DOI: 10.71317/jgst.2.11.2026.1051
Journal of Global Social Transformation
Journal homepage: https://rjsaonline.org/index.php/JGST

Cyber Threats to Pakistan's National Security: Conceptualizing Counter Measures

Muhammad Nabeel Ulfat[1]
[1] Student, Iqra University, Islamabad, Pakistan.
Email: nabeelraja127@gmail.com

ARTICLE INFO

Submission:
October 13, 2026
Revised:
November 01, 2026
Accepted:
November 06, 2026
Available Online:
November 16, 2026

Keywords:
Cybercrime, Cybersecurity Governance, Cyber Sovereignty, Disinformation, National Security, Pakistan, Realism, Türkiye.

Corresponding author:
Muhammad Nabeel Ulfat
Email: nabeelraja127@gmail.com

ABSTRACT

With the growing reliance on digital infrastructure, Pakistan faces severe cyber security threats that pose a serious threat to the nation's security, state sovereignty and governance. The present study highlights the catastrophic cyber threats facing Pakistan, assesses the efficacy of the existing cybersecurity framework in the country and envisions realistic countermeasures for enhancing the cyber resilience of the nation. In particular, it explores the threats of cyber espionage, financial cybercrime, disinformation, attacks on critical infrastructure and their impact on Pakistan's digital sovereignty. A realist theory is applied in this study, which focuses on the roles of the state, sovereignty and state survival in the anarchic international system. Methodologically, it uses a qualitative approach through the study of a case with document analysis and structured, focused comparison of Pakistan, India and Türkiye. While Pakistan's legal framework, including the Prevention of Electronic Crimes Act (PECA) 2016, and policy framework, the National Cyber Security Policy (NCSP) 2021, provide critical legal and policy foundations, their effectiveness is limited due to overlapping institutional mandates, inadequate technical expertise, weaknesses in the enforcement mechanisms, and lack of coordination. The evolving market in cybersecurity highlights the need for institutional coherence, specialized cybersecurity structures, and centralized coordination, as evidenced by comparative findings from India and Türkiye. The study proposed a phased and integrated approach that includes legal changes, the setting up of a National Cyber Security Authority, technology capacity building and strategic cyber diplomacy. It suggests transitioning from a fragmented and reactive approach to a coordinated and sovereignty-driven approach to bolster Pakistan's cybersecurity, while also considering the limited resources and institutional structures in the nation. The study's contribution to the literature of cyber security governance is the realist approach in the cyber environment in Pakistan and the development of policy solutions for Pakistan's cyber environment.

Introduction

Digital technologies have transformed the nature of the relationship between national security, state sovereignty and governance. Digitalization of government has led to greater exposure to cyber espionage, financial cybercrime, disinformation, and attacks on infrastructure. In recent years, the Internet has become the backbone of national power and sovereignty and thus demands integrated legal frameworks, institutional capacity, qualified personnel, and cooperation—both national and international—in order to ensure the security of the Internet (DeNardis, 2014; Klimburg, 2018; ITU, 2024). While there is a central coordinating structure in National Cyber Security Policy 2021, specific roles, responsibilities and effective enforcement mechanisms are needed for effective institutional coordination (Ministry of Information Technology and Telecommunication & Government of Pakistan, 2021). While the National Cyber Security Policy 2021 (NCSP) is an important step towards creating a safe and resilient digital environment,

issues remain in its implementation, institutional coordination, technical capacity (Ministry of Information Technology and Telecommunication & Government of Pakistan, 2021). The Prevention of Electronic Crimes Act, 2016 (PECA) has a framework to tackle electronic crimes such as unauthorized access to information systems or data, unauthorized copying of data or information and interference with information systems, among others, but there is a need to discuss overall protection of critical infrastructure, and co-ordination of cyber security institutions, more. According to the previous studies, the weaknesses of Pakistan are Cyber Espionage, Financial Cybercrime, and Institutional preparedness (Shad, 2019, Ahmad, 2022). Moreover, disinformation can be digitally coordinated and can affect the public opinion, lack of trust in information sources and in the democratic process, and limit the possibility for informed public debate (Bradshaw & Howard, 2019).

The susceptibility also poses implications on an international relation level, not just an issue of disrupted single digital systems. The realist theory is on the international system of states, power, sovereignty, security and survival (Mearsheimer, 2003, Waltz, 1979). The protection of digital infrastructure, sensitive information, communication systems, is part of state sovereignty and the fact that the internet is a virtual space, without borders, generates tensions between control and interconnection (Corn & Taylor, 2017; DeNardis, 2016). Nye (2016) also notes that attribution of cyber-attacks to actors and the ability to impose credible costs on them are difficult. He distinguishes between four complementary ways in which states can discourage harmful cyber behavior, namely punishment, denial, entanglement, and normative mechanisms. The issues raised point to the need for the effective development of the cybersecurity capabilities and institutional responses within the national policy for national security. So, cybersecurity governance is not just a techno-management task, it is a part of national security.

