the selective Operation of Cyber Security Incident Response Teams (CSIRT) at the organisational level highlights a fragmented and piecemeal national strategy to counter massive cyber threats arising with mass digitalisation. Without a unified national framework it leads to inconsistencies in cyber-attack responses and mitigation strategies.

In 2018, to rectify these shortcomings, the National Centre for Cyber Security (NCCS) was established to stimulate research and development in the cyber domain. However, the persistent disparity between demand and supply of digital skills in cyber-security remained persistent. For that, in 2021, the National Cyber Security Policy was given[36] which marked a strategic shift in protecting critical cyber infrastructure of Pakistan. The policy aims to create a central platform for developing strategies to address issues regarding data governance, online privacy, critical information infrastructure, and data protection. Under this policy, a national cyber committee is also established to enhance the capacity of public institutions and private sector. However, the absence of a centralised operational framework limits the policy's effectiveness. The establishment of national cyber security committee is a step towards coordination; however, it lacks the required authority and resources to enforce regulation comprehensively which leaves a gap in data protection and online privacy enforcement.

In 2023, further legislative advancements were made to address cyber-crimes, including the E-Safety Bill and the Personal Data Protection Bill. Although, these

[36] Ministry of Information Technology and Telecommunication, *National Cyber Security Policy 2021* (Government of Pakistan, 2021), https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf .

initiatives are commendable, the absence of a centralised cyber-security framework continues to leave Pakistan vulnerable to cyber threats. It requires an integrated approach that unifies national policy, regulatory framework, and operational capabilities to effectively enhance national cyber-security of Pakistan.

The government of Pakistan initiated multiple campaigns to warn masses about potential cyber threats. For instance, warning SMS messages to mobile users are often sent to advice people on avoiding common cybercrimes and tips on protecting personal information. Although, such SMS alerts reach a wide audience, their impact on educating digital illiterate consumers is limited. Many users not fully understand the technical details or ignore the warnings due to ignorance on cyber threats and their vulnerabilities. Additionally, Public Service Announcements (PSA) campaigns are run on social media but those users that do not follow official government accounts fail to reach these campaigns.

To protect the cyber sovereignty, Pakistan Air Force has also assumed a central role in strengthening the national cyber infrastructure. As a constructive step, the National Cyber Security Academy was established within the National Aerospace Science and Technology Park (NASTP). This academy is dedicated to train skilled cyber-security experts for defence institutions, government agencies, and public/private organisations. Additionally, the PAF has instituted a Cyber Command to safeguard its digital assets and augment its cyber defence capabilities. In the domain of research and development, PAF has forged collaboration with academic institutions such as National University of Science and Technology (NUST) and Air University (AU). Although these initiatives project a positive development in cyber domain, however, without digital

literacy and indigenous digital setup, a full spectrum cyber defence could not be achieved which is the need of time.

The above stated description of cyber landscape of Pakistan delineates that myriad initiatives have been taken by the concerning authorities and the government to mitigate the cyber perils. It includes legislating cyber-crimes, regulating cyber space, upgrading digital infrastructure, policy making, and increasing the cyber-literacy. However, the people of Pakistan are still prone to cyber threats; therefore, following recommendations are provided to ensure cyber security and a progressive digital future of Pakistan.

# 7. WAY FORWARD

## 7.1 Learning from Best Practices

China is one of the emerging powers in cyber security. Pakistan could learn valuable lessons from China's approach. In 2014, China took cyber security as its top priority with the objective to make China's IT sector economically and technologically self-reliant. For that China gave its National Cyber-security Strategy, an International Cyber Cooperation Strategy, and comprehensive Cyber-security Laws. It shows the holistic approach of China to tackle cyber impediments from all directions. Similar to China's Transmission Control Protocol (TCP), Pakistan has also successfully completed firewall trial that would be used to monitor social media to stop propaganda; a unified national cyber strategy is still required.

