SOCIAL SCIENCE REVIEW ARCHIVES
ISSN Online: 3006-4708
ISSN Print: 3006-4694
https://policyjournalofms.com

Cybersecurity Governance in the Digital Era and IT: Integrating Regulatory Oversight, Risk Management, and Organisational Resilience in Pakistan

Yasir Majeed[1], Anas Majeed[2], Muhammad Tahir Minhas[3]

[1]The University of Lahore, Email: yasirmajeedsatti@gmail.com
[2]Victoria University Melbourne, Australia, Email: anssatti7@gmail.com
[3]University of Management and Technology (UMT), Email: mtahir.minhas@gmail.com

DOI: https://doi.org/10.70670/sra.v4i1.1711

Abstract

The increased pace at which the Pakistani economy and infrastructure in the public sector is being digitalised presents a logical multiplicity of cybersecurity threats that require a strong, multi-layered governance structure. The current paper looks at the present situation on cybersecurity governance in Pakistan with an emphasis on the combination of regulatory oversight, enterprise risk management, and organisational resilience. Based on leading international standards like the NIST Cybersecurity Framework 2.0 (NIST, 2024), the ISO / IE 27001:2022, the European Union General Data Protection Regulation (GDPR, 2016), and the NIS2 Directive (European Parliament, 2022) and placing them into the framework of the Pakistan socio-economic and institutional context, the paper will assess the efficacy of the current laws, including the Prevention of Electronic Crimes Act (PECA) 20 The study also explores the organizational level management of the risks in public institutions and the private companies in Pakistan in this research, and the findings revealed the gaps in systems of awareness, technology capacity, incident management, and inter-agency coordination. The paper claims that to address the issue of sustainable cybersecurity governance in Pakistan, a paradigm shift is needed, shifting reactive and compliance-based strategies toward proactive and resilience-oriented strategies enshrined in national digital transformation agendas.

***Keywords**:* Cybersecurity Governance, Pakistan, Risk Management, Regulatory Oversight, Organisational Resilience, PECA 2016, National Cybersecurity Policy, Digital Transformation, NIST Framework, ISO 27001, IT Governance, PKCERT.

Introduction

The twenty-first century has seen the most remarkable integration of digital technologies into the life of the government, business, and civil life. In the case of developing countries such as Pakistan, this digital revolution has offered a revolution as well as an extreme vulnerability. With the nation pursuing aggressive actions in terms of digital transformation, such as the Digital Pakistan Vision, e-government operations, fintech, and cloud implementation, its digital security situation has not been able to keep up with the transforming threat environment (U. P. Khan & Anwar, 2020; Saleem et al., 2025). The result of such an inappropriate fit is physical: since the state utility networks suffer data breaches or are repeatedly intruded upon by hackers, the digital infrastructure of Pakistan is left vulnerable to advanced attacks both inside and outside of its borders (Yasin, 2020). The term cybersecurity governance is used to refer to systems, processes, policies, and institutional forms on how societies and organisations deal with the risks involved in information and communication technologies (Klimburg, 2012; Von Solms & Van Niekerk, 2013). These three pillars, regulation, risk management and resilience, are an integrated system in mature digital economies (Craigen et al., 2014). In Pakistan, they are still very divided, under expressed, and intermittent (Javed, 2023; M. F. Khan et al., 2021). The worldwide cybercrime has an estimated cost of USD 8 trillion in a single year and is expected to go up to USD 10.5 trillion by 2025 (Morgan, 2020; J. Sharma & Jain, 2025). In the case of a developing economy like Pakistan, a small percentage of this exposure is an enormous macroeconomic risk, as GDP is in the range of USD 340 billion. The Global Risks Report (WEF, 2023a) by the World Economic Forum continues to identify cybersecurity failures as one of the ten most probable risks globally, and this classification, in particular, has acute implications in the context of Pakistan because of its increasingly large cyberattack surface and institutionally relatively underdeveloped defence against it. This scholarly article presents an in-depth discussion on cybersecurity regulations in Pakistan in the wider framework of the digital age in the world. The paper also provides a futuristic outlook of how Pakistan can establish a more harmonious, dynamic, and robust framework of cybersecurity governance that can enable it to advance its national developmental goals. The theoretical framework and literature review will be presented in Section 2 of the paper. Section 3 examines the international cybersecurity governance situation. Section 4 looks at the legislative and regulatory climate of Pakistan. Section 5 examines structural risk management and strength. The main issues are discussed in Section 6. Section 7 provides policy recommendations. Section 8 concludes.

Theoretical Framework and Literature Review

Defining Cybersecurity Governance

Cybersecurity governance is a multidisciplinary phenomenon located at the crossroad of information technology, the administration of a state, organisational behaviour and international relations (Dunn Cavelty, 2014). Regarding the issue of public policy, Cavelty and Wenger (2020) determine cybersecurity governance to be the set of rules, norms, institutions and practices which regulate the behaviour of state and non-state actors within cyberspace. Organisational In terms of an organisation, the COBIT 2019 framework proposed by ISACA (Lanter, 2019) describes IT governance as a board and executive responsibility to direct, evaluate, and monitor IT performance and risk management in accordance with organisational goals. Cybersecurity governance is also carried out at three levels that are interdependent, and they include: national (macro), sectoral (mesa), and organisational (micro)(Nye, 2011). On the national level, governments play the role of passing laws, interagency coordination and international cybersecurity diplomacy (Tikk & Kerttunen, 2020). On the sectoral level, the sectoral standards are established by regulators and industry bodies and adhered to (Slayton & Clarke, 2020). Security controls are followed in the boards, CISOs, and the IT departments at the organisational level to manage risk and have resilience (Deloitte, 2023; PwC, 2023). Cybersecurity governance involves consistency at all three levels, which is more of an idealistic situation in most developing countries.

Key Theoretical Perspectives

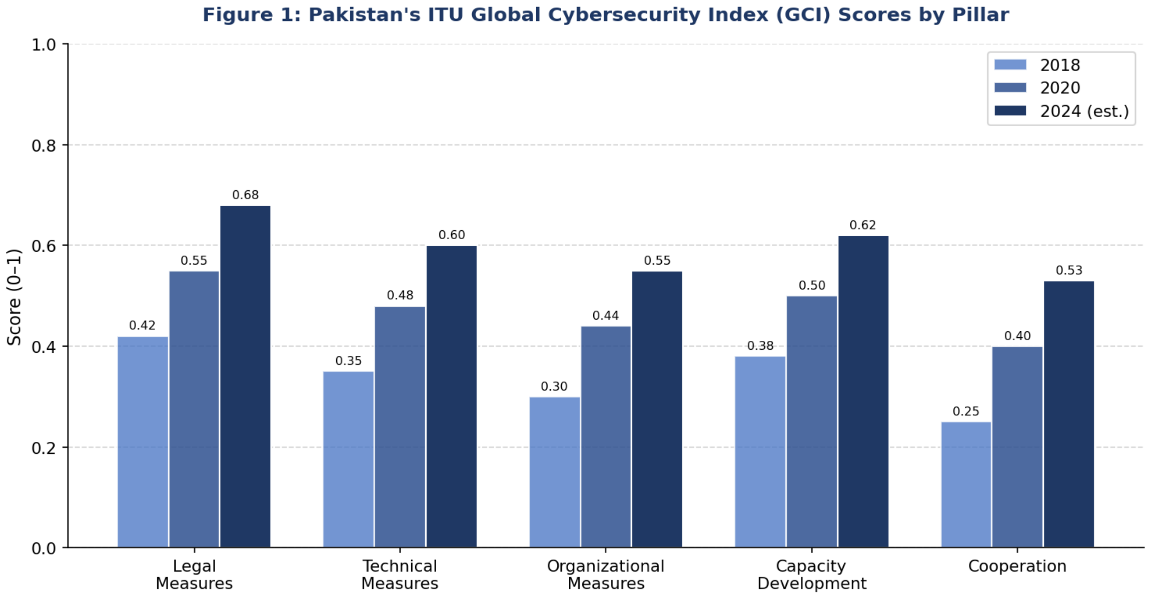
Cybersecurity governance can shed some light through several theoretical lenses. The principal-agent theory (Jensen and Meckling, 1976) can be used to understand why organisations do not invest in cybersecurity: information asymmetry between principals (boards, regulators) and agents (IT departments, vendors) results in moral hazard and adverse selection. Cybersecurity is considered a partially non-excludible good, which explains the need to involve the government in the delivery of the product (Anderson & Moore, 2006). The rationale behind cybersecurity practices in organisations is explained by institutional theory (DiMaggio & Powell, 2000): isomorphic pressures, as a result of regulators, industry colleagues and professional associations, drive convergence towards accepted standards like ISO 27001 and NIST CSF. Resilience theory (Hollnagel et al., 2006) and systems thinking (Meadows, 2008) are rather complementary viewpoints, which conceptualise cybersecurity governance as a complex adaptive system that should be engineered not only as resistant to attacks, but also to absorb and adapt to disruptions. United States (CISA, 2021), the United Kingdom (NCSC, 2023a), and the European Union (ENISA, 2023).

International Standards and Frameworks

There are a number of global frameworks that offer principles on which cybersecurity governance is based. Published and greatly updated in its 2.0 version in 2024 (NIST, 2024), the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a collection of cybersecurity activities organised around six main functions, namely Govern, Identify, Protect, Detect, Respond, and Recover. Inclusion of a Governance feature to CSF 2.0 is indicative of the increased awareness that cybersecurity risk management needs to be integrated in organisational strategic plans and accountability frameworks (Barrett et al., 2017). The international standard of information security management systems (ISMS) called ISO/IEC 27001:2022 (ISO, 2022) is more prescriptive, and it mandates organisations to have a set of systematic security controls in place within a cycle of continuous improvement in line with the Plan-Do-Check-Act (PDCA) model. The ISO/IEC 27001 certification has now become a non-standard practice as the standard of cybersecurity maturity in organisations and specifically within the financial, telecommunication and healthcare sectors (Malatji, 2023; Naserinia & Ullah, 2025). The General Data Protection Regulation (Regulation, 2016) established by the European Union has had a profound effect on cybersecurity governance practices both globally and domestically because it stipulates that organizations must ensure that they adopt suitable technical and organizational controls to safeguard the personal information as well as mandating them to notify individuals about breaches occurring in 72 hours (Voigt & Von Dem Bussche, 2017a). The NIS2 Directive (European Parliament, 2022) broadens the scope of the mandatory cybersecurity provisions to encompass the critical infrastructure industries, setting the minimum level of security and reporting of the measures that member states have to integrate into national legislation. The two tools affected the legislative development process in Pakistan (Haque et al., 2023; MOITT, 2023).

