Journal of Media Horizons
ISSN: 2710-4060 2710-4052 Volume 6, Issue 5, 2025

USE OF AI, SOCIAL MEDIA AND CYBER CAPABILITIES TO PROJECT STATE INFLUENCE: A CASE STUDY OF PAKISTAN

Dr. Khyber Khan[*1], Dr. Jawaria Andleeb Qureshi[2], Sahreen Rafiq Khan[3], Malik Umer Mushtaq Aziz[4], Mufleha Zulfiqar[5]

[*1]*Department of Management Science, NUST Institute of Peace and Conflict Studies, Islamabad*
[2]*Department of Management Science, Hazara University*
[3]*Department of International Relations, AUST University*
[4]*Department of Management Science, NUST Institute of Peace and Conflict Studies, Islamabad*
[5]*Department of Management Science, Bahria University, Islamabad*

[*1]Khyber.mgs@nipcons.nust.edu.pk, [2]javeria@hu.edu.pk, [3]sahreenm@gmail.com, [4]umer.mushtaq82@gmail.com, [5]muf28.1995@gmail.com

DOI: https://doi.org/10.5281/zenodo.17510798

Keywords
Digital Diplomacy, Cyber Strategy, Artificial Intelligence (AI), Narrative Engineering, Disinformation, Hybrid warfare, Strategic Communication, Pakistan

Article History
Received: 12 September 2025
Accepted: 28 October 2025
Published: 31 October 2025

Corresponding Author: *
Dr. Khyber Khan

Abstract

In the modern world, countries more frequently utilize cyberspace, social media, artificial intelligence (AI), and other technologies to exercise influence and control over their citizens. This research analyzes secondary sources such as policy documents, scholarly literature, media, and reports from EU DisinfoLab and Graphika to understand Pakistan's interaction with these technologies for strategic communication and narrative forming. It examines the digital diplomacy, counter-propaganda, AI-enabled surveillance, and memetic warfare of layers of primary state institutions like ISPR, MoFA, PTA, and NITB. A high-level synthesis unveils a fractured digital ecosystem replete with AI perception monitoring, ordered deafness, citizen counter-disinformation activism, and advanced perception management. This research also illustrates the overwhelming dominance of these institutions in the configuration of Pakistan's digital influence and cyber operations. It closes with policy proposals stressing planned unification via a centralized communication system, institutional capacity enhancement with AI and cyber training, ethical governance, cyber diplomacy, cooperation between academia and industry, public education, engagement with the youth, and transparent digital regulation. All in all, this research enhances the theoretical literature on smart power and digital statecraft. It also provides practical suggestions for policymakers, civil society, and security organizations to address the contemporary phenomenon of information warfare in the twenty-first century.

Introduction

In the 21st century, the focus of power and warfare has changed from conventional military strength to the informational and cognitive aspects of statecraft. Conflicts have metamorphosed into forms of warfare which are non-kinetic, where the primary battlegrounds are perceptions and narratives due to the emergence of AI, social media, and cyberspace (Nye, 2010; Rid, 2020). Digital technologies serve as instruments of influence for Pakistan, a nuclear-armed country of the world which has difficult internal issues—terrorism, political instability, economic hardship, and ethnic divides—and external rivalries and alliances with India, China, the USA, and the Gulf. In the

ever-changing geopolitical world, digital technologies enable Pakistan to strengthen state control, manage disinformation, and shape narratives which serve its strategic objectives on both the international and domestic levels.

The strategic integration of artificial intelligence (AI) in governance and national security is apparent from recent developments in Pakistan. The Draft National Artificial Intelligence Policy (2024) aims to incorporate AI in defense, education, policing, and public service delivery (Business Recorder, 2024). The designing of AI-powered surveillance systems able to predict social sentiment during protests and to monitor extremist networks epitomizes the fusion of AI with internal state security. Meanwhile, social media serves as a vital medium for ideological and information domination. The Pakistani military, together with civilian agencies, has an active presence on X (formerly Twitter), Facebook, and YouTube to disseminate patriotic information, counter dissent, and control narratives, especially on Kashmir and counterterrorism, for international audiences. Within the military, the ISPR is primarily responsible for the creation of professional multimedia products intended to convey the image of the military as the defender of the ideological and strategic frontiers of the nation (Qamar, 2021).

There are also new uses of digital technology in politics. One example came in May, 2023 when the supporters of ex-Prime Minister Imran Khan, even when he was imprisoned, disseminated an AI-created speech which Khan 'addressed' using an AI 'voice.' This example shows how AI can break the molds of traditional censorship and alter the boundaries of politics (AP News, 2023). Also, Pakistan's increasing focus on both defensive and offensive cyber capabilities indicates their incorporation into the national defense policy. Particularly during escalations with India, Pakistan has been targeted with a growing number of cyber-attacks aimed at its financial systems, governmental repositories of information, and even some media houses. In reaction to these developments, PakCERT and the Prevention of Electronic Crimes Act (PECA) 2016 have been established, together with some other initiatives aimed at improving cyber governance. Although these same instruments have been blamed for enabling forms of digital censorship, 'freedom' has also been infringed upon with their enforcement (Freedom House, 2023).

