



Muhammad Nayyer Adnan¹

¹MPhil Scholar in International Relations at Riphah International University, Islamabad.

Email: Nayyeradnan9955@gmail.com

KEYWORDS	ABSTRACT
strategic communication, counter-propaganda, deepfakes, media literacy, information integrity, disinformation, and hybrid war, highlighting the critical importance of these concepts in the context of Pakistan.	In the modern shape of conflict, strategic communication has emerged as an integral part of national security, as the battle now hinges on a mix of military pressure, cyber, politics, terrorism, economic coercion and the manipulation of the information environment. Pakistan is especially vulnerable to these pressures. Its media landscape is polarised, its digital population is growing, terrorist groups are still using media for recruitment and intimidation, and both domestic and foreign actors are abusing social media to spread fake, out-of-context and/or emotionally manipulated information. The paper explores Pakistan's strategic communication architecture, maps the main propaganda/disinformation tools targeting national institutions and society and reviews the measures under the current framework. It identifies substantial institutional assets but no adequate national system through a qualitative analysis of official policies, laws, peer-reviewed research, institutional reports, material on platform transparency and the international governance standards. Sharing confidential information regarding threats to the information is recognized as a policy in Pakistan, a public-information body was established, Pakistan has diplomatic communication networks, counter-extremism narratives have been developed, cyber-response capacity has been built and an emerging artificial-intelligence policy has been formulated in the country. Requirements are still somewhat dislocated, however answers are often reactive, requirements for attribution are not consistent, there is a limited ability to use the local language, and success is sometimes measured by product, and not by changes in belief, trust or resilience. The paper suggests a rights-based national coordination of civilian policy, a permanent fusion mechanism for information and environment, standards of evidence and attribution that are transparent, fast communication in multiple languages, independent fact-checking, artificial-intelligence and deepfake forensics, and media-literacy that is tailored to the needs of the audience, as well as platform cooperation, public diplomacy integration, legal safeguards, and measurable performance indicators. The main thesis of this text is that the better way to deal with the negative narrative is not to propagate Pakistan-centric propaganda but to communicate the truth quickly, credibly, inclusively and in a manner more aligned to the performance of policy.
ARTICLE HISTORY Date of Submission: 24-04-2026 Date of Acceptance: 18-05-2026 Date of Publication: 20-05-2026	 2026 Journal of Social Research Development
Correspondence	Muhammad Nayyer Adnan
Email:	Nayyeradnan9955@gmail.com
DOI	https://doi.org/10.59075/jsrd.v7i3.609
Volume/Issue	7(3), 2026, 64-81

Introduction

The information landscape now becomes a space where national power is wielded, challenged and assessed. Text, images, video and emotion are transmitted quickly and effectively through networks that mediate military operations, diplomatic relations, law enforcement, economic policy, public health, disaster response and political legitimacy. A false post can spread to millions before an official institution can verify the facts; a true video can be posted with a fake date or location; an anonymous account can act as one of a government office; and a coordinated network can create a sense of public consensus. These practices are not intended to be a substitute for traditional security concerns. They communicate with them, which determines citizens' response to emergency calls, foreign audience's perception of a state's version of an emergency, and the recruitment, intimidation, and polarization of members of violent groups.

This is the challenge that Pakistan is facing in an unprecedented manner. Terrorism and violent extremism have been ongoing in the country, with political confrontations and civil-military issues occurring regularly, followed by regional strategic competition and the mistrust among segments of the public, political parties and media. Meanwhile, digital connectivity has grown the scale and speed of national communication. According to the Pakistan Economic Survey 2025-26, there are nearly 160 million broadband subscribers till March 2026 and cellular coverage is provided to more than 160 million people, the broadband penetration rate is over 64 percent (Government of Pakistan, Finance Division, 2026). These are not unique users, but they are the clear sign that social, messaging and mobile video are no longer 'side channels'. They play a crucial role in political engagement, crisis awareness and routine news use.

Strategic communication is not just that so-called publicity. It is the systematic organisation of policy, action, words, images, relationships and feedback such that national institutions "tell a credible story regarding what they are doing and why. It involves public information, crisis communication, public diplomacy, military communication, counter-terrorism message, digital engagement and societal resilience building in the longer term. It is effective only if there is consistency between what institutions say and what citizens do. If the performance doesn't align with the messaging, then communication can't fill the credibility void. On the other hand, if disclosure is done in a timely manner, uncertainty is acknowledged, errors are corrected and accountability is seen, trust can be maintained even in the event of an adverse occurrence.