Cybersecurity Governance in Developing Nations: A Literature Review

The existing knowledge on cybersecurity governance in the developing countries is characterised by the constant emphasis on structural barriers to effective governance (Hurel & Lobato, 2018). It has been found that the main barriers are economic constraints, technical capacity, weak institutional structures, and insufficient legal infrastructure (Calderaro & Craig, 2020a; Savaş & Karataş, 2022). In the case of Pakistan, there is quite scanty academic literature. Baloch et al., (2022) record the disconnect between the policy goals and the actualities of implementing cybersecurity, as the effects of legislative improvements since 2016 are uneven, with low levels of organisational awareness of the subject. According to Gondal et al., (2023), the cybersecurity governance of Pakistan lacks institutional fragmentation. Sadiq, (2025) analyse the problem of digital transformation in the Pakistani public sector, and one of the bottlenecks here is cybersecurity governance. Abbas et al., (2022) examine the implementation issues of PECA and report the conflict of cybersecurity and civil liberties. Comparisons between regions are educational. (Sadiq, 2025a; Tabansky, 2011) examine how smaller countries may establish adequate cybersecurity governance without resource limitations, which have some lessons that apply to Pakistan. Singh et al., (2024) focus on the development of cybersecurity governance in India, paying special attention to the CERT-In framework.



Source: ITU Global Cybersecurity Index (2018, 2020); 2024 estimated from national policy disclosures.

Figure 1: The ITU Global Cybersecurity Index (GCI) Score of Pakistan by Pillar (20182024). The national policy disclosures presented in the 2024 estimates will be the source of information.

Global Cybersecurity Governance Landscape: Benchmarks and Comparisons

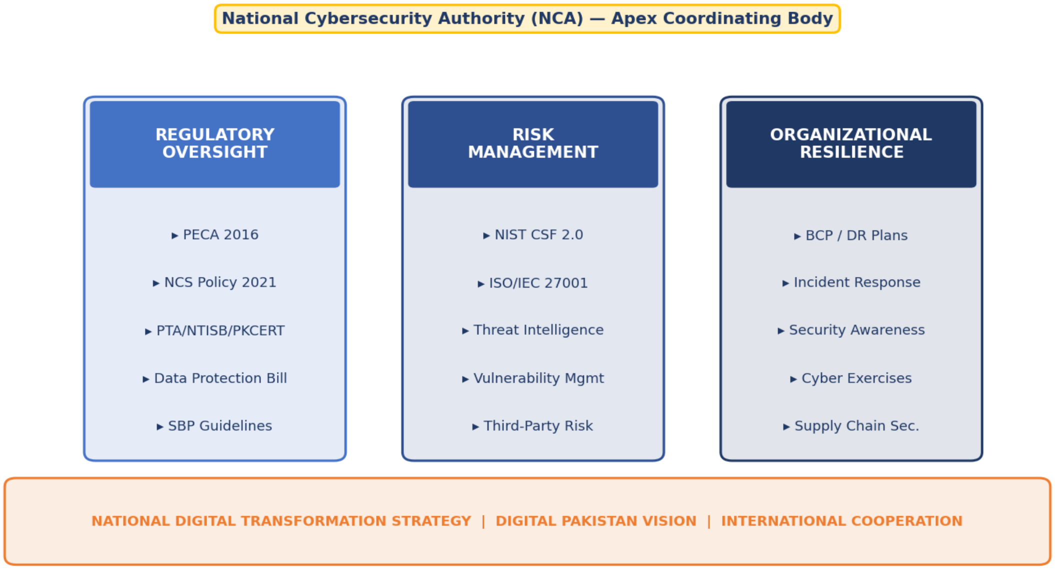
Advanced Economies

Clearly, the United States has a developed national cybersecurity plan through its Cybersecurity and Infrastructure Security Agency (CISA), which incorporates critical infrastructure resilience, a public-private collaboration, workforce building, and international interaction (CISA, 2023; White House, 2023). The 2023 National Cybersecurity Strategy is an important development, as it reflects the transfer of the burden of cybersecurity to the large technology vendors and government and calls for mandated minimum requirements on critical infrastructure sectors (Lewis et al., 2023; White House, 2023). The supranational regulation is harmonised in the European approach of the European Union. In 2016, the Network and Information Systems (NIS) Directive was replaced by the NIS2 Directive (European Parliament, 2023): it developed binding security provisions for operators of essential services and digital service providers in member states. Together with the security aspects of GDPR and the upcoming EU Cyber Resilience Act (European Commission, 2023), the EU has developed one of the most comprehensive cybersecurity governance frameworks in the world (Calderaro & Craig, 2020b; Christou, 2016). The National Cyber Security Centre (NCSC) of the UK has the program of Active Cyber Defence that is often referred to as an example of the implementation of the governmental protective services in the context of a low-resource environment (NCSC, 2023b; Roba Abbas et al., 2023).

Emerging Economies: India, Malaysia, and the UAE

Pakistan has a lot to learn, especially through comparisons with India, Malaysia and the UAE, which are emerging economies. A legal framework is underpinned by the National Cyber Security Policy (2013) and subsequent amendments to the Information Technology Act have created an active incident response agency in the form of CERT-In, and the most recent action has been the introduction of mandatory reporting of breaches (Basu, 2025). The Cybersecurity Act 2024 (Malaysia, 2024) of Malaysia is one of the newest comprehensive and country-level cybersecurity laws in the Asian region, which introduced a new Cybersecurity Agency (CSM), obligatory licensing of cybersecurity service providers, and onerous demands on the owners of national critical information infrastructure (NCII). The UAE Cybersecurity Council (UAE, 2020) is the coordinating force of national cybersecurity policy in a highly digitised economy, and the sector-specific regulations of the UAE in the fields of financial services and telecommunication systems offer a paradigm of state-led cybersecurity regulation in developing economies of the world (Alshabib & Martins, 2021; Tsukanov & Valiakhmetova, 2025).

Figure 2: Integrated Cybersecurity Governance Framework for Pakistan

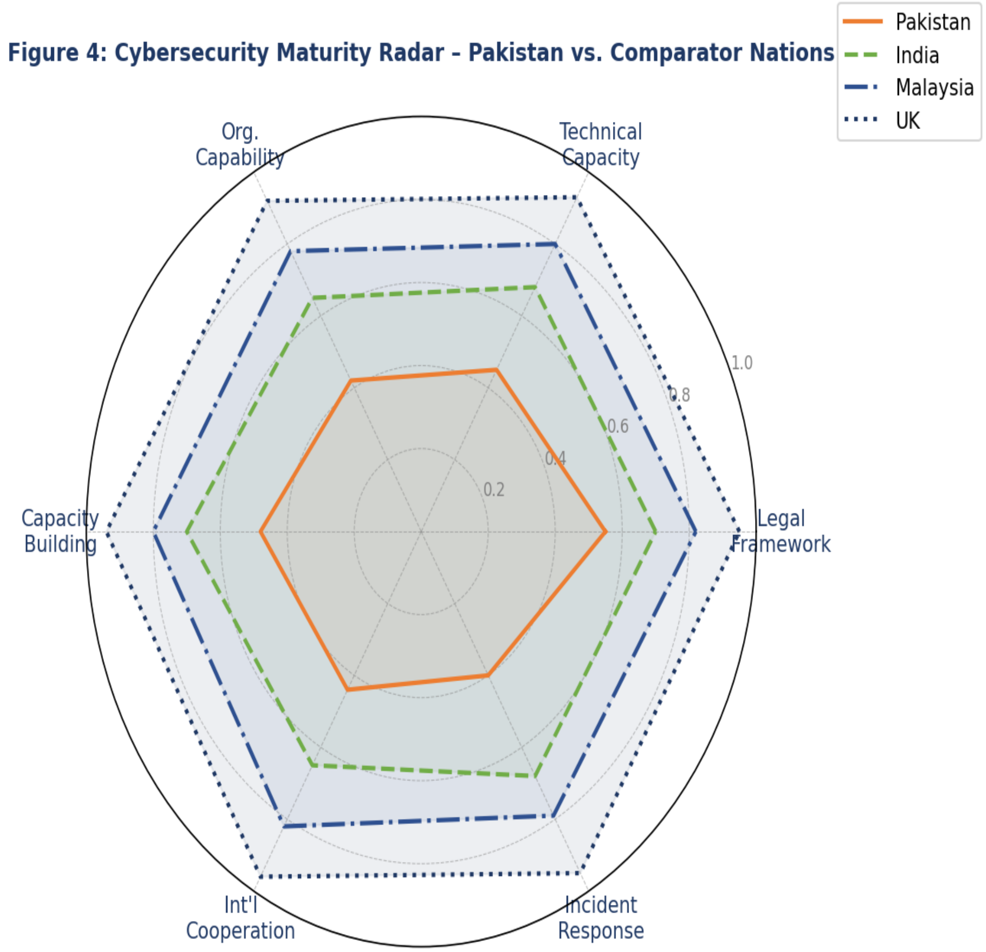


Source: Authors' framework based on NCS Policy 2021 and NIST CSF 2.0 (NIST, 2024).

Figure 2: Cybersecurity Governance Framework of Pakistan. Reference: The framework presented by its authors is grounded on NCS Policy 2021 (MOITT, 2021), and NIST CSF 2.0 (NIST, 2024).

Pakistan's Position in Global Cybersecurity Indices

The position of Pakistan on the global scales of cybersecurity demonstrates that there is a large disparity between the digital goals and the security readiness of this country. The Global Cybersecurity Index (GCI) 2020, created by ITU, placed Pakistan in the Evolving category, and all five pillars of its score were better than in 2018, yet it remained lower than other countries in the region, including India, Malaysia, and Sri Lanka (ITU, 2020). As Figure 1 indicates, the most notable negative performance of Pakistan is observed in the technical measures and the organisational measures pillar that can be seen as the capacity and institutional gaps established throughout this paper (ITU, 2021a). Pakistan has achieved 88 in the NRI 2023 (WEF, 2023b), which shows a growing digital ecosystem, but the supporting infrastructure, such as cybersecurity, has fallen behind the rate at which it is adopted. Digital Society Index, created by the Economist Intelligence Unit and Cybersecurity Dashboard by the BSA Software Alliance rank Pakistan continually under the global median in governance indicators, which have reputational and commercial expenses as the global digital trade partners question the security stance of their Pakistani peers (BSA Software Alliance, 2022; EIU, 2022).



Source: ITU GCI (2020); author-constructed indices drawing on GCI, NRI, and national cybersecurity assessments.

Figure 3: Cybersecurity Maturity Radar- Pakistan vs. Comparator Nations. Reference: ITU GCI (2020); indices that were prepared by the author based on GCI, NRI, and national cybersecurity indexes.