Despite rising research and policy interest on the cyber vulnerabilities of Pakistan, the question of how Pakistan's institutional fragmentation and digital sovereignty relate to its cyber vulnerabilities has received little attention in the literature. There is a lack of attention in current debates to the interaction of the different cyber threat, legal and institutional dimensions, in other words to an integrated approach in which the different dimensions are connected and linked to state capacities and policy options. Moreover, the models of cybersecurity that have been created in technologically advanced countries may not be easily replicable in Pakistan because of institutional maturity, financial resources and differences in the geopolitical context. To address this, the current study will evaluate and analyze the main cyber threats in Pakistan, compare the current status and effectiveness of the existing cybersecurity legal and institutional framework in Pakistan with other countries like India and Türkiye, and draw conclusions and lessons learned from comparing the two countries using a structured and focused methodology (George & Bennett, 2005).

Main Research Objectives

This study has three objectives:

1. To know the main cyber threats of Pakistan like espionage, cybercrime, disinformation and infrastructure sabotage; and their implications on state sovereignty and governance.
2. To critically assess the effectiveness of the current legal and institutional cybersecurity framework of Pakistan in comparison with India and Türkiye.
3. To think of and envision a package of countermeasures for Pakistan along legal, institutional, technological and strategic lines which could be realistically implemented and based upon a sovereign approach.

Main Research Questions

This study has following questions:

1. **RQ1:** What are the major cyber threats to the national security of Pakistan and how do they impact the national sovereignty, governance and critical infrastructure?
2. **RQ2:** What is the effectiveness of current legal, institutional and policy measures in Pakistan, such as PECA 2016 and NCSP 2021, in combating these threats?
3. **RQ3:** What lessons can be drawn from the practices of two middle powers, India and Türkiye, with similar structural challenges, and what is feasible to adopt for Pakistan's cybersecurity governance?
4. **RQ4:** What are the legal, institutional, technology and strategic countermeasures that can be envisioned for Pakistan based on a realist perspective of cyber sovereignty?

Literature Review and Theoretical Framework

Cybersecurity, National Security and State Sovereignty

The linkage of cybersecurity with national security has been gaining more and more prominence in international relations and in cybersecurity research. As governments, financial institutions and critical services become increasingly reliant on interconnected digital networks, the range of potential impacts of cyber incidents has broadened beyond technical. Cyber security is now recognized as a governance and strategic issue that is about the security of information, digital infrastructure and state functions (DeNardis, 2014; Klimburg, 2018). It also serves as a reminder to consider cyber threats not just in technical terms but as well as their effects on the exercise of state power, institutional capacity and national security.

The literature mentions various cyber threats with different impacts on state security. Cyber espionage refers to the unauthorized access to and acquisition of information or data from computer systems or networks and gaining access to information or data stored on or transmitted through these systems or networks, including information or data of a potentially high value, such as information relating to government, military and strategic communications that could be accessed by unauthorized persons (Banks, 2017; Akram & Malik, 2023). However, identifying the actors involved in cyber intrusions is challenging because technical evidence and political and strategic decision making are needed (Rid & Buchanan, 2015). Cybercrime, including financial fraud and ransomware (Klimburg, 2018), can lead to economic losses and disruption of organizational functions and loss of trust in digital services. Similarly, there is also the potential for organized social media manipulation and disinformation to influence the public debate, alter political communication and undermine faith in democracy (Bradshaw & Howard, 2019). In addition, there are concerns about the attacks against critical infrastructure; that is, attacks that can impact systems beyond those being attacked (Klimburg, 2018). Together, these threats are sufficient to justify any consideration to devote time to cyber security on legal, institutional, technological and strategic levels.

Digital network and State sovereignty are also covered under the Cybersecurity scholarship. The classical concept of sovereignty is grounded on the power of the State within its territorial boundaries; the Internet, however, deals with a transnational architecture, with it being a challenge to establish a state's power. The state and private technology actors are sources of competing authority and control that shape the digital infrastructure, information flows and internet governance (DeNardis, 2014). The sovereignty of the cyberspace therefore relates to the capacity of a state to establish its digital sovereignty, protect its information and have the right to use it. However, international cooperation and individual rights must also be taken into account, along with the need for greater state control (Akhtar & Iqbal, 2025).