The term counter-propaganda can be taken as a license to manipulate audiences in response to the manipulation of other audiences. The term is used more narrowly and normatively here: Exposure of false stories, providing verifiable facts and context, the breaking of coordinated manipulation (by legal means), and the enhancement of the public's ability to assess information. When it challenges official claims, it is not propaganda, it is legitimate criticism, investigative journalism, satire, or academic research or political dissent. To treat them as such creates a divide between evidence-based security communication and partisan control, ultimately weakening national resilience.

The paper offers four answers to the questions. First, who or what forms the current strategic communication infrastructure and policies in Pakistan? Second, which actors, techniques and technological conditions influence propaganda and disinformation that impacts on Pakistan? Third, what are the effectiveness of current counter-propaganda and resilience programs? Fourth, what could be a more comprehensive framework to enhance coordination, credibility, technological capacity, public trust, and legal legitimacy? What follows is an argument for why Pakistan has many of the institutional pieces in place, but they lack a shared doctrine, standards for evidence, enduring coordination procedures, and independent measurement systems. Instead, the focus of reform ought to be on integration and credibility, not more channels or content.

Conceptual and Analytical Framework

Hallahan et al. (2007) see strategic communication as the intentional use of communication by an organization to accomplish its purpose or mission. This definition should be broadened in the national-security world beyond the message. Paul (2011) proposes that effective strategic communication involves the synchronization and coordination of words, images and actions and that the effect of a policy is not only brought to the fore by official statements, but also by operational actions, institutional competence, and by the experiences of those who are impacted. While citizens assess a measure's protection by its implementation, procedure, and outcomes, a government can assert that it is both. The say-do gap (and the discrepancy between what is said and what is done) is thus a focal point of analysis.

The second conceptual lens is strategic narratives. In the case of narratives, Miskimmon et al. (2013) say that they are the ways in which actors in the political system try to make sense of the international system, national identity and policy issues in particular. In Pakistan, debates on sovereignty, constitutionalism, terror, economic development, religious identity, regional tension and civil-military relations are all happening at the same time in the same information space. National strategic narrative cannot be established by slogans. It should be coherent in time and connect to the widely shared values, and it should provide space for multiple viewpoints within the constitutional system. Public diplomacy has a similar role in the external sphere, which involves building relationships, explaining a country's views and inspiring attraction and/or legitimacy instead of just force (Nye, 2008).

The paper distinguishes between the concept of propaganda and that of information disorder. Propaganda is normally defined as a deliberate and systematic attempt to manipulate perceptions and influence behaviour in a manner that is conducive to the propagandist's aims (Jowett & O'Donnell, 2019). Wardle and Derakhshan (2017) define misinformation as false information that is disseminated without evidence of malicious intent, disinformation as intentionally false or deceptive information, and malinformation as information that is true but has been used in a harmful, misleading, or decontextualised way. The differences are significant when it comes to doing business. It is essential that a citizen who unwittingly forwards an old video is corrected and educated; a coordinated network that creates fake government documents must be investigated,

attributed and platform-enforced. An authentic record that has been leaked doesn't need to be claimed to be "a fake", it needs to be put in context and the personal information protected.

The linking principle is trust. Studies indicate that fake news can travel faster and further than factual news, particularly when they evoke emotion and novelty, which leads to human sharing (Vosoughi et al., 2018). Both echo chambers and partisan clustering can decrease exposure to corrective information (Cinelli et al., 2021); language attacking an out-group was strongly linked to social-media engagement (Rathje et al., 2021). This encourages official communicators to copy sensational content. This can create a short-term impression but can lead to a loss of credibility in the long term. Instead, the goals of strategic communication should be to maximize verified reach, correction uptake, confidence in institutions, and behavioural resilience. The United Nations Global Principles for Information Integrity, then, have societal trust, public empowerment, independent media, healthy incentives and transparency at the heart of information governance (United Nations, 2024).

Methodology and Limitations

The research method applied in this study is a qualitative method with a type of interpretive review of the secondary evidence. The sources were drawn from five categories: Sources from official Pakistani policy and legal documents; Sources from institutional descriptions and reports on the performance; Sources from peer-reviewed scholarship on strategic communication, misinformation, algorithms, violent-extremist narratives, and deepfakes; Sources from transparency reports by digital platforms and by specialist investigations; and Sources from international standards on information integrity and platform governance. The key materials of Pakistan are the National Security Policy 2022-2026, National Cyber Security Policy 2021, National Artificial Intelligence Policy 2025, National Action Plan and revised National Action Plan, National Prevention of Violent Extremism Policy 2024 and Prevention of Electronic Crimes (Amendment) Act 2025, Pakistan Economic Survey 2025-26.