Pakistan's Legislative and Regulatory Environment

Prevention of Electronic Crimes Act (PECA) 2016

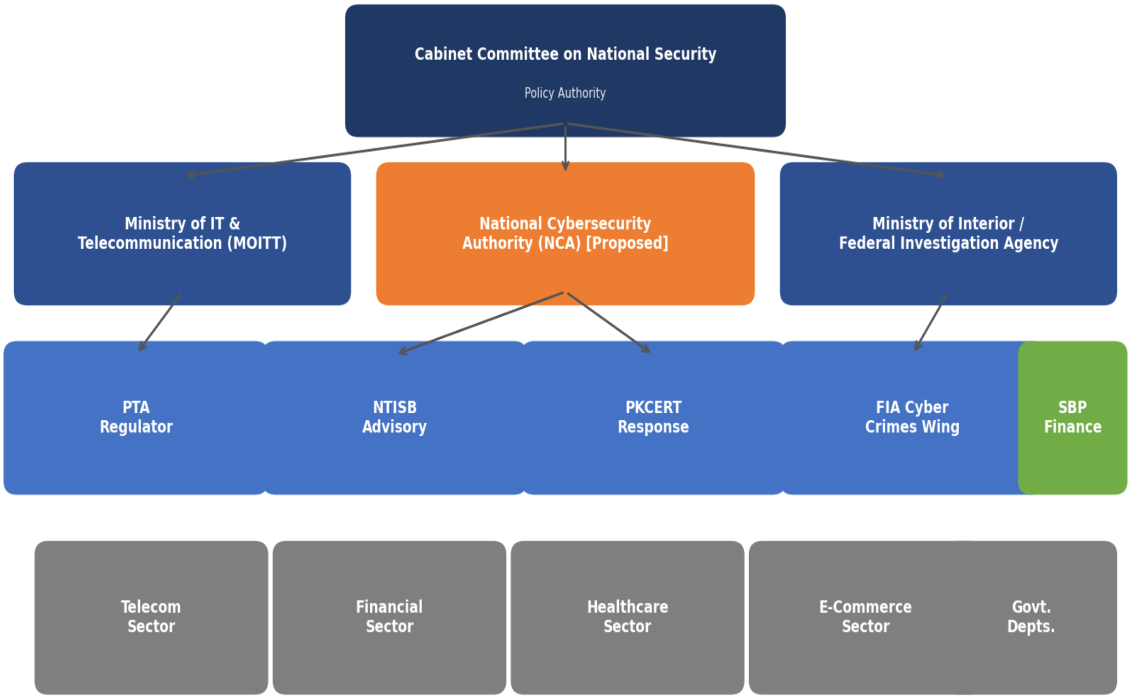
PECA 2016 is the first law in Pakistan that defines the issue of cybercrime and provides a legal framework for the management of cybersecurity (Government of Pakistan, 2016). The Act makes it an offence to access information systems, data, and conduct cyberterrorism, cyberstalking, electronic fraud, and online harassment illegally, and defines the punishments for different levels of severity. It also gives investigative capacities to law enforcement agencies and sets up a system of international collaboration in the investigation of cybercrime (S. Khan et al., 2019). PECA 2016 has aroused a lot of controversy. Civil societies, digital rights advocates, and the law community have asserted that some of the provisions, especially those touching on online defamation and content regulation, are so wide and have been applied to stifle good political expression and journalism (V. Sharma & Anil, 2024; Vardanyan et al., 2022). This scandal has complicated the process of establishing a national consensus on cybersecurity policy and has given some stakeholders the sense that cybersecurity laws are not intended to enhance security but are more of a political instrument (Alsharif & Hnit, 2025; Elliott et al., 2021). Cybersecurity-wise, PECA has serious limitations; in general, it is purely technical. The scope of the definition in the Act fails to keep up with the fast-changing threat centre, and its application has practical challenges that are caused by the lack of technical skills in the Federal Investigation Agency (FIA, 2024). Reporting centers According to PECA, the Cybercrime Reporting Centre of the FIA reports a caseload that has increased between 14,500 cases and 2024 (FIA, 2024), which is much faster than institutional capacity development. Changes to PECA, such as those made in 2022, still bring up a controversy regarding the need to prioritise security over civil liberties (Imran & Kazmi, 2025; Leghari et al., 2024).

National Cybersecurity Policy 2021

The National Cybersecurity Policy 2021 of Pakistan is a more recent and all-encompassing effort at developing a consistent national cybersecurity approach (MOITT, 2021). It models a National Cybersecurity Authority (NCA) as the highest authority on cybersecurity regulation, which is based on the examples of the UK NCSC (NCSC, 2023), Australia ACSC (ACSC, 2023), and Singapore CSA (CSA, 2023). The Policy is ambitious, and the implementation has also been highly hampered by structural issues. By 2025, the suggested National Cybersecurity Authority is expected to be operationalised, and the functions are still spread across various agencies, such as NTISB, PTA, PKCERT, and MOITT (Zeb & Rahim, 2025a). This fragmented form of governance, which Gondal and Ahmed (2021) refer to as the governance dispersion, is the biggest structural vulnerability of cybersecurity governance architecture in Pakistan. The Policy also fails to provide specific implementation schedules, specific financial commitments, and specific performance measures, which are weaknesses typical of the cybersecurity strategies in poorer countries (Asif, Ali, et al., 2025; Karnouskos, 2022).

Regulatory Bodies and Their Roles

The cybersecurity mandate of PTA consists of issuing cybersecurity directives to licensed telecom operators, applying technical standards, and providing internet regulation under PECA (PTA, 2023; PTA, 2022). PTA has already made a number of circulars in connection with the cybersecurity requirements, such as SIEM requirements, yet those requirements are not consistently implemented throughout the industry (Chang & Wei-Liu, 2022; Seng, 2024). The National Telecom and Information Technology Security Board (NTISB) is the cybersecurity advisory body to the Government of Pakistan that assists in providing threat intelligence, security advisories, and guidance to federal ministries and departments (Iqbal & us Shan, 2024a). NTISB has been engaged in sending security alerts on state-sponsored threat actors targeting government networks, including those which can be attributed to advanced persistent threat (APT) groups based in India (SideWinder, APT36) and China (APT41) (Clarke et al., 2023). Pakistan Computer Emergency Response Team (PKCERT), which is an entity set up by MOITT, is tasked with leading the incident response, disseminating threat intelligence, and offering technical support to the impacted organisations (PKCERT, 2024). The capacity of PKCERT is still limited in relation to the extent of its mandate. The level of staffing of about 45 analysts is not favourable in comparison with 200+ staffing of CERT-In India or 120 personnel of My CERT Malaysia (S. Khan et al., 2023). It is generally accepted that one of the priorities would be the development of a more empowered and well-resourced national CERT (Guarda & Vardanian, 2024; Yamin, 2021).



Cabinet Committee on National Security
Policy Authority
Ministry of IT & Telecommunication (MOITT)
National Cybersecurity Authority (NCA) [Proposed]
Ministry of Interior / Federal Investigation Agency
PTA Regulator
NTISB Advisory
PKCERT Response
FIA Cyber Crimes Wing
SBP Finance
Telecom Sector
Financial Sector
Healthcare Sector
E-Commerce Sector
Govt. Depts.

Figure 6: Pakistan's Cybersecurity Institutional and Regulatory Architecture

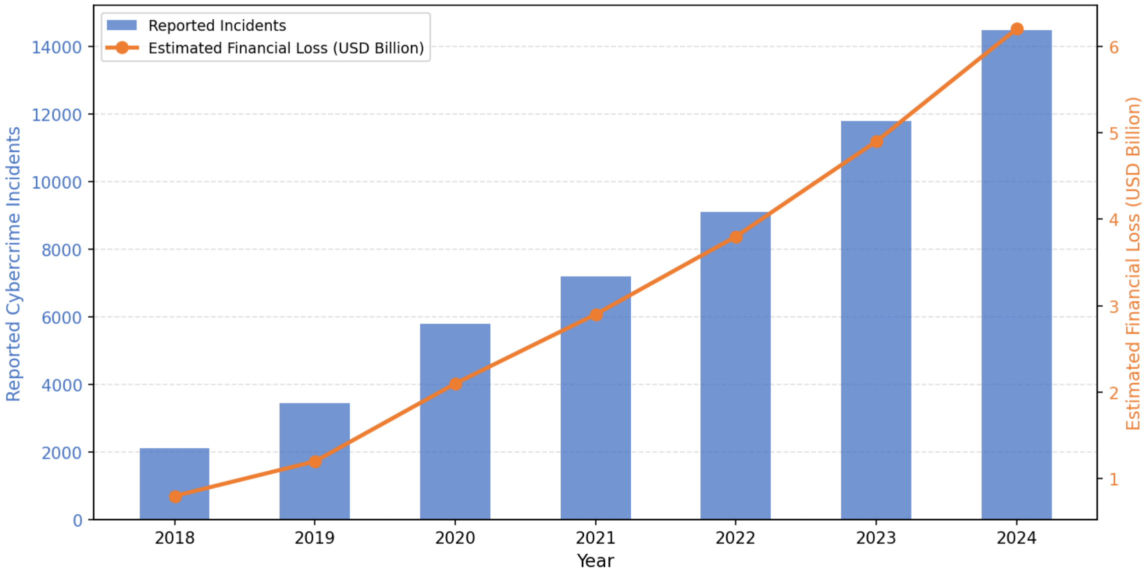
Source: Author's compilation based on MOITT organizational structures, NCS Policy 2021, PECA 2016.

Figure 4: The Cybersecurity Institutional and Regulatory Architecture in Pakistan. Source Author compiled it, according to MOITT (2021), PECA (2016), and PTA (2023) structural designations.

Sector-Specific Regulatory Frameworks

The State Bank of Pakistan (SBP) has been particularly active in the financial sector, providing documents such as Cybersecurity and Technology Controls Guidelines (SBP, 2023), a Risk Management Framework (SBP, 2021), and requirements for incident reporting, third-party risk management, or business continuity planning. The regulatory strategy adopted by the SBP is the best practice within the Pakistani context of the public sector and has proven to be effective in enhancing the cybersecurity practices of licensed financial institutions (Afzal et al., 2024; M. Khan, 2024). SECP has also published cybersecurity policies on listed firms and regulated entities (SECP, 2022), which are voluntary in many types of organisations. This may represent a considerable gap since healthcare is an industry that depends on digital health records and telemedicine platforms that lack a specific regulatory framework due to the sensitivity of health information and the life-saving aspects of medical system breaches (Bin Naeem et al., 2024; Naseem, 2024). The fast-growing e-commerce industry in Pakistan also does not have sufficient sector-specific cybersecurity requirements, and, as a result, consumer data is regularly not well-secured (Héroux & Fortin, 2020; Sultan et al., 2025).

Figure 3: Cybercrime Incidents and Financial Loss Trends in Pakistan (2018–2024)



Source: FIA Cybercrime Reporting Center (2024); PTA Annual Reports (2019–2024); Author estimates.