The formation of the E-Safety Authority in 2023 illustrates the need of Pakistan geostratefically for the formation of cyberspace governance (Business Recorder, 2023). This newly formed office within the country still has room for further progress, especially in the area concerning the scholarship of Pakistan in the context of digital soft power. Global research focused on AI, cybersecurity, and digital diplomacy has paid little attention to the Pakistani context, especially the integration of AI, social media, and cyberspace within the strategic framework of emerging states. There remains an area of research which investigates the use of such technologies for the construction, consolidation, and protection of state narratives while dissent is removed in achieving geopolitical goals.

In this case, the focus of this study is on the adoption of AI, social media, and cyber capabilities in the digital statecraft of Pakistan. The study will utilize a qualitative and descriptive technique which is based on the assessment of secondary data, and aims to explore the strengths and weaknesses and ethical considerations of Pakistan's strategy for digital influence. This study is intended to widen the scope of international relations, cyberspace governance and political communications, and provide nuanced understanding of the contemporary world in relation to the AI development and digital statecraft of Pakistan.

Literature Review

2.1 The Digitalization of State Influence

In the 21st century, the means of projecting power has changed considerably. Traditional instruments of diplomacy, military force, and economic manipulation are now enhanced, and in many respects, substitutes, by digital instruments. Nye (2010) propounded that the 'cyber power' is the third type of capability a state posses; during the information age, dominion over knowledge and information circulation is believed to determine a state's capacity, capability and influence to, in turn, influence others. Within this paradigm, AI, social media,

and the internet have now become fundamental instruments of statecraft. These instruments enable real time monitoring, analysis, predictive modeling and communication of state objectives aimed at perception shaping both domestically and abroad (Seib, 2012).

In Pakistan, the increasing prevalence of the aforementioned technologies is a reflection of this global phenomenon. The National AI Policy (Ministry of IT & Telecom, 2023) and the establishment of an E-Safety Authority shows the intent to cultivate, close to, 'national' digital capabilities in governance, security and influence operations as well. Interesting though, as opposed to the advanced democracies, Pakistan's cyberspace policies are more reactive, and are a reflection of the need for order and security, both internal and in relation to neighbors.

2.2. Artificial Intelligence and Statecraft

States are adopting the use of AI to monitor, understand sentiment, detect threats, and generate content (SNAC). AI technology that imitates political leaders in the voice of the speaker has sparked political debate in Pakistan and also more political anxiety concerning deep fake technology (AP News, 2023). AI can enhance the quality of service and governance, but entails the risks of information distortion and manipulation of personal data.

As Horowitz et al. (2018) note, AI technology is not merely applied to civilian activities, but also to gain strategic advantage in the IR. In the case of Pakistan, the military use of AI-enabled strategic surveillance, facial recognition, and data mining illustrates the dual use nature of such technologies. Nevertheless, there is a dearth of literature on how Pakistan's AI capabilities connect to wider influence strategies.

2.3. Social Media as a Tool of Influence and Narrative Control

Public diplomacy, legitimization regimes, and information warfare construct an amalgamation of new domains which utilize social networks as a primary theater of operation development. Direct interfaces with state citizens and counter activity towards the opposition, as well as narrative control and psychological operations, fall under the purview of government functions. Particularly, in conflict contexts, narrative control with framework ISPR (Inter Services Public Relations, 2021) has been revealed as a primary stakeholder within Pakistan's emerging digital storytelling ecosystem. ISPR digital presence on Twitter and Youtube serves as a blatant demonstration of the manner in which countries can engineer public opinion by curating digital information islands.

Having said that, tightening control and increasing state grip on the narrative does come with the increased risk of diversity and more strech censorship. To that end, the Freedom House (2023) report has determined there to be a sharp deterioration of the digital freedom within Pakistan, censorship of content, state surveilence, and arrests of citizens for digital postings. The phenomenon of the use of information technologies to silence dissent. Democratic social media serves to highlight the social and political limits of social media which in many developing contries is used by autocrats rather then democrats to silence opposition.

2.4. Cyber Capabilities and Strategic Influence

The range of cyber capabilities include cyber espionage, cyber diplomacy, development and other indirect op-erations. In Pakistan hypothesis of cyber policy has been developed within counter terrorism domain and online jihadist content and information obscenity. Surprisingly, Pakistan is positioning itself strategically cyber wise as well. For example, narratives associated with China Pakistan Economic Corridor (CPEC) development are digitally tailored as counter narratives of critique from Indian and Western countries. These, according to Rid (2020) form part of "active measures," a twentieth century cocktail of disinformation, influence operations, and political warfare designed to manipulate world opinions.

2.5. Public Perception and Information Operations

During the time period considered, it appears to me that the Pakistan state sponsored digital narratives program has three primary objectives, the construction and consolidation of a

defensive global and positive national perception. These objectives are articulated through the purchase and deployment of social media influencers, the creation of advocacy content, and the advertisement of digital campaigns. These campaigns include Kashmiris Killing Kashmiris and aim to achieve national cohesion and unity. It is remarkable how the Pakistan state has mastered the art and science of global defensive India positioning memory. Despite the positive outcomes and national cohesion, the secondary and tertiary impacts of such actions are worrisome. Seib, Mahmod, and Azhar point out that the Ukrainian and Russian war, authoritarian regimes are constantly leaning to content manipulating, disinformation, and censorship to achieve political objectives. There is a double edge sword as state narratives becomes relentless and there is increasing discomfort and scrutiny from global narratives and media organizations. This shows the consequences of using digital propaganda.