The technique used is the triangulation method. Establishing official mandates and declared achievements is done through official sources, whereas institutional self-reporting is not as good as official tracking. Assumptions of audience behaviour, rights and programme design are tested through academic research and civil-society analysis. Platform reports are used to show how to work with coordinated manipulation; they do not reveal the entire information in platforms. Limitations of the study include the lack of classified threat assessments, limited access to platform level datasets from Pakistan, the fast-paced evolution of technology and the challenges faced in attributing information operations to a state without a public evidentiary trail. It thus distinguishes verified findings, official claims, and analytical inferences, and refrains from attributing state responsibility in the event evidence is made available that proves an operation had certain interests.

Strategic Communication Architecture of Pakistan

Integrated approach has the best basis at the policy level with the National Security Policy 2022-2026. It has a whole-of-government perspective on security, focuses on the state-citizen linkages and sees the integration of social cohesion and a coherent national identity as key concerns of the state. It further cautions that by internal or external support divisive discourse can be nurtured, and urges an all-inclusive national discourse (Government of Pakistan, National Security Division, 2022). These principles integrate communication within a more citizen-oriented security model. The policy itself, however, is not publicly available to provide detailed operating procedures for information incidents, does not set out attribution thresholds or a single institution for cross-government communication performance.

Table 1. The functions of the principal institutions and strategic communication.

Institution	Current role	Priority coordination need
National Security Division	Whole-of-government security policy; social cohesion and citizen-state link.	Translate policy principles into doctrine, roles, crisis protocols, and annual assessment.
MoIB / Press Information Department	Domestic public information, media monitoring, feedback, briefings, and dissemination.	Direct access to verified operational data; multilingual digital correction and disclosure protocols.
Ministry of Foreign Affairs	Public diplomacy, strategic communications, missions abroad, and international media engagement.	Shared evidence packages and sustained relationships with foreign media, researchers, and diaspora audiences.
NACTA	Counter-terrorism policy, PVE, national narrative, and counter-extremism outreach.	Audience segmentation, local-language delivery, community partnerships, and outcome evaluation.
Defence / ISPR liaison	Communication on military operations, terrorism, border incidents, and defence policy.	Civilian-military deconfliction, common timelines, casualty standards, and evidence-release procedures.
MoITT / National CERT	Cyber policy, incident response, technical analysis, AI policy, and digital capacity.	Fuse cyber indicators with influence analysis while maintaining privacy and human oversight.
PTA / PEMRA / NCCIA	Telecom and media regulation, complaints, content processes, and cybercrime investigation.	Narrow legal thresholds, transparency, independent review, notice, appeal, and accuracy audits.
Provincial and local institutions	Local crisis information, policing, health, education, disaster response, and community engagement.	Common tools, regional-language capacity, trained spokespersons, and two-way feedback.

The basic structure of the public-information system within the country is the Ministry of Information and Broadcasting and the Press Information Department attached to it. According to its own description, the ministry's main department for timely and accurate dissemination is PID, which has mechanisms for media projection, monitoring, feedback, facilitation and research throughout the day (Press Information Department, n.d.). This provides it with a history of the press, and institutional memory. However, modern strategic communication doesn't just revolve around gathering coverage, issuing releases and that's it. It needs access to reliable operational data, social listening without infringing on privacy, clear correction procedures, multilingual digital production, and the right to have quick answers from line ministries. If the public-information system has no connections, then it can become a downstream publisher of the material produced at different speeds and evidentiary standards.

The external communication/public diplomacy side is provided by the Ministry of Foreign Affairs. In 2020, it started its Strategic Communications Division to bring about a revolution in communication and enhance technology-based engagement by way of Pakistan's missions abroad. The ministry's work on the coordinated social media presence and the establishment of the Share Pakistan Portal to map the public-diplomacy activity has also been in progress (Ministry of Foreign Affairs, Government of Pakistan, n.d.). This network is important because it has a strategic value for foreign audiences, the international media, the multilateral institutions, the think tanks and the diaspora communities, who need evidence and a different framing from the domestic. It is effective when it is used at the beginning of the crisis to provide an accurate record to both sides and continues in use throughout the relationship between crises, not as a counter-argument to an already entrenched political narrative.

NACTA has a specialized counter-terrorism and prevention-of-violent-extremism piece. The National Action Plan of 2014, its revision in 2021, Paigham-e-Pakistan national narrative and National Prevention of Violent Extremism Policy 2024 also acknowledge that the fight against terrorism cannot be done just through kinetic action (National Counter Terrorism Authority, 2014, 2021, 2024). Paigham-e-Pakistan is significant for building a consensus between scholars across all the sects on the issue of terrorism and the illegal application of violence. It offers theological and constitutional legitimacy to reject extremist claims. Meanwhile, on the other side of the discussion, the research finds limitations in audience segmentation, audience-specific local-language dissemination, political ownership, civil-society involvement, root-cause engagement, and the use of credible former extremists/community intermediaries (Makki & Khan, 2019). The message of the lesson is that an authoritative national text is not a complete communication strategy.