Pakistan's Cybersecurity Landscape and Governance Challenges

Studies of Pakistan's cybersecurity landscape highlight the nation's growing reliance on information and communication technology and ongoing issues with cyber readiness. The analysis of Pakistan's cyber threat environment reveals hacking, organized cybercrime, cyberterrorism and cyberwarfare are all relevant areas of concern and the assessment of its preparedness is done under legal, technical, organizational, capacity-development and international-cooperation perspectives (Shad, 2019). This analysis is an important starting point for appreciating the state of cybersecurity as a national preparedness issue as opposed to just a technical incident.

A more recent study has focused on the connection between the laws of cybersecurity and institutional arrangements and national readiness of Pakistan. When evaluating the laws, regulations and policies in the field of Cyber Security, a comparative study of them is carried out to determine what is relevant to Pakistan in comparison to international laws and regulations and the demands of the changing digital environment (Saleem et al., 2024). The discussion of cyber sovereignty in the context of Pakistan's security landscape also indicates that the state has a role to play in safeguarding its national interests through digital infrastructure (Akhtar & Iqbal, 2025). Collectively, these contributions are not a comprehensive assessment of the interaction between legal clauses and the legal obligations and technical capabilities of the cybersecurity governance in the country, but they do contribute to the understanding.

Key components of the cybersecurity policy and the legislation of Pakistan are the National Cyber Security Policy 2021 and the Prevention of Electronic Crimes Act 2016. However, the existence of legislation and policy commitments do not necessarily mean that they have been well implemented. Effective implementation will require enforcement, institutional coordination, technical preparedness and availability of suitable trained staff. The difference is quite substantial because a national cybersecurity cannot be achieved without the effective integration of legal frameworks, organizational arrangements and technical capabilities (Shad, 2019; Saleem et al., 2024).

Comparative Cybersecurity Governance and Research Gap

Comparative research can be helpful in deriving information about the organization of the national cybersecurity strategies in states. For example, a comparative analysis of ten countries shows that national strategies for cybersecurity in the countries contain common priorities like protection of critical assets, investment in research and development, prevention of cybercrime and international cooperation (Odebade & Benkhelifa, 2023). However, the countries under the study have been technologically advanced European countries, Asia Pacific and North America. Therefore, conclusions drawn are applicable as guidance for other countries in light of their shared strategic challenges, but may not be directly applicable to countries that are institutionally and resource-wise different.

The existing research literature provides specific insights in the field of cyber threat, national preparedness, digital sovereignty and cybersecurity governance. The existing literature offers valuable insights into the changing character of cyber threats, national cybersecurity preparedness, national cyber security sovereignty and cyber security governance. Research on the cyber threat environment in Pakistan underscores the issues and weaknesses of Pakistan's increasing reliance on ICT infrastructure and the lack of national readiness (Shad 2019). At the international level, studies on the implementation of national cybersecurity strategies provide insight into the policy choices states make for building cybersecurity capacity and preparedness (Craig et al., 2023). In addition, there has been a focus in the governance literature on the need for coordinated strategies and the involvement of all stakeholders in responding to cybersecurity issues (Savaş & Karataş, 2022). More recently, cybersecurity is also being linked to digital sovereignty, covering issues of technological autonomy, digital resilience and the defense of national digital assets (Katsikas, 2025).

However, there is still potential for a deeper discussion on the interactions among these dimensions in Pakistan. Especially the linkage between cyber vulnerabilities, legal and institutional arrangements, state capacity and digital sovereignty needs to be analyzed further. Comparative analysis between India and Türkiye can be useful to study alternative approaches towards cyber security governance and regional security conditions and institutional arrangements. Comparing the two models is not an attempt to see which one can be directly replicated in Pakistan, but rather to identify practices that could be adapted to Pakistan's institutional and resource context. With this in view, the present study aims to fill the gap of an integrated and theoretically sound evaluation of the cybersecurity issues in Pakistan. It ties together cyber threat analysis with effectiveness of legal and institutional measures and explores comparative experiences to formulate contextually appropriate countermeasures.

Theoretical Framework: Realism and Cyber Sovereignty

The main theory used in this study is realism. The realist school of international relations focus on the centrality of the state in international politics, the anarchic nature of the international system, the distribution of power among states and the quest for security and survival (Waltz, 1979; Mearsheimer, 2001; Lobell, 2017). In the absence of a higher power to ensure their security, states pay attention to their own capabilities and strategic resources (Waltz, 1979). Offensive realism also highlights the importance of relative power and pursuing strategic advantage in a world characterized by uncertainty in international relations (Mearsheimer, 2003).