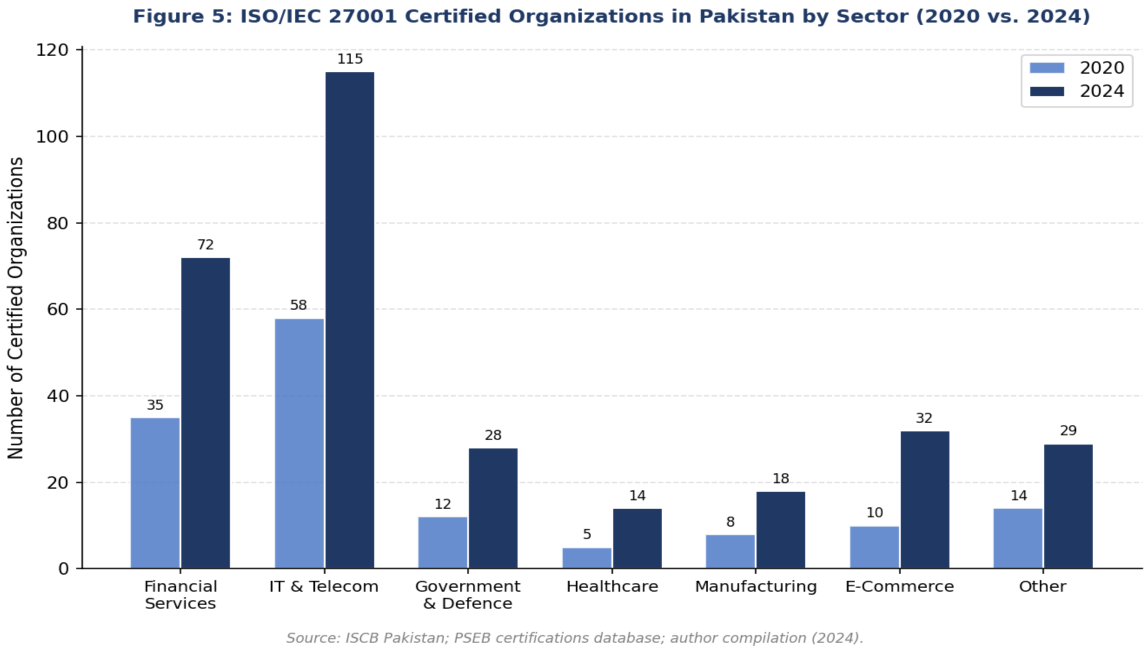
Figure 5: Trends in Cybercrime Incidents and Financial Loss in Pakistan (201824). To obtain the values in this table, the author used the FIA Cybercrime Reporting Centre (2024), PTA Annual Reports (20192024), and personal estimates.

Risk Management Frameworks in Pakistani Organisations

Cybersecurity as an application of enterprise risk management (ERM) means that companies need to identify, evaluate, rank, and address information security risks as part of their business goals and risk tolerance (Nawaz et al., 2019; Tahir et al., 2025). A large part of the overall economy, such as SMEs, state bodies and institutions, as well as operators of critical infrastructure, run unstructured risk management procedures (Butt & Khan, 2020; Shah et al., 2020). Studies into the financial sectors of Pakistan suggest that large commercial banks, which are under the SBP regulatory pressure, have developed comparatively advanced cybersecurity risk management, such as specially designed and dedicated information security functions, formal risk assessment processes, security operations centres (SOCs), and incident response services (Ahmed et al., 2025; Hussain et al., 2025). Most government establishments have a significant dearth of these capabilities. The Federal Board of Revenue (FBR) systems data breach of 2021 that disclosed sensitive data of millions of Pakistanis taxpayers was a vivid example of the practical implications of poor and poorly managed cybersecurity governance in government (Amjad, 2026; Sadiq, 2025b).

ISO 27001 Adoption and Certification Trends

The use of ISO/IEC 27001 certification offers an effective proxy variable of organisational cybersecurity maturity (Laghnimi et al., 2024; Makhija, 2021). The base of Pakistan's ISO 27001 certification has been increasing continuously, mainly due to the export of IT services and other commercial service providers with extensive international client contracts where certification is frequently a condition, and the financial sector, where it is prescribed by regulatory bodies (Podrecca & Sartor, 2023). The total number of certified organisations has increased by a factor of about two since the number of certified organisations was around 142 in 2020, to an estimated 308 in 2024, with the highest number of results in the IT and telecom sector (see Figure 6). The major issue is the so-called certification theatre whereby the organisations attain certification with the main aim of securing profits without truly adopting the security culture and practices that the standard envisages (Jevelin & Faza, 2023; Pathirana & Wilenius, 2025). The successful monitoring of ISO 27001 is impossible without the long-term commitment of senior management, sufficient allocation of resources, and a real organisational culture of security (Todström, 2024), which are not evenly distributed in Pakistani organisations where the certification has already been obtained (Ramli et al., 2025).



Source: ISCB Pakistan; PSEB certifications database; author compilation (2024).

Figure 6: Certified Organisations by Sector of the ISO/IEC 27001 in Pakistan (2020 vs. 2024). Source: ISCB Pakistan; PSEB certifications database; ISO Survey (2023); author compilation.

Cybersecurity Incident Response Capabilities

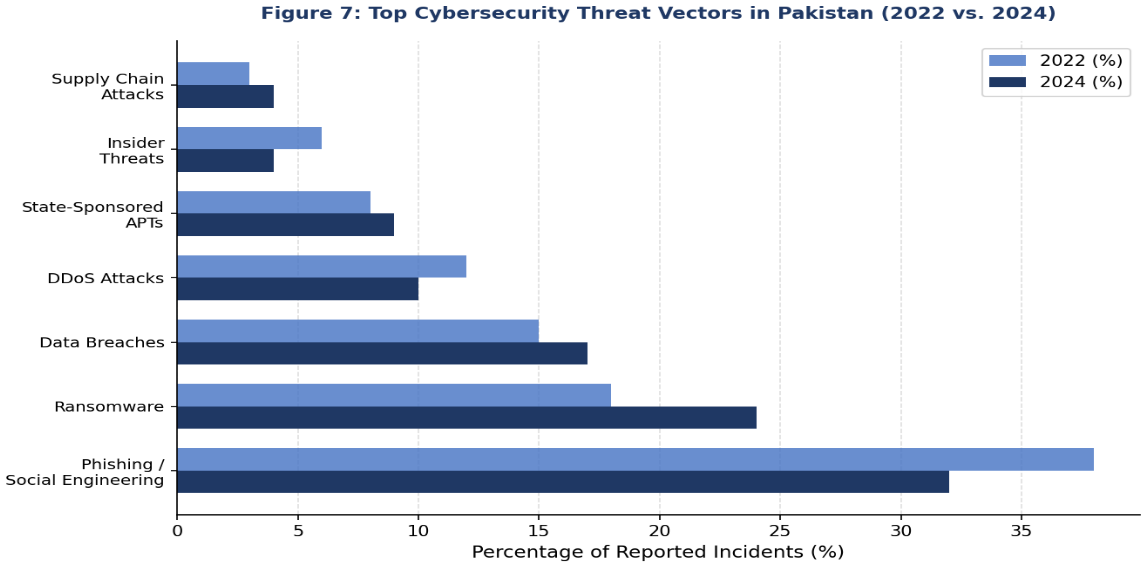
The capabilities of incident response in Pakistani organisations differ dramatically in terms of their sphere, size, and ownership (Iqbal & us Shan, 2024b; Qasim et al., 2025a). Financial institutions, telecommunication firms, and IT services firms with large sizes have invested in security operations centres, incident response teams, and response procedures relying on playbooks (AlMoqbali, 2022; SBP, 2023). Most organisations, nevertheless, do not have focused incident response capacities, but rather rely on informal responses, which often lead to failure to detect, respond sufficiently, and cause long-term recovery periods (Naseer et al., 2023; Umar et al., 2025). Under-reporting is a severe problem. The tendency of cultures and businesses to uphold the image instead of transparency, coupled with the lack of the disclosure obligation of incidents that is compulsory in most industries, provides powerful incentives to hide the events (Digital Rights Foundation, 2021; Kashan et al., 2022). Such under-reporting denies PKCERT and regulators of the sector the incident information they require to recognise the threat patterns, to generate threat intelligence, and to offer guidance, developing a negative feedback loop continuing to sustain systemic vulnerability (ENISA, 2022; ITU, 2021b).

Human Capital and Cybersecurity Awareness

Human aspect of cybersecurity governance is also always defined as the most vulnerable, as well as, the most valuable point of investment (Shen et al., 2023; Spencer, 2024). Attacks of phishing, social engineering, and insider threats are based on human weaknesses and not technical weaknesses (Parvez, 2025; Shafik & Khang, 2024). The issue of employee awareness on cybersecurity is particularly a concern in Pakistan among employees and IT professionals (M. S. Malik & Islam, 2019; Ramim & Hueca, 2021). The higher education sector in Pakistan is starting to react to the demand, and more and more universities have started providing cybersecurity courses at both undergraduate and graduate levels (Choi, 2025; Kondhar et al., 2023). Nevertheless, the number of trained cybersecurity workers still remains significantly under the demand. According to PSEB (2024) estimates, there will be a gap of about 25,000 cybersecurity talent positions in 2024, which is in line with regional workforce deficit data (Shan et al., 2025). The Pakistani cybersecurity diaspora operating in developed countries is a potential source of knowledge that is underutilised (World Bank, 2021).

Business Continuity and Disaster Recovery

Organisational resilience is more than incident response to include business continuity planning (BCP) and disaster recovery (DR), the ability to sustain the necessary operations in response to disruptions and recover normal operations post-disruption (Aliya & Nicola, 2024; Raimi, 2023). In Pakistan, BCP and DR capabilities are not even distributed. BCP and DR are comparatively strong in the financial sector, which is predetermined by the needs of SBP (Osman & Rahman, 2024). Infrastructure operators, government institutions, and SMEs usually possess less strength (Asif, Shah, et al., 2025; Das, 2022). The COVID-19 crisis resembled a stress test that demonstrated the capabilities of digital technologies to continue operations under the conditions of a crisis and the vulnerability of the poorly protected remote access schemes (ENISA, 2022; Lallie et al., 2021). The quick transition to remote working opened new points of attack on home networks, personal devices, and consumer-based VPN tools that were utilised by attackers around the world, including in Pakistan (Rizwan, 2023). In certain sectors, investment in secure remote access and endpoint security has increased faster as a result of the pandemic experience, but lessons have been inconsistently implemented (Saeed et al., 2023).



Source: PKCERT Threat Reports (2022, 2024); FIA Cybercrime Center; NTISB Security Advisories.

Figure 7: Leading Cybersecurity Threats in Pakistan (2022 vs. 2024). This information can be obtained in the PKCERT Threat Reports (2022, 2024), FIA Cybercrime Center and NTISB Security Advisers.

Key Challenges and Systemic Gaps

Institutional Fragmentation and Coordination Failures

The institutional fragmentation is, perhaps, the most basic structural issue in the governance of cybersecurity in Pakistan (Qasim et al., 2025b; Zeb & Rahim, 2025b). The responsibility of cybersecurity is shared among NTISB, PTA, PKCERT, MOITT, FIA, the Ministry of Defence, NADRA and sector regulators lacking a clear apex body, defined coordination mechanisms and national posture (Azhar et al., 2025). This fragmentation leads to overlap of mandate, lack of coverage, incompatible priorities, and ineffective resource usage (Ali, 2019). The suggested National Cybersecurity Authority proposed in the 2021 Policy would, once fully implemented, overcome most of these issues, but the issue of institutional consolidation is still confronted by opposition from most agencies unwilling to relinquish control (Azam et al., 2025; Bhatti & Afraz, 2025).

Technical Capacity Deficit

The cybersecurity governance of Pakistan is characterised by an omnipresent lack of technical capacity in all levels of government and a significant number of organisations in the private sector (Arshad et al., 2024; Mubeen & Usman, 2026). Police departments do not have the necessary forensic capacity and skills to research cybercrime (Hafeez & Tahir, 2025; Sadat et al., 2025). Regulatory authorities do not have technical personnel to provide significant security audits of the entities that are being regulated (M. M. Malik, 2024). The IT divisions of the government do not possess the capability to design secure systems, implement them, and operate (Tahir et al., 2019; Watto et al., 2024). In this lack of capacity is increased by uncompetitive government IT pay and the loss of qualified professionals to the corporate sector and foreign prospects (Nazuk et al., 2025).