2.6. Pakistan in the Global Context: A Unique Case

In contrast to advanced countries e.g., USA, China, and Russia, and owing to its geo-political uncertainty, emerging economic climate, and newly developing tech sector, Pakistan remains digitally defensive. However, integration of social media, AI, and cyber tools shows marked improvement in digital governance from decades past. Bradshaw and Howard (2018) noted that more than 70 nations engage in systematic disinformation as an organized and state-sponsored activity, especially on social media. Within this global movement, Pakistan is unique in that digital technology serves the purpose of external influence is also internally aimed at achieving political legitimacy and stability, public image enhancement of the military, and political control.

2.7. Missing Gaps in Earlier Literature

Despite an abundance of literature on the artificial intelligence (AI) technologies, social media, and cybersecurity in relation to global governance and security, there is still a relative lack of scholarship on their integrated and strategic use by developing countries like Pakistan. Much of the scholarship has focused on the technologies in question in isolation of one another—either on the inherently technical components of AI and cyberspace or on the social media articulation—while their integration in the context of advancing national interests and statecraft has been overlooked. Regarding Pakistan, the scholarship has been largely dominated by the legalistic issues of censorship, surveillance and control under the frameworks of the Pakistan Electronics Crimes Act (PECA) (Azhar & Mahmood, 2022) without incorporating the strategic use of AI, Information and Communication Technology (ICT), and cyberspace for public opinion and information operations at the national and international levels. In addition, the literature remains focused on particularly advanced authoritarian or democratic regimes, like China and Russia (Bradshaw & Howard, 2018; Rid, 2020), and thus lacks regional focused studies on South Asia, where Pakistan is situated in a distinctive constellation of geopolitical and security challenges coupled with a transmuting digital environment largely influenced by India's strategic communications.

This study addresses these gaps by analyzing Pakistan's use of AI, social media, and cyberspace as tools of state power, and contributing to debates on policy, governance, and security. This also sheds light on the impacts of digital strategies on democratic governance and civil liberties and in the emerging economies in South Asia.

2.8. Conceptual Framework

This study synthesizes three overlapping theories: Soft Power Theory, Information Warfare Theory and Technological Determinism. Together, these theories provide a framework of how modern nation-states like Pakistan, using digital tools of artificial intelligence (AI), social media and cyberspace, attempt to shape perceptions, project national power, and address geo-strategic challenges.

2.8.1. Soft Power Theory

Soft power entails being able to make others achieve ones goals without using the traditional "hard power" of payment and threats. Nye considers culture, political values, and the foreign policies essential to building the image and global attractiveness of the state. In the

contemporary world, soft power is exercised using online fora, e–diplomacy and mass media. Pakistan uses social media campaigns, employs military sponsored digital content, and e–diplomacy in line with the spread of soft power. The positive image of region peace, CPEC projects, and the development of the nation is promoted by ISPR and the MoFA. This theoretical prism illustrates how digital technologies are used to enhance the state's international legitimacy without the use of military and economic coercion.

2.8.2. Information Warfare Theory

Information warfare (IW) "is the strategic use of information and communication technologies (ICTs) to out compete, influence and disrupt hostile narratives from within target audiences" (Libicki, 1995). IW entails psychological operations, propaganda, disinformation, and cyberspace perception management within the context of cyberspace.

In the case of Pakistan, AI-generated content (e.g., synthetic voices of political leaders), cyber laws, and the digital censorship policy are fragments of information warfare. The state employs cyber technologies not only for eavesdropping and other monopolistic forms of control but also for countering subversive narratives determined by the regime, regardless of whether they emanate from foreign media, political opposition, or separatist movements (Hamayun, Alam, & Khan, 2025; Ullah, Khan, & Tahir, 2025). This model of cyber and AI operations might serve as a useful analytical framework to evaluate how AI, social networks, and other cyber tools are utilized for information manipulation, management, or countering (Alam, Bin Abid, Khan, & Gulzar, 2025; Alam, Kamal, & Awan, 2025). Moreover, state-backed digital strategies and AI-driven narratives can influence public opinion and organizational creativity in shaping collective perceptions (Shah, Tufail, & Khan, 2025; Alam & Khattak, 2025; Alam, Khan, & Khattak, 2025). "Information warfare is who tells the story" (Libicki, 1995).

2.8.3. Technological Determinism

The social theory of technological determinism explains that technological development sf social change and social change systems of social relations, culture and even political relations (Smith & Marx, 1994). Such theory believes that technology claims and use changes relationships of power and govern in the society. For example, in the case study of Pakistan, in how Pakistan has fully turned digital and how the state is trying to control and engage the emergent media. Also, the media transformation of the digital space is in the context of the growth of internet access, development of AI policies, and expansion of cyber space infrastructure.

This reconfiguration of the state and the citizen relationship in a country such as Pakistan with so little technology, but so much state control is what explains the paradox. In addition, there is a deep reconfiguration of the relationship of the state and the Pakistan's technology users with external world. These sentiments were so properly expressed by Smith and Marx (1994) in their emphasis of the question of how people use technology as what they value and what they think.