In cyberspace, realism offers a framework for analyzing the rationale behind the interest of states in the protection of their digital infrastructure, their information and their strategic communication systems. These resources are increasingly used for government purposes, economy and national defense. The fact that a state may have only limited capacity to ensure their acquisition can thus limit its strategic independence and open significant national interests to foreign influence. Internet governance also entails multiple sources of authority and control, and there is a significant link between the digital infrastructure and the role of states in the exercise of its power (DeNardis, 2014). However, in cyberspace the scope of deterrence extends beyond the fear of response – other elements that can deter bad behavior include defensive denial, interdependence, and norms of behavior (Nye, 2016).

Methodology

Research Design

This study has adopted qualitative comparative case study design to analyze the cyber threats to the national security of Pakistan and come up with feasible countermeasures. A qualitative method is suitable as it is a study that is interested in the understanding of cybersecurity threats, the evaluation of legal and institutional arrangements and the implications of such arrangements in terms of strategy. The study is based on realism, giving an analytical perspective for understanding state capability, institutional coherence, technological capacity and digital sovereignty.

The comparative analysis is based on the structuring-focused comparative model developed by George and Bennett (2005). The method allows a number of cases to be examined with common research questions and analytical tools to compare similarities and differences and draw out relevant policy lessons.

Case Selection

The study includes Pakistan, India and Türkiye. The main focus is on Pakistan while India and Türkiye are used as comparative examples. India was selected because it was geographically close, it was a rival nation and institutions and incident-response mechanisms in India were developing. Türkiye was selected due to its ongoing efforts of developing a cybersecurity governance mechanism and recent legislative and institutional initiatives. These cases offer different perspectives and approaches in cybersecurity governance that can inform a policy debate and analysis of options for the policy of Pakistan. The comparison is not based on the premise that the three countries are technologically, financially or institutionally equal. Rather, it will explore their arrangements in relation to various analytical standards and their possible applicability in Pakistan.

Data Collection

The study uses document analysis and secondary data. Sources are national cybersecurity policy and strategy documents, legislation, government publications, institutional reports, policy documents and cybersecurity and national security scholarly research. Specific focus is placed on the Prevention of Electronic Crimes Act (PECA) 2016 and the National Cyber Security Policy (NCSP) 2021 in Pakistan in addition to the legal, policy and institutional measures in India and Türkiye. Theories and concepts are explored in the academic literature and journal articles, national priorities and institutional responsibilities, and formal governance structures are explored in official documents. Appropriate technical evaluations and policy reports are also considered to gain an understanding of cyber security threats and national readiness and implementation challenges.

Data Analysis and Analytical Framework

The data collected are analyzed by the method of structured comparison and qualitative thematic analysis. Common questions relating to cyber threats, legal powers, institutional duties, technological capacity, coordination and enforcement are considered for each country. The analysis is organized around four dimensions: legal, institutional, technological and strategic. As a first step, the coding structure follows the four dimensions and other themes that could emerge from the documentary material will be included. A qualitative analytical approach, as suggested by Braun and Clarke (2019), is used, involving both theory driven and inductive coding. The three cases are then analyzed from a realistic perspective to identify policy practices and countermeasures that could be implemented in Pakistan's context, given the institutional and resource constraints in the country.

Scope and Limitations

The study is based on Pakistan, India and Türkiye, with special focus on the cybersecurity environment in Pakistan. Its conclusions are based on documentary evidence which must be available and reliable. The research will not feature interviews with cybersecurity practitioners or policy makers, quantitative assessments of cyber incidents, or technical penetration testing. Thus, the effectiveness of the institution is evaluated based on existing documents and not based on performance measurement of the agency. In addition, the constantly changing nature of cybersecurity will impact the ongoing significance of some findings. The proposed countermeasures should therefore be interpreted as suggestions for policy rather than concrete outcomes of implementations.

Cybersecurity Threats and Their Implications for Pakistan

Nature of Cyber Threats to Pakistan

With the growing reliance on digital technologies, cybersecurity has become a critical aspect of Pakistan's national security landscape. Interdependent information systems are used in various critical sectors, such as government administration, financial services, telecommunications and others. While digitalization provides opportunities for economic development and administrative efficiency, it also creates vulnerabilities for organizations regarding cyber activities which could have an impact on sensitive information, cause disruption and bring doubts to the public. According to Shad (2019), one of the most significant components of Pakistan's cyber threat is hacking, but so are organized cybercrime and cyberterrorism, which are increasingly making inroads into the country, along with cyberwarfare. Cyber threats don't only strike computer networks. Their consequences are far reaching in terms of economic stability, institutional performance, political communication and the capacity of the state to safeguard strategically important information.