Regulatory Gaps and Enforcement Weaknesses

In spite of PECA 2016, the National Cybersecurity Policy 2021, and other industry-specific guidelines, there are major gaps in the regulatory environment of cybersecurity in Pakistan. No universal data protection legislation that incorporates rights of data subjects and the responsibilities of data controllers can be compared with GDPR which aims at removing the legal gap of data protection in all sectors (Kaifa et al., 2025; Nazuk et al., 2025). And the Personal Data Protection Bill that has been in development since 2018 has not been adopted yet, which means that Pakistan has no legal framework to rely on to regulate personal data (Bokhari, 2023). Regulations are either violated unevenly or have no effect at all even in places where they do exist: the FIA has limited resources to investigate cybercrime, which currently is a vast amount of reported cases compared to its capabilities (Muhib et al., 2025), and even the judicial system has little resources to prosecute cybercrime offenders due to inadequate knowledge of digital evidence (Habib et al., 2024).

Supply Chain Security

The digital economy of Pakistan is highly interconnected with the global supply chains, which pose a high third-party cybersecurity risk (Boyens et al., 2022). The organisations that use software, hardware and managed services within Pakistan, such as government agencies, use products of foreign origin, most of which are located in jurisdictions with varying security standards and threat environments. The SolarWinds supply chain attack (2020) has shown the world that when an attack through just one breach of a trusted vendor is performed, it can spread across thousands of downstream organisations (Chishti et al., 2025). There are similar vectors in the technology ecosystem of Pakistan, which are largely not covered by the existing governance schemes (Kausar & Laghari, 2025).

Emerging Threats: Artificial Intelligence and Deepfakes

The fast inclusion of artificial intelligence (AI) into offensive and defensive cybersecurity is a new problem in the governance structures in Pakistan, which were created in a pre-AI-weaponisation era

(Brundage et al., 2024; Taddeo et al., 2021). Such AI-enhanced phishing, malware running autonomously, and deepfaking-related fraud can already be observed in the threat environment in Pakistan (NTISB, 2023; PKCERT, 2024). Fraud, extortion, and disinformation are especially worrying since deepfake technology is widely abused in Pakistan due to the already tense information environment and the rather low media and digital literacy rates of the country (Oxford Internet Institute, 2023; Freedom House, 2023). The governance frameworks of cybersecurity in Pakistan have not yet considered AI-enabled threats, which should be addressed in the near future.

Policy Recommendations

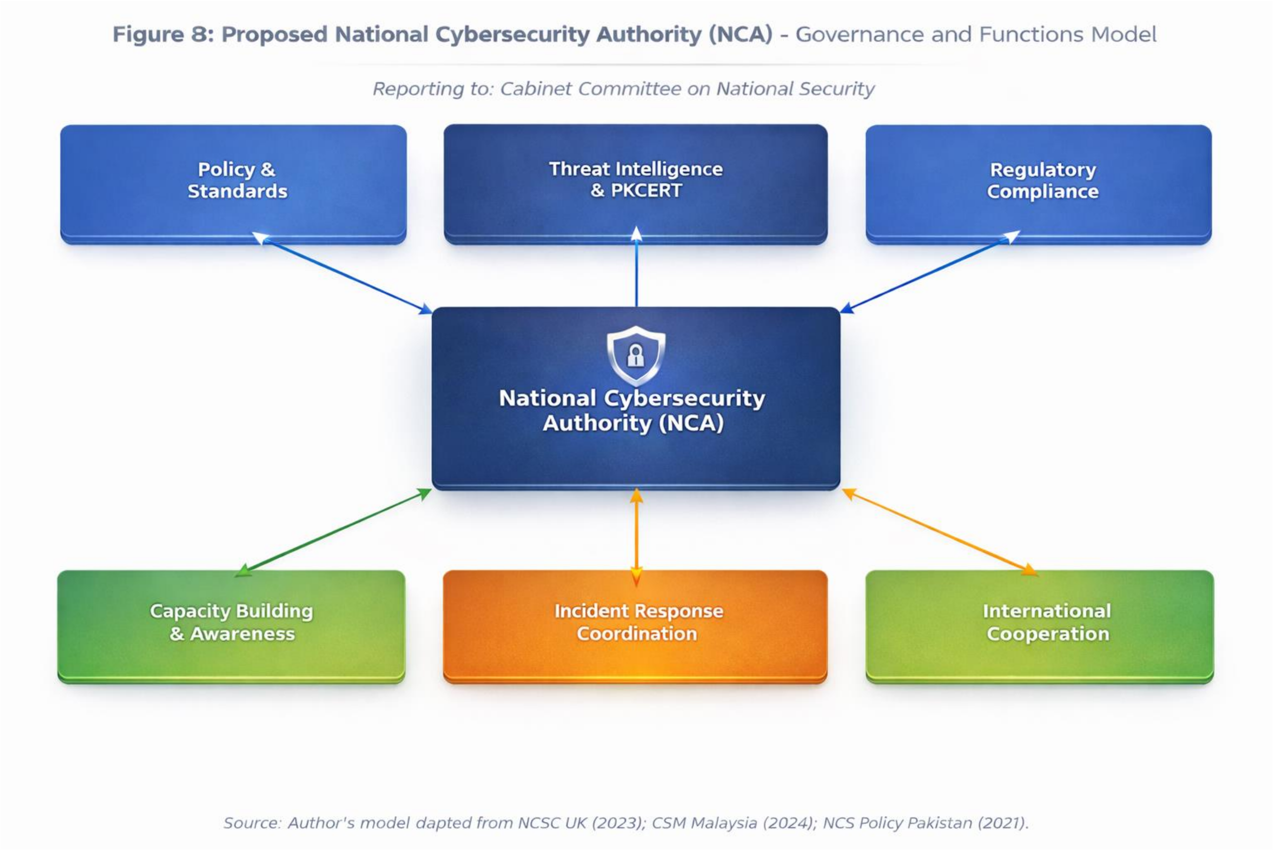


Figure 8: Proposed National Cybersecurity Authority (NCA) - Governance and Functions Model

Reporting to: Cabinet Committee on National Security

Policy & Standards
Threat Intelligence & PKCERT
Regulatory Compliance
National Cybersecurity Authority (NCA)
Capacity Building & Awareness
Incident Response Coordination
International Cooperation

Source: Author's model dapted from NCSC UK (2023); CSM Malaysia (2024); NCS Policy Pakistan (2021).

Figure 8: National Cybersecurity Authority (NCA) Governance and Functions Model Proposal. Bases: The model created by the author is based on NCSC UK (2023); CSM Malaysia (2024); NCS Policy Pakistan (2021).

Establish a Unified National Cybersecurity Authority

The creation of the National Cybersecurity Authority (NCA) as proposed in the 2021 Policy (MOITT, 2023), with the model of the NCSC in the UK (NCSC, 2023), the CSM in Malaysia (Malaysia, 2024), and the CSA in Singapore (CSA, 2023) should be a priority for Pakistan. According to Figure 8, NCA is supposed to have the mandate to organise PKCERT, communicate with NTISB and PTA, establish standards that critical infrastructure operators have to follow, represent Pakistan in global forums, and issue compulsory guidelines on incident reporting. The NCA is expected to have specific legislation and sufficient funds (internationally standardised as 0.05–0.10% of government IT spending) and an effective chain of accountability to the Cabinet Committee on National Security (Batool et al., 2025).

Enact Comprehensive Data Protection Legislation

The Personal Data Protection Bill is the law that should be enacted as a first priority, creating a detailed legal framework that balances the rights to privacy with justified business and security interests modelled after GDPR (2016) but adjusted to the situation in Pakistan (MOITT, 2023; Privacy International, 2023). It should be stated in the legislation the creation of a special Data Protection Authority, active rights of the participants of the data processing, obligatory notification of breach of all data controllers within 72 hours and serious fines to non-observance(Voigt & Von Dem Bussche, 2017b).

Mandate Sector-Specific Cybersecurity Standards for Critical Infrastructure

Based on the model of the SBP (SBP, 2023), the government needs to establish and require industry-specific minimum cybersecurity requirements for all the critical infrastructure industries: energy, water, telecommunications, transport, healthcare, and e-government. These standards are supposed to be risk-based instead of being prescriptive (NIST, 2024; ISO, 2022), including supply chain security evaluations (Val et al., 2024), frequent penetration testing, incident response strategy development and testing, and obligatory incident reporting. The strategy must be based on the NIS2 Directive (European Parliament, 2022) and the CISA model of protection of critical infrastructure (CISA, 2023), but should be adjusted to the resource limitations available in Pakistan.

Invest in National Cybersecurity Capacity Building

The governmental agencies are to implement a National Cybersecurity Capacity Building Program with dedicated resources that would cover the shortage of talents in industries (ISACA, 2023; (ISC) 2, 2023; PSEB, 2024). The program must include cybersecurity education scholarships, support on professional development of government employees in cybersecurity, an effective government career path to cybersecurity, compulsory cybersecurity training on all government employees, and public education. The collaboration with the ITU (ITU, 2021), UNDP (UNDP, 2021), and the networks of diaspora professionals should be actively sought. Blueprints (CSA, 2023; KISA, 2023) can be taken based on the effective models of cybersecurity workforce development of the experience of Korea and Singapore.

Strengthen International Cybersecurity Cooperation

The first step is to ensure that Pakistan ratifies the Budapest Convention on Cybercrime, the leading international instrument of cybercrime cooperation, which would mean the commitment to the global standards and the benefits of the mutual legal assistance treaty (MLAT) to 68 signatory countries (CoE, 2023; UNODC, 2021). Additional steps that Pakistan should take are to seek bilateral cooperation on cybersecurity with major partners such as the US, EU member countries, and regional allies; be an active participant of the SCO and OIC cybersecurity working groups (SCO, 2023; OIC, 2022); and join ITU Global Cybersecurity Agenda (ITU, 2021). The Tallinn Manual 2.0 (Schmitt, 2017) offers the concept of the involvement of the principles of international law in cyberspace, which the diplomatic community of Pakistan can actively participate in.

Develop a National Cyber Resilience Strategy

In addition to threat prevention and compliance, Pakistan should have a National Cyber Resilience Strategy that considers that effective cyberattacks are unavoidable and aims at reducing the impact and speed of recovery (Anjum, 2022). Frequent exercises on cyber resilience on a country level, useful to the strategy, include cyber resilience exercises such as the Waking Shark series (NCSC, 2023) in the UK and the Exercise SG Cyber Safe (CSA, 2023) in Singapore.

Address Emerging Threats: AI Governance and Deepfakes

The governance structures of cybersecurity in Pakistan ought to be revised proactively to respond to the AI-driven threats. This involves the creation of a national AI security working group in the NCA to oversee AI-enabled threats evolutions, preparation of guidelines for the responsible development of AI by domestic technology firms, and integration of AI security in regulatory standards of specific sectors. Combating the fraud through deepfaking should be a special provision in PECA amendments, the creation of public awareness of the issue through media literacy programs, and the establishment of the technical standards of authenticity of digital content (Partnership on AI, 2023; Oxford Internet Institute, 2023).