3. Research Methodology

3.1 Research Design

This study develops a qualitative and exploratory design approach from the perspective of critical realism. According to critical realism, our comprehension of these realities–strategic policies of the state, geopolitical infrastructures, and their cyber operations–is sociologically constructed and institutionally bound, albeit they are real (Bhaskar, 1978). This philosophical orientation allows the study to identify the deeper layers of the power configuration that underpin digital statecraft in Pakistan. The Soft Power Theory (Nye, 2004), Hybrid Warfare Theory (Mahnken, 2012), and Technological Determinism (Smith & Marx, 1994) serve as the guiding frameworks for the deductive reasoning aspect of the design alongside inductive reasoning, wherein the researcher identifies patterns and themes from the data.

A single-case study strategy is employed and the state of Pakistan is taken as the core to examine the ways in which the artificial intelligence, social media, and cyber power of the state are employed for the construction and projection of influence. This is the case focus of the study. Yin (2018) argues this is the most useful way to understand the context of the case and the strategic digital actions. The digital policies, the communication and propaganda campaigns institutionally mobilized by the state, and the ISPR and MoITT are the sub-units of analysis.

3.2 Data Collection and Analysis

This research uses only secondary sources of information like policy documents, global publications, (UN, WEF, NATO), academic books and journals, press articles, and think-tank research (ISSI, EU DisinfoLab, Graphika) obtained through Scopus, Web of Science, and Google Scholar. Ail sources checked for authenticity, credibility, and relevance due methodological rigor and systematics. Using thematic analysis (Braun & Clarke, 2006; Creswell & Poth, 2018), the research identified the dominance of the theme related to the control of digital information and strategic communication and analyzed these themes digital information, comms, and control, with triangulation improving the credibility of the results. The time-limited analysis, 2020-2024, studied the digital transformation of Pakistan because of the National AI Policy and the E-Safety Authority Act. The secondary data retrieval method employed some secondary synthesis, but the research did the right thing in the research ethics because the methods were transparent. Sourcing, citation, and scope data was acknowledged appropriately.

4. Data Analysis & Discussion

Table 1. The following table summarizes the sources used and the relevance to research objectives:

Source	Nature of Data	Relevance to Research Objectives
PTA Annual Reports (2022)	Policy & regulatory data	Social media regulation, national cybersecurity initiatives
MoITT AI Policy (2023)	Strategic document	National AI vision, digital transformation framework
EU DisinfoLab (2020)	Disinformation campaign investigation	Foreign propaganda counter-strategies
Graphika Reports (2021)	Influence operations analysis	Social media manipulation, bot networks
Reuters Investigations (2021)	Journalistic exposé	Cyber propaganda, regional information warfare
Academic Studies (West, 2020; Chertoff, 2018)	Scholarly analyses	AI & cyber capabilities in statecraft

4.1 Strategic Use of Social Media and Digital Diplomacy

Pakistan uses social media, including Facebook, YouTube, and Twitter for digital diplomacy, building narratives, and reinforcing national identity. The ISPR, MoFA, and even the PM office work together and run campaigns like Kashmir Solidarity Day and Digital Pakistan to try and mold people's perceptions on and offline. As reported by PTA (2022) and Relui (2021) social media has become a "force multiplier" to state narratives and oppose counter-narratives. Research works by Graphika (2021) and EU DisinfoLab (2020) argue state-sponsored info warfare campaigns with bot networks, hashtag diplomacy, and other constituents of bots to pursued information warfare which reflects Nye's Smart Power principle. Prolonged credibility issues, however, can be self-defeating, for they reduce the chances of international acknowledgment. This can be attributed to an authenticity gap like the Rule of the Citizen Protection (Against Online Harm) 2020, which raised concerns on global levels on censorship acts.

4.2 Integration of AI in National Governance and Security

In recent years, Pakistan has also commenced deployments of AI for national governance and public engagement. The implementations of the "National AI Policy" (MoITT, 2023) policy, for instance, predictive policing, facial recognition, sentiment analysis, and surveillance. All of these systems bolster the state's capacity to manage narratives and counter threats. The NITB, for instance, leads the operationalization of AI policies within the public sector.

To West (2020), the governance and control of power AI has advanced to is considered the most critical pivot. The ethical dilemmas of opacity, privacy, and fairness of algorithms are constituent parts of uncritical technological determinism (Smith & Marx) the notion that the social and political relations which technology sustains are often more authoritarian for failing governance.

4.3 Cyber Capabilities and Strategic Communication

In Pakistan, Cyber security, and digital defense strategy has been as important as the other pillars of the country's power structure. '2021 National Cyber Security Policy' together with operational entities such as NR3C and CERT exemplifies digital defense and cyber offensive strategy parallelism. Pakistan's digital infrastructure is aimed at, threat prevention and forming digital diplomacy offerings, particularly in times of high tensions with India.

For instance, Reuters (2021) and EU DisinfoLab (2020) provide proof of cyber warfare, digital defense, and espionage documentation. The scholarly approach (Chertoff, 2018) attempts to situate this in the broader context of hybrid war, where non-kinetic cyber systems are deployed to achieve strategic aims.

4.4. Counter-Propaganda and Narrative Engineering

The first disinformation counter-narratives verged on the use of counter PR tactics that evolved into and integrated with social media influencer outreach, strategic hashtag activism, and content creation designed to direct conversation. While these efforts bolster social harmony, their lack of substance and critical attention often draw sharp criticism. Integration of disparate elements of digital soft power is also lacking; low response times from automated chatbots aside, the foreign policy communications of Pakistan are not yet consolidated into a single robust digital offering. Incorporation of digital narrative elements – specially memes and infographics – into a single coherent narrative within the lattice-work of diplomacy will richly reward soft power efforts and sharpen the geopolitical positioning of Pakistan.