Cyber Espionage and Intelligence Operations

Cyber espionage, often known as cyber spying, is the act of collecting personal, sensitive, or private information from persons without their knowledge or agreement (Freet & Agrawal, 2017). Pakistan has been subjected to ‘targeted' cyber-espionage operations against government and strategically important organizations. The National Telecom and Information Technology Security Board (NTISB) of Pakistan on 23 December 2020 released an advisory alerting public on the presence of a malware campaign using spoofed email messages targeting civil, military and intelligence organizations. The advisory noted that malicious attachments could break into targeted computers, expose files and user names and passwords to unauthorized persons (Government of Pakistan, 2020). The official warning highlights the type of threat that is impacting on the sensitive government networks, but does not necessarily mean that all of the organizations targeted were ultimately compromised.

More targeted activity is visible in the Council on Foreign Relations' Cyber Operations Tracker. According to its February 2021 report, Android spyware was used by the Confucius threat actor to intercept calls and messages on WhatsApp and other applications from the government officials of Pakistan and Kashmir. The suspected victims were electoral officials in Kashmir, authorities associated with Pakistan's nuclear agencies and the military. The tracker designates India as the suspected state sponsor, but any such attribution must be regarded as a “guess” and not a certain responsibility on the part of the state (Council on Foreign Relations, 2021). Another report dated 2022 July claimed that the same threat actor was responsible for a spear-phishing attack against government, military and energy-sector organizations in Pakistan (Council on Foreign Relations, 2022).

The impact of the activities goes beyond the disclosure of confidential information. If the communications are compromised, it could expose institutional weaknesses, give some indication of how decisions are made within institutions and help the adversary see where they can find weaknesses in strategically significant organizations. This information could then feed into diplomatic, political or security decision making. Therefore, from a realist point of view, cyber espionage can affect the strategic balance between two rival states by giving one state information that can help it gain a better understanding of the other state's capabilities and intentions (Mearsheimer, 2001; Waltz, 1979). It is, therefore, vital for Pakistan to safeguard government and defense related information and thus minimize the chances of getting the information influenced by outsiders.

Financial Cybercrime and Economic Security

New technologies such as electronic banking, digital payments and online financial services have also opened new doors for cyber criminals. Payment-card theft, phishing, identity fraud, unauthorized accounts access and any other digital financial exploitation constitute financial cybercrime. These activities can have direct monetary effects, and can also impact the confidence in financial institutions and electronic payment systems.

The recent attack on payment cards in Pakistan in 2018 is a good example of the financial system's vulnerability. This data was extracted through a card skimming scheme initiated against 22 banks in Pakistan, according to Reuters, citing the leaked data in a card skimming attack. The State Bank of Pakistan instructed banks to strengthen monitoring and examination of transactions, however, denied any hacking of their systems by hackers (Hassan & Shahzad, 2018). The difference lies in how the incident showed that payment-card data was compromised, not whether the affected banks' internal systems were compromised, since the incident did not involve any of those banks.

Financial cybercrime does not just affect the financial loss. Fraudulent transactions can lead to higher recovery expenses, put new pressures on regulators, and diminish consumer trust in digital economic providers. Multiple such events can also deter individuals and businesses from using electronic payment facilities, which will have a negative impact on the overall growth of the digital economy. Similarly, Shad (2019) notes that financial cybercrime is also a significant component of the overall cybercrime situation in Pakistan. Financial systems protection must be understood in the context of economic security – the reliability of digital transactions contributes to financial confidence and economic resilience; the stability and resilience of financial institutions.

Disinformation and Hybrid Information Operations

Disinformation is a very specific attack, typically aimed at shaping the public opinion, but not necessarily affecting computer systems, unlike other types of cybersecurity attacks. Disinformation aims to disrupt truth-seeking by distorting one's perception of reality or highlighting one's preexisting ideas, which in turn affects public opinion. People may get confused about fundamental truths and current affairs as a result of misleading information, posing a risk to public safety, corporate reputations, or governmental operations (Caramancion et al., 2022).

Disinformation is one of the greatest challenges in the realm of cyber security because it does not necessarily need to be directly on the computer, but it may make people think differently. The spreading of purposeful false and misleading information to advance polarization, undermine trust in institutions, and/or change attitude. These types of contents can be amplified on a multimedia platform by having fake accounts, being able to post automatically, edit photos and videos and spread false stories out in a flash.

The turmoil of times of uncertainty, insecurity and security incidents with neighboring countries makes disinformation even more potent in a country like Pakistan. These days, misinformation can spread and polarise, affect public opinion and comments, and question official activities and government policies. This can also hinder the ability for coordination to happen within the institutions and make it easier to spread misinformation that isn't true before real information. These can undermine public confidence and enable bad governance to take hold.