Conclusion

Pakistan is at a very crucial crossroads in its cybersecurity governance. The key aspects of a national cybersecurity governance framework are already in existence: PECA 2016, the National Cybersecurity Policy 2021, the regulatory framework, and the increasing group of cybersecurity specialists. However, these components are yet to manifest into an effective, unified system that can improve the online infrastructure of Pakistan, secure the information of citizens, and advance the goals of the national development. As it has been demonstrated in this paper, the issues related to cybersecurity governance in Pakistan are both structural and technical. The system is vulnerable to institutional fragmentation, insufficient resource distribution, lapses in enforcement, and regulatory loopholes, which can only be prevented through technical means. To ensure the relationship between cybersecurity governance aspirations and reality in Pakistan is bridged, the politics, sufficient financial allocation, and an actual whole-of-society commitment to create a culture of cybersecurity awareness and responsibility are essential to achieve this. The relative approach presented in this paper would imply that Pakistan does not have to reinvent the wheel. The models of cybersecurity in India in CERT-In (MeitY, 2022) and Singapore in CSA model framework (CSA, 2023) discuss practical blueprints, which can be adapted to the Pakistani institutional background with the help of the Cybersecurity Act 2024 of Malaysia (Malaysia, 2024). Technical guidance that has the potential to inform national standards and regulatory requirements is international frameworks, NIST CSF 2.0 (NIST, 2024), ISO/IEC 27001:2022 (ISO, 2022), and the NIS2 Directive (European Parliament, 2022). Budapest Convention (CoE, 2023) and the Global Cybersecurity Agenda of the ITU (ITU, 2021) provide avenues of tapping into external knowledge. The stakes are high. The global digital economy, foreign investment inflow, and the development of trust in digital government services by the citizenry increasingly require proper cybersecurity governance. The way forward towards good cybersecurity governance in Pakistan is to shift to the proactive paradigm of resiliency-driven forms of cybersecurity regulation, where cybersecurity is not an imposed regulatory mandate but a strategic necessity carried over into organisational culture, investment choices, and country development strategies.

References

Abbas, H. S. M., Qaisar, Z. H., Ali, G., Alturise, F., & Alkhalifah, T. (2022). Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. *Plos One*, *17*(11), e0274550.

Afzal, M., Ansari, Mohd. S., Ahmad, N., Shahid, M., & Shoeb, Mohd. (2024). Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: An integrated model approach. *Journal of Financial Services Marketing*, *29*(4), 1503–1523. https://doi.org/10.1057/s41264-024-00279-3

Ahmed, S. S. U., Moin, N., & Ahmed, R. (2025). Digitalization in Pakistan Economy: A Review of the Transformation of the Banking Sector. *International" Journal of Academic Research for Humanities"*, *5*(4), 18–25.

Ali, M. (2019). Cybersecurity Frameworks For Critical Infrastructure: A Study Of Current Approaches And Their Implementation. *Computer Science Bulletin*, *2*(01), 81–96.

Aliya, H., & Nicola, H. (2024). *Enhancing Corporate Resilience: A Comprehensive Disaster Recovery Plan for Ensuring Business Continuity in the Age of IoT Security*. https://www.researchgate.net/profile/Henrietta-Nicola/publication/387502238_Enhancing_Corporate_Resilience_A_Comprehensive_Disaster_Recovery_Plan_for_Ensuring_Business_Continuity_in_the_Age_of_IoT_Security/links/6771140ac1b0135465feda0c/Enhancing-Corporate-Resilience-A-Comprehensive-Disaster-Recovery-Plan-for-Ensuring-Business-Continuity-in-the-Age-of-IoT-Security.pdf

AlMoqbali, F. S. H. (2022). *Readiness of Situation Awareness for Cybersecurity Incident Response: A Case of a Finance Organisation in Oman*. Sultan Qaboos University (Oman). https://search.proquest.com/openview/8e54077e76af7b7f9fa0dea34f96787d/1?pq-origsite=gscholar&cbl=2026366&diss=y

Alshabib, H. N., & Martins, J. T. (2021). Cybersecurity: Perceived threats and policy responses in the Gulf Cooperation Council. *IEEE Transactions on Engineering Management*, *69*(6), 3664–3675.

Alsharif, M., & Hnit, H. (2025). Digital human rights: Legal debates and emerging foundations under the international bill of human rights. *Social Sciences & Humanities Open, 12,* 102160.

Amjad, B. (2026). From Cash to Code: Examining the Legal Framework for the Future of Digital Currency in Pakistan. *Journal of Conferences Proceedings Publication*. https://journals.scopua.com/index.php/JCPP/article/view/117

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992

Anjum, A. (2022). Adopting a strategy of urgency to achieve cyber resilience. *NDU Journal*, *36*, 26–37.

Arshad, N., Ahmad, W., & Manzoor, K. (2024). *Unleashing the potential of Pakistan's IT Industry: Building for massive software export growth*. https://rasta.pide.org.pk/wp-content/uploads/05.157-Naveed-Arshad_Paper.pdf

Asif, M., Ali, A., & Shaheen, F. A. (2025). Assessing the Effects of Artificial Intelligence in Revolutionizing Human Resource Management: A Systematic Review. *Social Science Review Archives*, *3*(4), 2887–2908.

Asif, M., Shah, H., & Asim, H. A. H. (2025). Cybersecurity and audit resilience in digital finance: Global insights and the Pakistani context. *Journal of Asian Development Studies*, *14*(3), 560–573.

Azam, A., Khattak, M. U., & Ul Ain, Q. (2025). A comprehensive assessment of Pakistan's national internal security policy framework. *Global Change, Peace & Security*, *36*(1), 21–42. https://doi.org/10.1080/14781158.2025.2474242

Azhar, S., Ahmad, W., & Tahir, M. (2025). AN EXPLORATORY ANALYSIS OF THE NEXUS BETWEEN CYBERCRIME AND NATIONAL SECURITY IN PAKISTAN: EVALUATING THE EXISTING LEGAL FRAMEWORK, INVESTIGATIVE CHALLENGES, AND PROPOSING A COMPREHENSIVE STRATEGY FOR EFFECTIVE CYBERCRIME PREVENTION AND PROSECUTION. *Journal for Current Sign*, *3*(2), 615–632.

Baloch, U., Muhammad, B., & Niaz, T. (2022). Pakistan's Cyber Security Governance: Challenges and Way Forward. *Insight*. https://zinormous.pk/issra/images/issra/01-Insight-Cyber-Security.pdf

Barrett, M., Marron, J., Pillitteri, V., Boyens, J., Witte, G., & Feldman, L. (2017). *The cybersecurity framework: Implementation guidance for federal agencies*. National Institute of Standards and Technology. https://csrc.nist.gov/CSRC/media/Publications/nistir/8170/draft/documents/nistir8170-draft.pdf

Basu, A. (2025). India's Cyber Resilience: Strategy, Financing, and Collaboration. *Asia Policy*, *20*(2), 10–24.

Batool, L., Madni, A., Nadeem, N., & Tariq, S. (2025). DEEPFAKE CRIMES AND LEGAL GAPS IN PAKISTAN: A CRIMINOLOGICAL REVIEW OF PECA IN LAHORE. *Contemporary Journal of Social Science Review*, *3*(3), 1223–1231.

Bhatti, A., & Afraz, T. (2025). *Digital Innovation, Data, And Rights: Reassessing Pakistan's Intellectual Property and Cyber Law Framework*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5990336

Bin Naeem, S., Azam, M., Kamel Boulos, M. N., & Bhatti, R. (2024). Leveraging the TOE framework: Examining the potential of mobile health (mHealth) to mitigate health inequalities. *Information*, *15*(4), 176.

Bokhari, S. A. A. (2023). A quantitative study on the factors influencing implementation of cybersecurity laws and regulations in Pakistan. *Social Sciences*, *12*(11), 629.

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). *Cybersecurity supply chain risk management practices for systems and organizations*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/161/r1/final?utm_source=www.resilientcyber.io&utm_medium=referral&utm_campaign=sbom-management

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., hÉigeartaigh, S. Ó., Beard, S. J., Belfield, H., Farquhar, S., … Amodei, D. (2024). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (arXiv:1802.07228). arXiv. https://doi.org/10.48550/arXiv.1802.07228

BSA Software Alliance. (2022). *Cybersecurity Dashboard: Pakistan Country Profile. BSA.*

Butt, A. S., & Khan, M. (2020). Contingency Factor, Risk Management and Organization Performance: A Case of Pakistani Business Organization. *Abasyn University Journal of Social Sciences*, *13*(1). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=1998152X&AN=145450928&h=9Ss3nAO%2BK9%2Fu3qksX7XvwXVbMvlvpRQRJ0gL9Tb3YJID2ugh8BybfVPQYYFEwJeynRhO2d6oBEka9uu%2F4EzsUQ%3D%3D&crl=c

Calderaro, A., & Craig, A. J. S. (2020a). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Calderaro, A., & Craig, A. J. S. (2020b). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Chang, L. Y., & Wei-Liu, H. (2022). Ensuring Cybersecurity for Digital Services Trade. *JW Kang et Al*. https://books.google.com/books?hl=en&lr=&id=3qynEAAAQBAJ&oi=fnd&pg=PT170&dq=The+cybersecurity+mandate+of+PTA+consists+of+issuing+cybersecurity+directives+to+licensed+telecom+operators,+applying+technical+standards&ots=cFAltpajTT&sig=kGYMx2tEvVpAu6VoA2sqpseTaJc

Chishti, M. M., Ahmad, M. I., & Ahmad, M. (2025). Regulating the Future: A Comparative Analysis of Pakistan's Need for EU-Based Cyber Privacy Frameworks. *Scholar Insight Journal*, *3*(4), 23–34.

Choi, S. (2025). Digital Transformation and Cybersecurity Challenges in Pakistan's Higher Education Institutions. *Kashmir Journal of Academic Research and Development*, *1*(3), 1–9.

Christou, G. (2016). *Cybersecurity in the European Union*. Palgrave Macmillan UK. https://doi.org/10.1057/9781137400529

CISA. (2021). *SolarWinds and Active Intrusion Campaign (Alert AA20-352A). US Cybersecurity and Infrastructure Security Agency*.