4.5. Regulatory Oversight and Governance Challenges

Pakistan is becoming more proactive in controlling the country's digital domain. The PTA's Citizen Protection Rules, together with PECA, are aimed at online data suppression, media regulation, and internet sovereignty consolidation. These laws are implemented not only under the guise of national security but also as mechanisms for dissent suppression and silencing critical voices (Sayyam, R. U. R., Mubarak, & Khan, 2025; Shahzad, Sayyam, Rahman, & Khan, 2024). Pakistan's strategy to develop an indigenous data ecosystem and store data locally is praiseworthy; however, its unilateral policy approach reflects inconsistency and raises concerns regarding transparency and accountability (Sayyam, A. A. K., Ur Rahman, & Ullah, 2025; Zeb, Sayyam, Amin, & Awan, 2025). Moreover, civil liberty proponents and scholars emphasize that while digital innovation supports organizational efficiency and social progress, excessive state monitoring and control may undermine digital freedom and public trust (Sayyam & Sabir, 2025a; Sayyam & Sabir, 2025b; Umair, Alam, Rahman, & Shah, 2025; Alam & Ilyas, 2024; Ilyas, Alam, & Rahman, 2024; Shah, Alam, & Rahman, 2024).

4.6 Civil Society and Disinformation

Resilience. Think tanks and digital rights organizations that operate independently and civil society organizations in Pakistan have played counteracting roles in the fostering of transparency and the upholding of disinformation. Collaborations with Graphika and EU DisinfoLab aid the promotion of awareness about coordinated influence operations and the promotion of digital literacy.

Within a securitized digital governance ecosystem, these actors, however, are under increasing strain.

4.7 International Perception Management

Pakistan undertakes the management of negative perception campaigns abroad in an effort to counter the more negative stereotypes about the country, particularly with regards to terrorism, extremism and democracy. These attempts consist of the mobilization of diaspora communities globally, the organization of international webinars, and the publication of op-eds in international media. Such measures, while serving to restore the image of Pakistan, are often undermined by a lack of credibility as well as competing geopolitical narratives.

4.8. Denial of Service Warfare Methods and Narrative Visualization

In Pakistan, the development and use of memes, infographics, and short videos that convey political information designed to convey easily digestible political information, particularly to the youth, have also been embraced for the purposes of 'memetic warfare.' Such images condense and simplify complex geopolitical positions such as the Kashmir conflict and anti-Israel sentiments, nationalism and the associated themes, and other complex—almost impenetrable—arguments at the level of speakable shareable materials.

During organized spectacles and in times of national emergency, visual art is also utilized as a propaganda device to enhance nationalism and leaven criticism. These tools tacitly promote anti-critical thinking and often fall short of addressing intricate dilemmas, instead, fostering complex, intricate issues and strengthening the audience isolation and the so-called echo chambers.

4.9. Automating Social Listening and Predictive Analysis

In Pakistan, the government and other security agencies are in a more secretive phase of the development and use of AI-powered social listening tools to monitor online chatter and identify/track new emerging potential threats and to proactively disrupt the coordination of activities for protest movements. Digital authorities employing sentiment analysis, keyword tracking, and predictive behavioral tools are able to construct tailored 'recipes' for narratives and social actions. Instead, fears are dominant about the tools being used for political badging, silencing, dissent, and the fostering of self-censorship.

Table 2. Synthesis of Findings in Context of Objectives and Questions

Research Objectives	Insight from Analysis
1. Analyze strategic use of AI, social media, and cyber capabilities	Pakistan uses these tools for national branding, defense messaging, and global outreach.
2. Explore how digital tools shape public opinion, counter propaganda, and promote national interest	Campaigns, AI surveillance, and cyber policies are key tools, though often controversial.
Research Question	**Answers from Findings**
1. How does Pakistan use AI, social media, and cyber tools to project its state influence?	Through narrative building, cyber posture, AI-driven surveillance, and strategic messaging.
2. In what ways do these tools shape public opinion and promote national interests?	By managing perception, suppressing dissent, and promoting state-aligned narratives.

5. Conclusion & Recommendations

Advances in technology and its growing prevalence in areas such as AI, social media, and cyber operations in Pakistan presents both advantages and disadvantages for the country's governance, diplomacy, and its national security to... the social power of Pakistan and its many security policies that emphasize a soft approach to digital technology...highlight the growing need for a coherent digital strategy policy framework. A policy framework in which Pakistan can control the unified efforts of its constituent intergovernmental organizations such as the ISPR, MoFA, MoITT and others in

furthering the country's strategic objectives...can emerge through the establishment of a Central Strategic Communication Authority. It is also recommended that the formation of a Rapid Response Digitized Defense Apparatus in the MoFA and the MoI would prove beneficial as Pakistan would then have the capacity to intercept and counter adversarial narratives in real-time, which strengthens strategic communication in Pakistan.

5.1 Capacity Building and Ethical Governance

Methodical enhancement of institutional capacity involves the integration of specialized AI and cyber training programs covering data analytics, behavioral science, and digital diplomacy. Military-civilian collaborations in these areas can enhance operational integration and readiness. Concurrently, Pakistan needs to foster responsible AI through an accessible "Ethical AI and Data Protection Bill" which aims at effective governance, oversight, and accountability. Amendments to existing cybercrime legislation like PECA should achieve a balance between the requirements of national security and the defense of individual freedoms, and must incorporate mechanisms for accountability to the public.