China increased its participation in international governance processes such as the UN Group of Governmental Experts on State conduct in cyberspace and the Open

Ended Working Group (OEWG) on ICTs in international security[37]. It indicates the importance of international cooperation in cyber-security. Additionally, recognising the critical role of skilled professionals in maintaining cyber-security, China invested heavily in IT education and training facilities. As Pakistan lags behind in educational training programs and international cooperation, there is a need to expand investment in IT education to develop a skilled workforce capable of addressing complex cyber-security challenges. Furthermore, active participation in regional and international cyber-security governance processes can improve the country's global standing and provide access to valuable resource of cyber knowledge, required for research and development.

### 7.2 Legislative Reforms

Though Pakistan has issued its Prevention of Electronic Crime Act 2016, it needs to expand its domain to prevent anonymous cyber-attacks, considering the evolving nature of cyber tactics. Firstly, Pakistan needs to specifically criminalise the creation, distribution, and use of malwares that that obstruct the functioning of networks. Provided the increasing sophistication of malware attacks, this step is essential to deter cybercriminals. Secondly, the Act should be expanded to criminalise privacy breaches through cyber-attacks, the distribution of rumours, subversive content, and organisation of heretic groups. High penalties should be imposed for such activities to deter individuals from cyber actions that compromise social stability. Thirdly, Pakistan needs to legislate on manipulation of financial markets through false information or bringing damage to the reputation of businesses as false campaigns through disguised social

[37] Rogier Creemers, "The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy," *˜the œJournal of Contemporary China/Journal of Contemporary China*, March 30, 2023, 1–16, https://doi.org/10.1080/10670564.2023.2196508.

media platforms that lead to financial loses to companies. By criminalising these actions, Pakistan could protect its economic interests and maintain market integrity.

### 7.3 Digital Literacy

To combat the evolving nature of cyber security methodologies Pakistan's should invest in increasing digital literacy. In past years, many digital learning and vocational training programmes had been initiated; however, their availability is restricted to major cities, excluding a vast majority of population from rural areas and small cities. This geographical limitation highlights the disparity in access to advanced cyber-security education and training. Therefore, Pakistan needs a bottom-up approach in which digital literacy should be made part of the curriculum for uniformity and reduce rural-urban gap.

### 7.4 Local IT Start-ups

To strengthen the indigenous IT industry and cyber-security, Pakistan should focus on two interrelated categories. Firstly, to set the foundation of IT led digitalisation, it requires software production and their usage by businesses and governmental institutions. Secondly, Pakistan needs to strengthen the broader digitalisation of the economy through technology based solutions, pioneered by start-ups exploring innovative business models that are cyber-protected. Investment in local start-ups is important for addressing the availability of IT services within Pakistan as it would enhance the country's technological capabilities and infrastructure. By fostering indigenous IT ecosystem, Pakistan would also reduce its dependency on imported technologies which expose the critical infrastructure and malwares. This strategic

investment would also drive economic growth and ensure a resilient digital infrastructure.

### 7.5 PETs in Critical Infrastructure

Privacy Enhancing Technologies (PET) also presents a liable solution for the protection of critical infrastructure of Pakistan and enhances data security and privacy across various sectors. These technologies lead organisations to conduct joint data analysis in privacy-friendly manner. Additionally, Federal learning brings the machine learning model to the data rather than requiring a central database. It reduces the risks of data breaches. Another technology, secure multi-part computation employs a toolkit of cryptographic techniques that enable multiple parties to use data jointly for calculations without exposing individual's data. By adopting these technologies, Pakistan can improve data privacy and security.

### 7.6 Policy Audit and Implementation

To ensure the effectiveness of Cyber Security Policy, it should be consistently and effectively implemented across all sectors. While the policy provides a comprehensive framework, the next step is to develop an applicable implementation framework for all governmental organisations. It should include an audit mechanism which would be a catalyst for enforcement and adherence to the policy's objectives.

To enhance compliance and accountability, the government should appoint ad-hoc audit teams to conduct regular checks of critical institutions. These should comprise technocrats and security personnel with expertise to evaluate cyber-security practices thoroughly. These audit teams would not only verify but would also identify areas for

improvement. It would breed a culture of continuous enhancement in cyber-security measures which is required considering the evolving cyber-crime methodologies.