CISA. (2023). *National Cybersecurity Strategy Implementation Plan. US Cybersecurity and Infrastructure Security Agency.*

Clarke, R., Ormrod, D., Lim, Y., & Slay, J. (2023). The Evolution of Chinese Cyber Offensive Operations and Association of Southeast Asian Nations (ASEAN). *Journal of Information Warfare*, *22*(1), 44–60.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10). https://www.timreview.ca/article/835

Das, R. (2022). *Business Recovery and Continuity in a Mega Disaster: Cybersecurity Lessons Learned from the COVID-19 Pandemic*. Auerbach Publications. https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.1201/9781003279143&type=googlepdf

Deloitte. (2023). *The Cyber Savvy Board: Governing in the Age of Increased Cyber Threats. Deloitte Insights.*

Digital Rights Foundation. (2021). *Online harassment in Pakistan: Annual report 2020–21. Digital Rights Foundation.*

DiMaggio, P. J., & Powell, W. W. (2000). *The iron cage revisited institutional isomorphism and collective rationality in organizational fields*. https://www.emerald.com/books/edited-volume/14074/chapter-abstract/84962949

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

EIU. (2022). *Economist Intelligence Unit. Digital Society Index 2022: Regional Profiles. EIU.*

Elliott, K., Price, R., Shaw, P., Spiliotopoulos, T., Ng, M., Coopamootoo, K., & Van Moorsel, A. (2021). Towards an Equitable Digital Society: Artificial Intelligence (AI) and Corporate Digital Responsibility (CDR). *Society*, *58*(3), 179–188. https://doi.org/10.1007/s12115-021-00594-8

ENISA. (2022). *European Union Agency for Cybersecurity (ENISA). ENISA National Capabilities Assessment Framework. ENISA Publications.*

European Commission. (2023). *Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). COM(2022) 454 final.*

European Parliament. (2023). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). Official Journal of the European Union.*

Gondal, A. J., Choudhry, N., Bukhari, H., Rizvi, Z., Jahan, S., & Yasmin, N. (2023). Estimation, evaluation and characterization of carbapenem resistance burden from a tertiary care hospital, Pakistan. *Antibiotics*, *12*(3), 525.

Guarda, P., & Vardanian, R. (2024). Certifications and protection of personal data: An in-depth analysis of a powerful compliance tool. *Comp. L. Rev.*, *15*, 27.

Habib, N., Hussain, S., & Ali Uddin Hafee, S. M. (2024). Securing Pakistan's cyberspace: Cyber counterintelligence strengths, weaknesses, and strategies. *International Journal of Innovations in Science & Technology*, *6*(4), 1586–1605.

Hafeez, A., & Tahir, U. (2025). The Economic Dimensions of Sino-Pakistani Technological Cooperation: Balancing Opportunities and Risks in the Global Tech Race. *Perspectives in Education, Development & Social Sciences*, *2*(1), 115–131.

Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: An analysis of the cyber threat landscape and readiness. *Ieee Access*, *11*, 40049–40063.

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd. https://books.google.com/books?hl=en&lr=&id=rygf6axAH7UC&oi=fnd&pg=PP1&dq=Hollnagel,+E.,+Woods,+D.+D.,+%26+Leveson,+N.+(2006).+Resilience+Engineering:+Concepts+and+Precepts.+Ashgate+Publishing.&ots=ir9AOY4Xcc&sig=RlXq1oJuTjOuskfWN1Qemx7cOGU

Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61–76. https://doi.org/10.1080/23738871.2018.1467942

Hussain, M., Akhtar, R., & Mushtaq, S. A. (2025). A comparative study of the implementation of corporate governance legal frameworks in the banking sector of Pakistan: Insights from emerging economies. *The Journal of Research Review*, *2*(02), 08–46.

Imran, M., & Kazmi, S. S. (2025). Role of Social Media in Securitization of Rule of Law Crisis in Pakistan. *Research Journal for Social Affairs*, *3*(5), 1013–1027.

Iqbal, Z., & us Shan, R. (2024a). Pakistan's Cybersecurity Landscape. *CISS Insight Journal*, *12*(2), P105-131.

Iqbal, Z., & us Shan, R. (2024b). Pakistan's Cybersecurity Landscape. *CISS Insight Journal*, *12*(2), P105-131.

ITU. (2021a). *International Telecommunication Union. Global Cybersecurity Agenda: Strategic Framework 2020–2025. ITU Publications, Geneva.*

ITU. (2021b). *International Telecommunication Union (ITU). Global Cybersecurity Agenda: Strategic Framework 2020–2025. ITU Publications, Geneva.*

Javed, T. (2023). Exploring the challenges of E-governance: A case study of Pakistan. *Social Sciences and Business Review*, *1*(2), 1–22.

Jevelin, J., & Faza, A. (2023). Evaluation the information security management system: A path towards ISO 27001 certification. *Journal of Information Systems and Informatics*, *5*(4), 1240–1256.

Kaifa, U., Yaseen, Z., & Muzaffar, M. (2025). A thematic analysis of Pakistan's cybersecurity policies, regulations and implications. *Journal of Climate and Community Development*, *4*(1), 39–54.

Karnouskos, S. (2022). Symbiosis with artificial intelligence via the prism of law, robots, and society. *Artificial Intelligence and Law*, *30*(1), 93–115. https://doi.org/10.1007/s10506-021-09289-1

Kashan, A. H., Mehmood, A., Khan, S. U. R., Aziz, T., & Khan, J. (2022). Implementation strategies of cybersecurity in Pakistan. *Journal of Public Policy*, *2*, 4.

Kausar, S., & Laghari, A. R. (2025). Social Engineering Attacks in Pakistan: Analyzing the Weakest Link in Cyber Security. *Journal of Development and Social Sciences*, *6*(1), 364–374.

Khan, M. (2024). *Impact of Digitalization after COVID-19 on Banking Sectors in Pakistan.* https://www.theseus.fi/handle/10024/874318

Khan, M. F., Raza, A., & Naseer, N. (2021). Cyber security and challenges faced by Pakistan. *Pakistan Journal of International Affairs*, *4*(4), 865–881.

Khan, S., Luo, F., Zhang, Z., Ullah, F., Amin, F., Qadri, S. F., Heyat, M. B. B., Ruby, R., Wang, L., & Ullah, S. (2023). A survey on X. 509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies. *IEEE Communications Surveys & Tutorials*, *25*(4), 2529–2568.

Khan, S., Tehrani, P. M., & Iftikhar, M. (2019). Impact of PECA-2016 provisions on freedom of speech: A case of Pakistan. *Journal of Management Info*, *6*(2), 7–11.

Khan, U. P., & Anwar, M. W. (2020). *Cybersecurity in Pakistan: Regulations, Gaps and Way Forward*. https://mro.massey.ac.nz/items/018f3ed9-5101-4074-9551-e86b72473948

Klimburg, A. (2012). *National cyber security framework manual*. NATO Cooperative Cyber Defense Center of Excellence.

Kondhar, A. K., Mallah, I. A., Shaheen, A., & Shah, A. M. (2023). Cyber Harassment and Digital Dilemma in Higher Education Institutions of Pakistan: Policy and Procedures of HEC Pakistan. *Journal of Asian Development Studies*, *12*(4), 438–449.

Laghnimi, J., Moumane, K., Ahmed, Z., Lamkimel, M., Kacimi, Z., & Wahi, Y. (2024). ISO/IEC 27001 certification in Moroccan companies: Trends and future recommendations. *2024 World Conference on Complex Systems (WCCS)*, 1–6. https://ieeexplore.ieee.org/abstract/document/10765551/

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Lanter, D. (2019). COBIT 2019 Framework Introduction and methodology. *ISACA Schaumberg, IL*.

Leghari, M. A., Wasiq, M. F., Younes, J., & Hassan, B. (2024). Global Legislation Muzzling Freedom of Speech in the Guise of Cyber Security. In H. Jahankhani, G. Bowen, M. S. Sharif, & O. Hussien (Eds.), *Cybersecurity and Artificial Intelligence* (pp. 263–279). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-52272-7_11

Lewis, J. A., Lonergan, E. D., Voo, J., Garson, M., & Ertan, A. (2023). *Evolving Cyber Operations and Capabilities*. Center for Strategic and International Studies. https://ciso2ciso.com/wp-content/uploads/2023/11/Cyber-Operations.pdf

Makhija, A. K. (2021). Information security management systems-evolving landscape and ISO 27001: An empirical study. *Journal of Accounting, Finance, Economics, and Social Sciences*, *6*(1), 9–17.

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. *2023 International Conference on Cyber Management and Engineering (CyMaEn)*, 117–122. https://ieeexplore.ieee.org/abstract/document/10051114/

Malik, M. M. (2024). Cybersecurity and National Security in the Digital Age: Challenges and Vulnerabilities in Governance. *Journal of International Law & Human Rights*, *3*(1), 42–53.

Malik, M. S., & Islam, U. (2019). Cybercrime: An emerging threat to the banking sector of Pakistan. *Journal of Financial Crime*, *26*(1), 50–60.

Meadows, D. (2008). *Thinking in systems: International bestseller*. chelsea green publishing. https://books.google.com/books?hl=en&lr=&id=CpbLAgAAQBAJ&oi=fnd&pg=PR9&dq=Meadows,+D.+H.+(2008).+Thinking+in+Systems:+A+Primer.+Chelsea+Green+Publishing.&ots=LBq9obrBMZ&sig=kPlcNlZPvMS4TrVQUOO2Mlf-q0M

MOITT. (2023). *Ministry of Information Technology and Telecommunication, Pakistan. Personal Data Protection Bill 2023: Draft for consultation. Government of Pakistan.*

Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*, *13*(11), 2020.

Mubeen, M., & Usman, A. (2026). *Cybersecurity Workforce Shortages and Their Implications for Global Power Balance*. https://www.researchgate.net/profile/Ayesha-Usman-12/publication/400345409_Cybersecurity_Workforce_Shortages_and_Their_Implications_for_Global_Power_Balance/links/698074ce42f94d1212a5cbcd/Cybersecurity-Workforce-Shortages-and-Their-Implications-for-Global-Power-Balance.pdf

Muhib, M., Muhib, K., & Muhib, Z. (2025). Pakistan's Cyber Laws and International Legal Standards on Digital Rights. *Policy Journal of Social Science Review*, *3*(3), 151–165.

Naseem, R. (2024). *Two Essays on Pakistan's Digital Policy and Digital Financial Policy: Focusing on Keyword Network Analysis and Cognitive Map Analysis* [PhD Thesis, Hoseo University, South Korea]. https://search.proquest.com/openview/993a50bcc1b9c8cea40d459df69d8f40/1?pq-origsite=gscholar&cbl=2026366&diss=y

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. *Computers & Security*, *135*, 103525.

Naserinia, V., & Ullah, S. (2025). *The Influence of ISO 27001 Standards on Agile Methodology-Trade-offs and Implications*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:2001374

Nawaz, A., Waqar, A., Shah, S. A. R., Sajid, M., & Khalid, M. I. (2019). An innovative framework for risk management in construction projects in developing countries: Evidence from Pakistan. *Risks*, *7*(1), 24.

Nazuk, A., Erkin, A. U. N., Noor, M., & Zahid, R. (2025). Exploring the potential and challenges of E-Governance in Pakistan. *Sustainable Futures*, *10*, 101472.

NCSC. (2023a). *NCSC Annual Review 2023. UK National Cyber Security Centre / GCHQ.*

NCSC. (2023b). *NCSC Annual Review 2023. UK National Cyber Security Centre / GCHQ.*

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly*, *5*(4), 18–38.

Osman, F., & Rahman, H. (2024). Planning for Cybersecurity Incidents and Recovery: Methods for Ensuring Business Continuity and Maintaining Information Assurance. *Algorithms, Computational Theory, Optimization Techniques, and Applications in Research Quarterly*, *14*(9), 1–17.