But there is a difference to be drawn between disinformation and politics on one hand, and criticism and freedom of expression on the other. It is important to note that contentious and incorrect content does not necessarily mean it is a coordinated influence operation. A national response should be evidence based, transparent public communication and adequate institutional protection. The realist perspective on information operations is that they can be seen as instruments or means by which state and non-state actors can seek political influence and strategic advantage, apart from the use of traditional military means. Therefore, the strengthening of information resilience in Pakistan is a relevant issue in order to build public trust and preserve the credibility of the national institutions.

Comparative Analysis: India and Türkiye and Lessons for Pakistan

India: Institutional Specialization and Cybersecurity Capacity

India is a relevant regional comparison because the concept of cyber security governance has been shaped by increasing dependence on digital means and strategic competition. It is mainly dependent on the Information Technology Act 2000 and the National Cyber Security Policy 2013. One remarkable aspect is that the two entities - Indian Computer Emergency Response Team (CERT-In) under Section 70B and the National Critical Information Infrastructure Protection Centre (NCIIPC) under Section 70A - are separate from one another. The CERT-In coordinates the national cybersecurity incident response and NCIIPC specializes in protecting critical information infrastructure. The National Cyber Coordination Centre (NCCC) and National Cyber Security Coordinator (NCSC) are both other supporting institutions which contribute to the overall coordination.

It is a lesson that Pakistan should learn from this functional specialization. The roles and technical capacities to respond to the national incident and to protect critical infrastructure are unique. In Pakistan the distinction between the response to cyber incidents and proactive defense of strategic infrastructure needs to be clearly demarcated, therefore. The Indian experience also brings into focus that compliance alone is not sufficient and having a robust audit, vulnerability assessment and readiness is crucial to be prepared. In this regard, the National Cyber Security Policy 2021 is applicable; it is still a challenge to implement and enforce the policy.

The institutional model cannot be exactly replicated in India. It has a more robust technological base; cyber security professionals and industrial base which Pakistan lacks. Furthermore, Pakistan-India strategic rivalry affects the development of cybersecurity in India. In a realist worldview, these trends would indicate a connection between cyber capabilities and national power and strategic security. Functional specialization and compliance as practiced in India could be replicated by Pakistan, although it must be tailored to match Pakistan's financial, technological and institutional limitations.

Türkiye: Centralization through Legal and Institutional Reform

Türkiye provides an alternative institutional lesson on the reforms in the field of cybersecurity, which were established under Cybersecurity Law No. 7545 of 2025. Prior to this reform, the role of cybersecurity was divided between various institutions such as the Information and Communication Technologies Authority (BTK), the Digital Transformation Office and the sector-specific regulators. This gave rise to coordination problems due to several institutional demands.

The 2025 law introduced the Cybersecurity Council led by the President and Cybersecurity Directorate to deepen and improve coordination and regulation in the country. Türkiye's Cybersecurity Directorate sets security requirements, performs inspections, applies sanctions, provides protection for critical infrastructure and is responsible for security certification. It has an incident-response structure that includes a national coordination element, the National Cyber Incident Response Centre (NCRC/USOM), and sectoral and organizational teams (SOMEs) for telecommunication, energy, banking and transport. This is a hierarchical model

which gives guidance to Pakistan to implement the structure of CERT in NCSP 2021 with the help of a legally empowered central authority with coordination and enforcement powers. But without centralization, there is no guarantee of effectiveness. There is a need for sufficient technical capabilities, financial resources, enforcement authorities and institutional support. Hence, Pakistan should adopt selectively the reforms of Türkiye and focus on effective implementation and institutional capacity to close the cybersecurity governance gaps that exist in the country.

Comparative Lessons for Pakistan

The comparative analysis points to two complementary strategies that can be adopted: The functional specialization of NRIs in India for national incident response and critical infrastructure protection, and centralized coordination with legal and regulatory authority in Türkiye. The governance problems in Pakistan are due to overlapping functions and responsibilities of various institutions, such as National CERT, NR3C, PTA, NACTA and NCCS. These institutional overlaps create difficulties with coordination, and a clear division of responsibilities and greater cooperation and enforcement are needed. Pakistan must take the best from India's specialization and compliance framework as well as Türkiye's central coordination framework that, due to their administrative, financial, technological and political constraints, are not suitable for Pakistan. Cybersecurity governance, from a realist point of view is tightly tied to state power, sovereignty and strategic autonomy. So, to achieve cyber sovereignty, it's not sufficient merely to enact laws or create new agencies. Requires a holistic approach with legal powers, institutional coordination, technology and ongoing capacity development to ensure the safety of the national digital infrastructure and national interests.

Policy Recommendations and Countermeasures for Pakistan

A holistic approach is needed for strengthening cyber security to make the cyber space more secure and resilient, which will also be beneficial in ensuring the national security of Pakistan and enhance the capacity of the institutions and minimize the technological vulnerabilities. Following are the countermeasures recommended based on the results and lessons learned of the study and other countries such as Türkiye and India.