5.2 Digital Diplomacy, Research, and Public Engagement

Pakistan's soft power could be enhanced by fostering digital public diplomacy, implementing multilingual public outreach campaigns, partnering with social media influencers, and engaging in regional and global cyberspace collaboration such as SCO, OIC, and the UN Digital Cooperation Agenda, and, as a consequence, strengthening the country's public diplomacy soft power. The promotion of digital influence, AI ethics, and cyber operations interdisciplinary research and policy formulation within the public and scholarly domain make the collaboration of the government with the scholarly domain. Furthermore, the collaboration of the government, civil society, private industry, and media in the development of digital policy and strategy frameworks augurs well for heightened accountability and improved innovation. Finally, the promotion of digital public diplomacy along with digital policy and strategy frameworks to school students and youth innovators will promote public resilience against disinformation and strengthen Pakistan's global digital footprint.

5.3 Responsible Digital Governance and Cross-Border Cooperation

Pakistan's ability to cope with adverse digital situations depends upon equitable policy formulation and democratically managed strategic governance of the digitization of the PTA, MoITT, NITB, and cyber units of the military. Along with routine independent evaluations, deep-seated algorithmic and ethical AI equity scrutiny, and sustainable society development, the establishment of tailored "centers of excellence" with set teaching modules in cybersecurity and AI ethics is a must. Geopolitically, Pakistan needs to devote resources to the proactive element of cyber diplomacy and foster public–private partnerships with leading tech companies to enhance its reputation within the cyber domain and expand its global "Clean-Space" image. Reconciling public trust and accountability in the National digital Policy and cyber defense, alongside enhanced governance, is achievable through public oversight, greater transparency, and improved digital manipulation and policy metrics.

Table 3. Summary Table: Recommendations by Theme

Code	Theme	Key Recommendations
T1	Strategic Integration	T1.1 = National digital influence policy T1.2 = Centralized communication authority
T2	Institutional Capacity	T2.1 = AI/cyber training in government and military T2.2 = Civilian-military knowledge sharing
T3	Ethical Governance	T3.1 = Ethical AI standards T3.2 = Reform of PECA and related cyber laws

T4	Global Cyber Diplomacy	T4.1 = International engagement T4.2 = Digital diplomacy outreach
T5	Research & Stakeholder Engagement	T5.1 = Interdisciplinary research support T5.2 = Civil society-Private sector partnerships
T6	Public Literacy & Youth Engagement	T6.1 = Digital literacy campaigns T6.2 = Innovation programs for youth
T7	Transparency & Oversight	T7.1 = Transparency reports on digital operations

5.4 Implications of the Study

This research fundamentally adds to the theory and practice of understanding digital technologies, governance and statecraft in Pakistan, and their wider ramifications. It advances the theoretical discourse in International Relations by adding to the Soft and Smart Power Theories the role of Artificial Intelligence, social media, and cyberspace in attraction and influence in the digitally-driven world. It further enriches Constructivist theory by showing the ways in which states craft online and digital narratives and identities to influence dominant perceptions and behavior. The study also broadens the understanding of Hybrid and Memetic Warfare by demonstrating how states exert non-kinetic power using memes, digital propaganda, and narrative exploitation. It interrogates the domain of Technological Determinism to analyze the paradox of the organizational augmentation of efficiency and the potential for authoritarian control derived from the integration of AI and surveillance technologies, raising the important issues of ethical governance and democratic oversight concerning digital influence operations.This work serves as an academic foundation for the study in question. In particular, the academic community can rely on the Interdisciplinary Center for Digital Innovation and the University of the Arts London for frameworks on national communication policy in the digital age. These works can inspire further study on other themes of digital statecraft, and on the various other facets of communication, and policy development. This multi-faceted communication policy, and the other policies of and for the state, can benefit from the tail-end of the 'technological gap' concept. Technology Diffusion and Adoption Theory may help demonstrate why certain structures and policies may help the national communication system achieve the 'hermeneutic self' the other works discuss.

This theory may help establish the effectiveness of strengthened state frameworks on policy and practice, embedded 'technological gap', and the proposed live policy system for the problem. This body of work can greatly enhance other digital international engagement policies and state action.

Ethical tools, devices, and procedures for governance can act as reference points or heuristics for other branches of state action.

In summary, the research combines the analysis of digital statecraft and practical policy development. Rather than more theory, it proposes ethnographic case study approaches as a starting point to build the 'real world' digitally on top of the 'digital suitcase' metaphors.

6. Conclusion

This research outlines how Pakistan has applied artificial intelligence (AI), social media, and cyber tools for extending its internal and external influence. It analyzes the state's use of soft power, information warfare, and technological determinism to shape narratives and counter opposing narratives. Pakistan institutes use social media like Twitter, Facebook, and YouTube for digital diplomacy and image building. Tools like sentiment analysis and predictive surveillance reveal a shift toward algorithmic governance. Pakistan pursues a dual cyber strategy, defense and influence projection, which has attracted criticism for a lack of transparency, data protection, and freedom of expression. While digital Pakistan's digital capabilities are still stultified by infrastructure and policy obstacles, the increasing use of digital tools illustrates progress towards strategy communication and soft power diplomacy.