Parvez, W. (2025). *The Impact Of Digital Illiteracy On Cybersecurity Vulnerabilities: A Demographic Study In Pakistan*. https://jyx.jyu.fi/jyx/Record/jyx_123456789_103514

Pathirana, A. I. W., & Wilenius, M. (2025). *ISO 27001 and Global Privacy Compliance*. https://www.utupub.fi/bitstream/handle/10024/182519/Pathirana_Asanka_Thesis.pdf?sequence=1

Podrecca, M., & Sartor, M. (2023). Forecasting the diffusion of ISO/IEC 27001: A Grey model approach. *The TQM Journal*, *35*(9), 123–151.

PwC. (2023). *Global Digital Trust Insights Survey 2023. Price water house Coopers.*

Qasim, M. S., Ahmad, Z., Maqsood, S., Zafar, S., & Azam, M. (2025a). ASSESSING CYBERSECURITY CHALLENGES AND RESPONSE READINESS IN PAKISTAN: A COMPREHENSIVE ANALYSIS. *Kashf Journal of Multidisciplinary Research*, *2*(01), 115–125.

Qasim, M. S., Ahmad, Z., Maqsood, S., Zafar, S., & Azam, M. (2025b). ASSESSING CYBERSECURITY CHALLENGES AND RESPONSE READINESS IN PAKISTAN: A COMPREHENSIVE ANALYSIS. *Kashf Journal of Multidisciplinary Research*, *2*(01), 115–125.

Raimi, L. (2023). Business continuity and disaster recovery strategies as resilience tools after cyberattacks in toxic enterpreneurship ecosystems. In *Cybersecurity for decision makers* (pp. 349–364). CRC Press.

https://www.taylorfrancis.com/chapters/edit/10.1201/9781003319887-21/business-continuity-disaster-recovery-strategies-resilience-tools-cyberattacks-toxic-enterpreneurship-ecosystems-lukman-raimi

Ramim, M. M., & Hueca, A. (2021). Cybersecurity capacity building of human capital: Nations supporting nations. *Online Journal of Applied Knowledge Management (OJAKM)*, *9*(2), 65–85.

Ramli, A., Darus, M. Y., Ali, F. H. M., Bakar, M. R. A., Kamarzaman, N. S., & Kasiran, Z. (2025). Strengthening Trust and Security through ISO 27001 Compliance: A Conceptual Framework for Information Management. *2025 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, 31–36. https://ieeexplore.ieee.org/abstract/document/11265109/

Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Regulation (Eu)*, *679*(2016), 10–13.

Rizwan, A. (2023). Cybersecurity Management in Modern Businesses: Challenges, Solutions, and Future Directions. *International Review of Business and Social Sciences*, *3*(1), 31–42.

Roba Abbas, K. M., Pitt, J., Vogel, K. M., & Zaferirakopoulos, M. (2023). Artificial Intelligence (AI) in Cybersecurity: A socio-technical research roadmap. *The Alan Turing Insitute*. https://www.turing.ac.uk/sites/default/files/2023-11/ai_in_cybersecurity.pdf

Sadat, A., Lawelai, H., Younus, M., & Nurmandi, A. (2025). Comparative analysis of National Cyber Security Index: A case study of Pakistan and Indonesia. *Kasetsart Journal of Social Sciences*, *46*(1), 460101–460101.

Sadiq, M. N. (2025a). *Digital Governance and Public Policy in Pakistan: Challenges and the Way Forward* [Master’s Thesis, Humanaties and Social Sciences]. http://dspace.bahria.edu.pk:8080/xmlui/handle/123456789/19586

Sadiq, M. N. (2025b). *Digital Governance and Public Policy in Pakistan: Challenges and the Way Forward* [Master’s Thesis, Humanaties and Social Sciences]. http://dspace.bahria.edu.pk:8080/xmlui/handle/123456789/19586

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges faced by the judiciary in implementing cybersecurity laws in Pakistan. *The Critical Review of Social Sciences Studies*, *3*(1), 1052–1066.

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

SBP. (2023). *State Bank of Pakistan. Cybersecurity and Technology Controls Guidelines—Update 2023. SBP, Karachi.*

Schmitt, M. N. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. https://books.google.com/books?hl=en&lr=&id=n9wcDgAAQBAJ&oi=fnd&pg=PR12&dq=Schmitt,+M.+N.+(Ed.).+(2017).+Tallinn+Manual+2.0+on+the+International+Law+Applicable+to+Cyber+Operations.+Cambridge+University+Press.&ots=MIQ_xzligZ&sig=AVxRrfZx_3JQ16OpPUyZS4lmyEA

Seng, N. (2024). Cybersecurity Regulation—Types, Principles, and Country Deep Dives in Asia. *International Cybersecurity Law Review*, *5*(3), 387–411. https://doi.org/10.1365/s43439-024-00127-z

Shafik, W., & Khang, A. (2024). Cybersecurity Techniques in Talent Management and Human Capital Management Systems. In *AI-Oriented Competency Framework for Talent*

Management in the Digital Economy (pp. 353–375). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003440901-22/cybersecurity-techniques-talent-management-human-capital-management-systems-wasswa-shafik-alex-khang

Shah, I., Elahi, N., Alam, A., Dawar, S., & Dogar, A. A. (2020). Institutional arrangement for disaster risk management: Evidence from Pakistan. *International Journal of Disaster Risk Reduction*, *51*, 101784.

Shan, S. A. F., Khan, S., Khan, S. N., Khan, S. B., & ul Islam, M. (2025). High Tech and Innovative Emerging Industries and Pakistan's Policies and Regulations towards Adaptation in the light of China's Strategies of Reverse Engineering. *Journal of Public Policy*, *4*, 1.

Sharma, J., & Jain, A. (2025). Cybersecurity and Crime in Industry 4.0: An Analysis of Legal Aspects of Cybercrime. In G. Kaur, T. Choudhury, & S. Balamurugan (Eds.), *The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0* (1st ed., pp. 19–42). Wiley. https://doi.org/10.1002/9781394242177.ch2

Sharma, V., & Anil, K. (2024). Protecting digital rights of India: Planning for succession at Internet Freedom Foundation (IFF). *Emerald Emerging Markets Case Studies*, 1–26.

Shen, Y., Buchanan Turner, C., & Turner, C. (2023). Cybersecurity training in organization as human capital investment: A qualitative grounded theory analysis. *International Journal of Business and Management*, *18*(4). https://par.nsf.gov/biblio/10428972

Singh, A. K., Siddiqui, Z. A., Singh, S., Singh, A. K., & Siddiqui, T. J. (2024). Recent advances in computational intelligence and cyber security. *Recent Advances in Computational Intelligence and Cyber Security*. https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.1201/9781003518587&type=googlepdf

Slayton, R., & Clarke, B. (2020). Trusting infrastructure: The emergence of computer security incident response, 1989–2005. *Technology and Culture*, *61*(1), 173–206.

Spencer, P. E. (2024). 2024 Sensitive Content Communications Privacy and Compliance Report. *Kiteworks*. https://www.academia.edu/download/116995272/Kiteworks_2024_Sensitive_Content_Communications_Report_FINAL_2024_07_18.pdf

Sultan, S., Amin, M. R., & Hashmi, M. A. I. (2025). The Role of SECP in Ensuring Corporate Accountability in Pakistan. *ASSAJ*, *3*(02), 2290–2302.

Tabansky, L. (2011). Basic concepts in cyber warfare. *Military and Strategic Affairs*, *3*(1), 75–92.

Taddeo, M., McCutcheon, T., & Floridi, L. (2021). Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword. In L. Floridi (Ed.), *Ethics, Governance, and Policies in Artificial Intelligence* (Vol. 144, pp. 289–297). Springer International Publishing. https://doi.org/10.1007/978-3-030-81907-1_15

Tahir, M., Farrukh, T., & Shahid, M. (2019). Cyber Laws and Cyber Security in Pakistan: Myths and Realities. *Global Social Sciences Review*, *4*(1), 485–493.

Tahir, M., Shahzad, M. N., & Sarfraz, Z. (2025). The Study of Effectiveness of Risk Management and Its Impact on Organizational Performance of Pharmaceutical Industry of Pakistan. *Journal of Social Sciences Research & Policy*, *3*(04), 280–294.

Tikk, E., & Kerttunen, M. (2020). *Routledge handbook of international cybersecurity*. Routledge London. https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.4324/9781351038904&type=googlepdf

Todström, S. (2024). *The effects of ISO 27001 certification: An interview study investigating what changes have small to medium-sized organizations in Sweden experienced after an ISO 27001 certification*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1871578

Tsukanov, L. V., & Valiakhmetova, G. N. (2025). Developing Cybersecurity Cooperation within the framework of the GCC: Prospects and Risks. *Уральское Востоковедение. Вып. 15: Ближний Восток–На Перекрестке Путей и Судеб: К Юбилею Академика РАН ВВ Наумкина к 25-Летию Кафедры Востоковедения УрФУ*, 158–164.

Umar, H. B., Wani, T. A., Liem, M., Khan, U. R., & Boyd, J. (2025). Human and Organizational Dynamics in Responding to Cybersecurity Incidents: Lessons from the Australian Healthcare Sector. In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (Vol. 15814, pp. 282–297). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-92833-8_17

Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). Strengthening cybersecurity measures for the defense of critical infrastructure in the United States. *Asian Journal of Research in Computer Science*, *17*(11), 25–45.

Vardanyan, L., Stehlík, V., & Kocharyan, H. (2022). Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. *TalTech Journal of European Studies*, *12*(1), 159–185. https://doi.org/10.2478/bjes-2022-0008

Voigt, P., & Von Dem Bussche, A. (2017a). *The EU General Data Protection Regulation (GDPR)*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Voigt, P., & Von Dem Bussche, A. (2017b). *The EU General Data Protection Regulation (GDPR)*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Watto, O. M., Islam, M., Hussain, S. A., & Shahab, M. (2024). Cyber law and cyber security policies in pakistan: A comparative study with USA, canada and australia. *Pakistan Journal of Humanities and Social Sciences*, *12*(1), 271–277.

WEF. (2023a). *World Economic Forum. Networked Readiness Index 2023 / Global Technology Governance Report. World Economic Forum, Geneva*.

WEF. (2023b). *World Economic Forum. Networked Readiness Index 2023 / Global Technology Governance Report. World Economic Forum, Geneva.*

White House. (2023). *National Cybersecurity Strategy 2023. Executive Office of the President, United States.*

World Bank. (2021). *World dev. Indic.* http://databank.worldbank.org/data/reports.2021.

Yamin, D. T. (2021). Cyberspace management in Pakistan. *Governance and Management Review*, *3*(1). https://journals.pu.edu.pk/journals/index.php/gmr/article/view/4267

Yasin, B. M. (2020). *SDPI's Study Group on Information Technology and Telecommunications*. https://sdpi.org/assets/lib/uploads/Current-Status-of-ICTs-Study-Group-Recommendations%20-1993%20to%202025%20-%20Updated%2022nd%20Jul%2025%20(F).pdf

Zeb, M. A., & Rahim, W. (2025a). Cybersecurity in Pakistan: Legal Gaps, Institutional Challenges, and the Need for a Comprehensive National Strategy. *Research Consortium Archive*, *3*(4), 1454–1465.

Zeb, M. A., & Rahim, W. (2025b). Cybersecurity in Pakistan: Legal Gaps, Institutional Challenges, and the Need for a Comprehensive National Strategy. *Research Consortium Archive*, *3*(4), 1454–1465.