# 8. POLICY RECOMMENDATIONS

## 8.1 Strict Regulations and Authentication Procedures

To protect critical systems multi-factor authentication, end-to-end encryption, and real-time fraud detection system could be indigenously designed. Moreover, facial recognition can be incorporated for higher-value transactions in banks.

## 8.2 Strengthen Digital Literacy

To mitigate the economic risks sector-specific cyber-security training could be made mandatory for employees in financial institutions, complemented by a government-led portal offering real-time threat alerts. Additionally, by integrating cyber-security education into national curricula, next generation could be equipped with foundational knowledge.

## 8.3 National Cyber Security Agency

To prevent identity theft and data leaks, a national cyber-security agency could be established. It could ensure swift action in case of a breach and enforce compliance with standards. It could also be made responsible for regular penetration testing and vulnerability assessments.

### 8.4 Stringent Laws against Online Harassment

To promote digital rights protection and prevent social unrest, Pakistan could enforce strict laws against online harassment with a focus on protecting vulnerable groups such as women and minorities. For that PECA 2016 could be expanded with the definition of online harassment to include emerging forms of digital abuse

## 9. CONCLUSION

This study concludes that the current cyber security landscape of Pakistan does not meet the criteria to address emerging threats and challenges posed by cyber-attacks. Pakistan has undergone significant digitalisation across various sectors without adequate cyber literacy and indigenous digital infrastructure. It exposed the people to cyber frauds, malwares, identity thefts, and digital harassment. The government took regular initiatives to mitigate these challenges but due to policy gaps and their lack of implementation, Pakistan could not achieve the set goal. Additionally, the intensity of cyber safety measures does not meet the gravity of cyber threats. It is concerning for the state as it could risk the national security of Pakistan through terrorism, misinformation, social unrest, and financial instability. Therefore the government needs to revamp the cyber landscape and indigenise digital infrastructure. This requires a holistic approach with inclusive policies for every sector. Additionally, cyber literacy is an important aspect to invest in for a prosperous and secure digital Pakistan.

# BIBLIOGRAPHY


Abbasi, Sindhu. “Pakistan’s Web of Cyber Scammers.” *DAWN.COM*, July 16, 2023. https://www.dawn.com/news/1764628#:~:text=Out%20of%20the%20respective%20totals,2021%20and%201%2C392%20in%202022.&text=cyber%20harassment%20complaints%2C%20but%20it,2021%20and%20500%20in%202022.

Baloch, Shah Meer, and Hannah Ellis-Petersen. “Pakistani Shias Live in Terror as Sectarian Violence Increases.” *The Guardian*, October 21, 2020. https://www.theguardian.com/world/2020/oct/21/pakistani-shias-live-in-terror-as-sectarian-violence-increases.

Bowie, Anthony. *Policing Cyber Crime*. London: Bookboon, 2021. https://bookboon.com/premium/reader/policing-cyber-crime.

Correspondent. “Spyware Attacks Increased by 300  in Pakistan.” *The Express Tribune*, May 10, 2024. https://tribune.com.pk/story/2466023/spyware-attacks-increased-by-300-in-pakistan.

Creemers, Rogier. “The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy.” *˜the œJournal of Contemporary China/Journal of Contemporary China*, March 30, 2023, 1–16. https://doi.org/10.1080/10670564.2023.2196508.

“Cyber Crimes as Reported by Category, Pakistan (Numbers) - Cyber Crimes as Reported by Category, Pakistan (Numbers).Csv - Open Data Pakistan,” n.d. https://opendata.com.pk/dataset/cyber-crimes-as-reported-by-category-pakistan-numbers/resource/fd18c91d-5334-49c0-b025-0ed151105ccb.

Day, Paul. *CyberAttack*. London: CyberTech Publishing, 2016.

Digital Rights Foundation. “Religious Minorities in Online Spaces.” *Digital Rights Foundation*, 2021. https://digitalrightsfoundation.pk/wp-content/uploads/2021/05/Religious-Minorities.pdf.