Legal Countermeasures. The Prevention of Electronic Crimes Act (PECA) 2016 can be even stronger if it is going to criminalize the perpetrators of electronic crimes and, at the very least, impose obligations on the state, in order to prevent the occurrence of cyber security. Security standards, frequent testing and assessment as well as reporting of incidents should be mandatory for operators in critical sectors (telecoms, energy, financial services). To cover the collection, storage and processing of personal and organizational data, there needs to be a comprehensive data protection law. The measures of accountability and oversight that should be part of such reforms should include measures to ensure that the law is not abused.

Institutional Countermeasures. The study suggests that the fragmentation of institutions can be overcome by forming a National Cyber Security Authority (NCSA) which will act as a coordination body. The Authority should establish and integrate existing institutions in Türkiye like NR3C, PTA, NCCS and the National CERT system with their specific legal duties and responsibilities. It should facilitate the sharing and coordination of information, and foster a greater cyber security cooperation between civilian, military and intelligence cyber security operations. It is also suggested that the National CERT should be expanded to Sectoral and Provincial teams in each of the sectors namely banking, energy, telecom, transport etc. in Pakistan. This change should be supported by qualified personnel who have incident response and digital forensics experience.

Institutional and capacity building measures. The government of Pakistan should invest more in the research and development of cybersecurity, including the creation of local cybersecurity products and solutions, threat intelligence, secure data storage, and encryption. Lack of skilled manpower and the requirement of specialized training and certification should be resolved by a synergy between Universities, Government and Industry. Escalon's investments in domestic cybersecurity start-ups and innovation centers are also important to ease overreliance on foreign hardware and software, cybersecurity in technological supply chains and gradually build up technological autonomy.

Strategic and Diplomatic Measures. Cyber security should be mainstreamed into national security, foreign policy and defense planning efforts in Pakistan. In order to enhance the country's engagement in international forums, cooperation in combating cybercrime, intelligence sharing and engagement in building international norms for responsible state behavior, a coherent cyber diplomacy strategy should be enhanced. Close cooperation with technologically advanced states should focus on training of technicians and transfer of technical skills, while avoiding over-dependency on external sources. Cooperation between South Asian countries to share information about incidents and build trust in the region can also mitigate cyber threats, but it needs to address existing geopolitical tensions.

Phased Implementation. A sensible sequence of reforms should be followed. Short-term measures (1-2 years) should focus on legal changes, data protection law, the reinforcement of the National CERT and staff training. Medium term (3-5 years) objectives should include building the NCSA, strengthening inter-agency coordination and expanding sectoral and provincial CERTs. Indigenous technology, encryption, secure national data infrastructure, threat intelligence and home-grown research were all priorities for the long term (5–10 years). A posture of credible deterrence should take shape as legal, institutional and defensive capabilities have grown, with deterrence by denial being more effective, rather than a primary method of punitive action.

All of these measures work towards building a more coordinated, proactively established, and sovereignty-based cyber security framework in Pakistan.

Conclusion

This research identified the existing cybersecurity system in Pakistan, the significant cyber threats in Pakistan and finally the contextually suitable countermeasures by comparing cybersecurity system of India and Türkiye. The outcomes reveal the multi-faceted nature of cyber insurgency, cyber financial crimes, disinformation and critical infrastructure attacks which holds a multi-dimensional threat for Pakistan's national security, governance and cyber sovereignty. The Prevention of Electronic Crimes Act (PECA) 2016 and National Cyber Security Policy (NCSP) 2021 are important legal and policy frameworks, but are weak because they are not coordinated and not technically competent or enforced.

Complementary lessons are revealed through the comparative analysis and include the institutional specialization approach adopted in India and the centralized approach to coordination of cybersecurity governance adopted in Türkiye. However, these models must be adapted selectively and not be replicated in Pakistan's institutional, monetary and technological constraints. From a realistic viewpoint, cyber security is an integral component of state power, sovereignty and strategic autonomy. Pakistan should move from ‘piecemeal’ and ‘reactive' to ‘coordinated' response model, which should involve legal accountability, institutional coherence, technological resilience and strategic cooperation. To drive the strengthening of cyber sovereignty, a sustained political will, national capabilities investment and implementation are needed. The paper contributes to the cybersecurity governance (CSG) literature as it incorporates the realist theory and hence, presents a framework for strengthening cyber resilience of Pakistan in the specific context of its cybersecurity challenges.