References

Alam, S. A., & Khattak, S. A. (2025). Variation in performance of faculty, relating to

their age: A case study of Women University Mardan. Journal for Current Sign, 3(3), 544–559.

Alam, S., Bin Abid, A., Khan, I., & Gulzar, R. (2025). Digital persuasion: Mediating effect of content quality in influencer marketing. Journal of Management Science Research Review, 4(2), 112–143.

Alam, S., Kamal, S. S., & Awan, S. H. (2025). Engineering financial resilience: Structuring turnaround and maintenance financing using derivatives and structured instruments. Advance Journal of Econometrics and Finance, 3(3), 143–153.

Alam, S., Khan, K., & Khattak, S. A. (2025). Challenges and success factors in implementing sustainable project management practices in Pakistan's construction industry. Journal of Management & Social Science, 2(4), 753–766.

Alam, S., Zaman, Y., Khattak, S. A., & Khan, I. (2025). Green ergonomics in banks: How it influences employee attitude and behavior intention: A theory of planned behavior approach. Journal of Management & Social Science, 2(2), 574–583.

Amnesty International. (2023). *Pakistan: Crackdown on dissent intensifies under cybercrime law.* Retrieved from https://www.amnesty.org

Amnesty International. (2023). *Pakistan: Online censorship and digital rights.* Amnesty International.

AP News. (2023, May 9). *Pakistan is stunned as party of imprisoned ex-PM Khan uses AI to replicate his voice for a speech.*

Azhar, H., & Mahmood, T. (2022). Digital authoritarianism in Pakistan: The rise of state surveillance and control. *Journal of South Asian Studies, 37*(2), 115–131.

Azhar, M., & Mahmood, A. (2022). Digital authoritarianism and online dissent in Pakistan. *South Asian Journal of Political Science, 11*(2), 45–59.

Azhar, M., & Mahmood, T. (2022). Artificial intelligence in Pakistan: Opportunities and challenges. *Technology in Society, 70*, 102008.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Bradshaw, S., & Howard, P. N. (2018). Challenging truth and trust: A global inventory of organized social media manipulation. *Oxford Internet Institute.*

Bradshaw, S., & Howard, P. N. (2018). The global organization of social media disinformation campaigns. *Journal of International Affairs, 71*(1.5), 23–32.

Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation.* Oxford Internet Institute.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Business Recorder. (2023, August 4). *Govt to regulate content on social network platforms.*

Business Recorder. (2024, November 14). *Pakistan set to roll out its first AI policy to boost cybersecurity.* https://www.brecorder.com/news/40332365

Chertoff, M. (2018). A public policy perspective of the cybersecurity challenge. *Journal of Cybersecurity, 4*(1), 1–5. https://doi.org/10.1093/cybsec/tyy001

Chertoff, M. (2018). *The role of cybersecurity in hybrid warfare.* Council on Foreign Relations Report.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications.

EU DisinfoLab. (2020). *Indian Chronicles: A disinformation network.* Retrieved from https://www.disinfo.eu/publications/indian-chronicles/

Freedom House. (2023). *Freedom on the Net 2023: Pakistan.* https://freedomhouse.org/country/pakistan/freedom-net/2023

Graphika. (2021). *Information operations report.* Graphika Inc.

Graphika. (2021). *Social media influence operations: Trends and tactics.* Retrieved from https://graphika.com/reports

Hamayun, K., Alam, S., & Khan, I. (2025). Harnessing artificial intelligence for green business model innovation: The role of environmental awareness in Pakistani SMEs. Annual Methodological Archive Research Review, 3(9), 29–44.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). *Digital citizenship in a datafied society*. Polity Press.

Horowitz, M. C., Allen, G. C., Kania, E. B., & Scharre, P. (2018). *Artificial intelligence and international security*. Center for a New American Security.

Khan, I., Alam, S., & Hamayun, K. (2025). Digital transformation of fashion entrepreneurship in Pakistan: AI adoption, social-commerce capability, and financial inclusion. Policy Journal of Social Science Review, 3(9), 180–195.

Libicki, M. C. (1995). *What is information warfare?* Washington, DC: National Defense University Press.

Mahnken, T. G. (2012). *Technology and the American way of war since 1945*. Columbia University Press.

Ministry of Information Technology and Telecommunication (MoITT). (2021). *National Cyber Security Policy of Pakistan 2021*. Government of Pakistan. https://moitt.gov.pk

Ministry of Information Technology and Telecommunication (MoITT). (2022). *National Artificial Intelligence Policy (Draft)*. Government of Pakistan. https://moitt.gov.pk

Ministry of Information Technology and Telecommunication (MoITT). (2023). *Pakistan National AI Policy*. Government of Pakistan. Retrieved from https://moitt.gov.pk

Nye, J. S. (2004). *Soft power: The means to success in world politics*. New York, NY: PublicAffairs.

Nye, J. S. (2010). *Cyber power*. Belfer Center for Science and International Affairs.

Pakistan Telecommunication Authority (PTA). (2022). *Annual report*. Retrieved from https://pta.gov.pk/en/annual-reports

Qamar, M. (2021). Role of ISPR in modern information warfare. *Pakistan Journal of Communication Studies, 9*(2), 33–45.

Rahman, R. U., Alam, S., Wali, S. S., & Khan, I. (2025). Environmental factors and innovation: The role of urban green spaces in entrepreneurial creativity and stress reduction. Annual Methodological Archive Research Review, 3(4), 465–474.