Feroze, Farooq. “Lack of Digital Media Literacy and Cyber Crimes.” Pakistan Observer, 2023. https://pakobserver.net/lack-of-digital-media-literacy-and-cyber-crimes-by-farooq-feroze/.

"Harassment of Women Journalists in Pakistan: Perspectives, Politics &Amp; Action / IFJ," August 18, 2022. https://www.ifj.org/media-centre/blog/detail/category/labour-rights/article/pakistan-harassment-of-women-journalists-perspectives-politics-action.

Harris, Shane. *The Rise of Cyber Warfare*. New York: Atlantic Monthly Press, 2014.

Hussain, Javed. "Nadra'S Biometric Data Has Been Compromised, FIA Official Tells NA Body." *DAWN.COM*, November 25, 2021. https://www.dawn.com/news/1660199.

International Trade Administration | Trade.gov. "Pakistan - Cybersecurity," January 12, 2024. https://www.trade.gov/country-commercial-guides/pakistan-cybersecurity#:~:text=Like%20other%20markets%2C%20the%20cybersecurity,terrorism%2C%20vandalism%2C%20and%20pornography.

Kranz, Thomas. *Making Sense of Cybersecurity*. Manning, 2022. https://www.manning.com/books/making-sense-of-cybersecurity.

Majlis-E-Shoora. *Prevention of Electronic Crimes Act Bill*, 2016. https://www.na.gov.pk/uploads/documents/1470910659_707.pdf.

Mascellino, Alessandro. "ChatGPT Cybercrime Surge Revealed in 3000 Dark Web Posts." *Infosecurity Magazine*, June 19, 2024. https://www.infosecurity-magazine.com/news/chatgpt-cybercrime-revealed-dark/.

Ministry of Information Technology and Telecommunication. *National Cyber Security Policy 2021*. Government of Pakistan, 2021. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf .

Saeed, Muhammad Arif, and Sial, Muhammad Hassan. "Issues of Legislation of Cryptocurrency in Pakistan: An Analysis." *ANNALS OF SOCIAL SCIENCES AND PERSPECTIVE* 4, no. 2 (December 29, 2023): 429–43. https://doi.org/10.52700/assap.v4i2.292.

Nakhoda, Aadil. "Propelling the ICT Sector via Imports of IT Products." *The Express Tribune*, May 20, 2024. https://tribune.com.pk/story/2467349/propelling-the-ict-sector-via-imports-of-it-products.

‘National Security Policy 2022-2026’. National Security Division, Government of Pakistan, January 2022.

NEC. “An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures : NEC Technical Journal | NEC,” n.d. https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html.

Report, Staff. “Hackers Steal Data From ‘Almost All Pakistani Banks’: FIA.” Profit by Pakistan Today, November 6, 2018. https://profit.pakistantoday.com.pk/2018/11/06/nearly-every-banks-data-got-stolen-in-security-breach-says-fia-cybercrimes-director/.

Reuvid, Jonathan, ed. *Be Cyber Secure: Tales, Tools and Threats*. Legend Business, Jonathan Reuvid and Individual Contributors, 2019. https://www.ubpopenbooks.com/index.php/ubp/catalog/view/3/2/8.

Sajid.Rauf. “How a Gang Duped the Biometric System to Get SIM Cards for Criminals.” *The Express Tribune*, April 24, 2019. https://tribune.com.pk/story/1957732/gang-duped-biometric-system-get-sim-cards-criminals.

Shahid, Abdullah. “Hacking Group Medusa Attacks a Public University in Islamabad: Student and Staff’s Personal Data up for Ransom.” TECHJUICE, March 2024. https://www.techjuice.pk/hacking-group-medusa-attacks-a-public-university-in-islamabad-student-and-staffs-personal-data-up-for-ransom/.

State Bank of Pakistan. “Digitization of Services in Pakistan.” *State Bank of Pakistan Annual Report 2017-18*, 2018. https://www.sbp.org.pk/reports/annual/arFY18/Chapter-07.pdf.