References

1. Ahmad, S. (2022). Cyber security threat and Pakistan’s preparedness: An analysis of national cyber security policy 2021. *Pakistan Journal of Humanities & Social Sciences Research*, *5*(1), 33.
2. Akhtar, N., & Iqbal, A. R. (2025). Cyber sovereignty: National security in the digital age. *Lahore Institute for Research and Analysis Journal*, *3*, 87-104.
3. Akram, M. S. (2023). Digital shadows: The menace of cyber espionage and Pakistan’s national security. *Journal of Development and Social Sciences*, *4*(III). https://doi.org/10.47205/jdss.2023(4-iii)80
4. Banks, W. (2017). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory Law Journal*, *66*(3), 513. https://scholarlycommons.law.emory.edu/elj/vol66/iss3/3
5. Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation.* Project on Computational Propaganda, Oxford Internet
6. Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *11*(4), 589-597. https://doi.org/10.1080/2159676X.2019.1628806
7. Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats. *Data*, *7*(4), 49. https://doi.org/10.3390/data7040049
8. Corn, G. P., & Taylor, R. (2017). Sovereignty in the age of cyber. *American Journal of International Law*, *111*, 207–212. https://doi.org/10.1017/aju.2017.57
9. Council on Foreign Relations. (2021). Targeting of government authorities in Pakistan and Kashmir. *Council on Foreign Relations*. https://www.cfr.org/cyber-operations/targeting-of-government-authorities-in-pakistan-and-kashmir

10. Council on Foreign Relations. (2022, July). Targeting of government, military, and energy sectors in Pakistan. *Council on Foreign Relations.* https://www.cfr.org/cyber-operations/targeting-of-government-military-and-energy-sectors-in-pakistan

11. Craig, A. J. S., Johnson, R. A. I., & Gallop, M. (2022). Building cybersecurity capacity: A framework of analysis for national cybersecurity strategies. *Journal of Cyber Policy, 7*(3), 375–398. https://doi.org/10.1080/23738871.2023.2178318

12. DeNardis, L. (2014). *The global war for internet governance.* Yale University Press.

13. DeNardis, L. (2016, July 19). *One internet: An evidentiary basis for policy making on internet universality and fragmentation.* Centre for International Governance Innovation. https://www.cigionline.org/publications/one-internet-evidentiary-basis-policy-making-internet-universality-and-fragmentation/

14. Freet, D., & Agrawal, R. (2017). Cyber espionage. *Encyclopedia of Big Data*, 1–5. https://doi.org/10.1007/978-3-319-32001-4_51-1

15. George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences.* MIT Press.

16. Government of Pakistan. (2020). *Advisory - prevention against cyber espionage (advisory no. 28).* https://download1.fbr.gov.pk/Docs/202118111563449Advisory-PreventionagainstCyberEspionage%28Advisory-28%29.pdf

17. Hassan, S. R., & Shahzad, A. (2018, November 6). Pakistan reports card-skimming, but says no mass bank data breach. *Reuters.* https://www.reuters.com/article/technology/pakistan-reports-card-skimming-but-says-no-mass-bank-data-breach-idUSKCN1NB2IM/

18. ITU. (2024). *Global Cybersecurity Index 2024.* https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

19. Katsikas, S. K. (2025). Towards a cybersecurity-oriented research agenda for digital sovereignty. *Procedia Computer Science, 254*, 279–288. https://doi.org/10.1016/j.procs.2025.02.087

20. Klimburg, A. (2017). *The darkening web: The war for cyberspace.* Penguin Press.

21. Lobell, S. E. (2017). *Structural realism/offensive and defensive realism* (pp. 1–23). Oxford University Press. http://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-304

22. Mearsheimer, J. (2001). *The tragedy of great power politics.* Norton.

23. Mearsheimer, J. J. (2003). *The tragedy of great power politics* (Updated ed.). W. W. Norton & Company.

24. Ministry of Information Technology and Telecommunication, & Government of Pakistan. (2021). *National Cyber Security Policy 2021.* Pkcert.Gov.Pk. https://pkcert.gov.pk/uploads/2023/06/2021-National-Cyber-Security-Policy-Final.pdf

25. Odebade, A. T., & Benkhelifa, E. (2023). A comparative study of national cyber security strategies of ten nations. *arXiv preprint arXiv:2303.13938.*

26. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1-2), 4-37.

27. Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review, 5*(4), 533-561.

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

29. Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies, 39*(1), 1-19.

30. *The prevention of electronic crimes act, 2016 contents.* (2016). https://www.pakistancode.gov.pk/pdffiles/administrator6a061efe0ed5bd153fa8b79b8eb4cba7.pdf

31. Waltz, K. N. (1979). *Theory of international politics.* Addison-Wesley.



2026 by the authors; Journal of Global Social Transformation (JGST). This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).