Rahman, R. U., Sayyam, A., Mubarak, R., & Khan, A. A. (2025). Green leadership: Driving organizational change toward sustainability. Center for Management Science Research, 3(3), 97–112.

Reuters. (2021). *How countries weaponize social media*. Retrieved from https://www.reuters.com

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. New York, NY: Farrar, Straus and Giroux.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.

Sayyam, A. A. K., Ur Rahman, R., & Ullah, M. (2025). Transforming academia: The role of AI in shaping engagement and organizational culture. Dialogue Social Science Review, 3(4), 551–568.

Sayyam, I. U. R., & Khan, S. (2021). Fear of COVID-19 and turnover intention: A mediated moderation analysis. Asian Social Studies and Applied Research, 2(3), 406–416.

Sayyam, M. H., & Adil, M. (2020). The role of talent management practices on employee innovative work behaviour: Moderating role of transformational leadership. International Review of Management and Business Research, 9(4), 338–346.

Sayyam, M. U., Tufail, M., & Ishaque, A. (2020). The role of informal learning in employee innovative work behaviour: Mediating role of transformational leadership. Journal of Business and Tourism, 6(1), 189–207.

Sayyam, R. B., Khan, M. T., & Adil, M. (2020). The impact of knowledge sharing behavior on project team performance:

Mediating role of project team effectiveness. Journal of Business and Tourism, 6(2), 101–115.

Sayyam, R. U. R., & Sabir, S. N. (2025). Sustainable practices, digital tools, and SME success: A pathway to long-term growth. Policy Research Journal, 3(3), 2025.

Sayyam, R. U. R., & Sabir, S. N. (2025). The digital edge: Social media strategies for SME success. International Journal of Social Sciences Bulletin, 3(3), 766–781.

Sayyam, R. U. R., Mubarak, R., & Khan, A. A. (2025). Green leadership: Driving organizational change toward sustainability. Center for Management Science Research, 3(3), 97–112.

Seib, P. (2012). *Real-time diplomacy: Politics and power in the social media era*. Palgrave Macmillan.

Shah, S. N., Tufail, M., & Khan, I. (2025). Analyzing the mediating role of perceived organizational support between authentic leadership and employee creativity. Journal of Media Horizons, 6(1), 449–461.

Shahzad, S. S., Sayyam, A., Rahman, R. U., & Khan, I. (2024). Determining the effect of realistic job preview on counterproductive work behavior: Evidence from degree awarding institutions Khyber Pakhtunkhwa, Pakistan. International Journal of Social Science Archives, 7(3), 20.

Sharma, R. (2018). Surveillance, censorship and digital freedoms in Pakistan. *Asian Journal of Cyber Law, 4*, 112–130.

Smith, M. R., & Marx, L. (Eds.). (1994). *Does technology drive history? The dilemma of technological determinism*. Cambridge, MA: MIT Press.

Ullah, S. H., Khan, I., & Tahir, M. (2025). Analyzing the impact of institutional and environmental sustainability factors on credit risk in banking sector: A multifaceted approach from Asian economies. Policy Research Journal, 3(3), 329–342.

Umair, M., Alam, S., Rahman, R. U., & Shah, S. T. H. (2025). Leadership and AI-driven innovation: Pathways to entrepreneurial success in Pakistani higher education. Qualitative Research Review Letter, 3(3), 385–407.

UNCTAD. (2022). *Data protection and privacy legislation worldwide*. United Nations Conference on Trade and Development.

Waheed, S. (2020). The shrinking space of digital rights in Pakistan. *Pakistan Journal of Human Rights, 3*(1), 87–102.

West, D. M. (2020). *How artificial intelligence is transforming the world*. Brookings Institution. Retrieved from https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/

West, D. M. (2020). *The role of AI in governance and policy*. Brookings Institution Report. Retrieved from https://www.brookings.edu/research/ai-governance/

Yousaf, F. (2021). Pakistan's digital diplomacy: Trends and challenges. *Journal of International Affairs, 5*(2), 45–60.

Yousaf, K. (2021). Pakistan's strategic communication through Twitter: A case study of the DG ISPR's account. *Journal of Content, Community & Communication, 13*, 51–61. https://doi.org/10.31620/JCCC.12.21/06.

Zeb, A., Sayyam, A., Amin, M. Y., & Awan, S. H. (2025). Sustainable leadership: Balancing people, profit, and planet. Center for Management Science Research, 3(2), 15–28.

Rahman, R. U., Alam, S., & Majeed, R. (2025). From challenge to growth: How opportunity recognition and digital adoption drive SME performance in Pakistan. Pakistan Journal of Social Sciences Review, 4(4), 993–1015.

Alam, S. G. Q., & Ilyas, M. (2024). Small firms, big impact: Exploring sustainability drivers in textile SMEs through reporting, risk, and leadership. Policy Journal of Social Science Review, 2(6), 69–90.

Ilyas, M., Alam, S., & Rahman, R. U. (2024). Leadership and digital transformation in hospitality industry: Evidence from Pakistan. Journal of Management

Science Research Review, 3(4), 1521–1536.

Shah, S. T. H., Alam, S., & Rahman, R. U. (2024). Unlocking collaboration: How organizational culture shapes knowledge sharing and hoarding among faculty. International Journal of Social Science Archives, 7(1), 620–637.