The digital-governance layer has been enriched. The National Cyber Security Policy, 2021, aims to safeguard the national digital ecosystem and the National Artificial Intelligence Policy, 2025, focuses on ethical and responsible use, respect for human rights, infrastructure, data protection, awareness, partnerships, and secure innovation (Ministry of Information Technology and Telecommunication, 2021, 2025). The National Computer Emergency Response Team has established incident-response, vulnerability-assessment, training and international cooperation

capabilities. During the initial nine months of fiscal 2025-26, National CERT enhanced regional cooperation, performed training, and evaluated hundreds of government websites, according to the Pakistan Economic Survey (Government of Pakistan, Finance Division, 2026). While cybersecurity and information integrity are not the same, many of the technical characteristics of a hack and leak, impersonation campaign or bot-enabled influence operation are similar. A mature system would have to link cyber incident responses with communication analysis without mixing in criticism and cyberattack.

There are regulatory and enforcement functions by PTA, PEMRA and cybercrime-investigation bodies. PTA regulates telecommunications and applies the relevant requirements to online content and PEMRA regulates private electronic media. Under Prevention of Electronic Crimes (Amendment) Act 2025, new institutional mechanisms have been introduced for the regulation of social media and for the establishment of the National Cyber Crime Investigation Agency (NCA) (Government of Pakistan, 2025). These instruments can be used to help make a complaint, investigate cases, preserve evidence, and seek redress in court for impersonation, threats, fraud, or organized crime activity. They also introduce legitimacy concerns where notions like “false information” are vague or where there is a wide scope of executive discretion or if there is inadequate notice and appeal. The constitution of the Islamic Republic of Pakistan, 1973, articles 19A and 248, as well as independent analysis by the Human Rights Commission of Pakistan (HRC) and the National Commission for Human Rights (NCHR), reinforces the necessity to ensure that expression and access to information is handled in a manner that is legal, necessary, proportional, in accordance with due process, and independently reviewed. Human Rights Commission of Pakistan, 19, 19A; National Commission for Human Rights, 2025, 2026).

The architecture is completed by provincial information departments, police, district administrations, health authorities, disaster-management institutions, educational institutions, and local governments. Usually, they are the first to be in touch with the communities concerned in matters of terrorism, sectarian tension, disasters, and fake rumours in the villages. But they typically lack digital capacity, access to common tools for verification, and local-language resources. A coherent national policy should therefore be decentralized: national standards and common infrastructure at the national level, and province and local adaptations of the message, but not national production of all messages.

Sources, Methods and Strategic Effects of Propaganda

Propaganda threat to Pakistan is not just an opponent campaign but an ecosystem. For example, foreign influence networks, terrorist and sectarian groups, domestic political parties, anonymous commercial pages, content generators looking for revenue, self-exiled groups and opportunists can create or boost false information. Their objectives differ. A foreign network can look for diplomatic isolation or institutional distrust; a terrorist group can look for recruitment, fear, polarization or proof of state weakness; a political campaign can look for an electoral gain; a commercial operator can look to make some money out of outrage. These actors may act out of the script without any central

authority. The process of attribution, then, should take place based on evidence of content, behavior, infrastructure, and organization, and command, not on political convenience.

EU DisinfoLab has investigated a documented foreign-influence case, called Indian Chronicles. Identified were a network of websites, organisations and identity practices based in Brussels and Geneva that re-posted content, utilised outdated organisations and media brands and promoted a significant agenda of undermining Pakistan and Indian interests (EU DisinfoLab, 2020). The public record establishes that the network exists and is going where, but it doesn't prove that any anti-Pakistan narrative is Indian government's. There is a difference in the distinction. Over-attribution can backfire, because it can lead to the trivialization of real domestic problems as foreign manipulation, and make subsequent, more substantiated attribution less believable.

It is important to note that platform transparency reports also emphasize the importance of not having a partisan approach. Meta has deleted coordinated inauthentic networks from India and Pakistan, as well as networks focused on audiences in India and Pakistan (Meta, 2019, 2020, 2021). Coordinated manipulation is not a nationality, these cases demonstrate. Accounts can hide behind the cover of their operators, pretend to be independent media, organize groups of pages, copy and paste content, or pretend to be characters to generate content that will be regurgitated by a real person. Public agencies must look for indications of this behaviour in the network patterns and technical evidence rather than making an assumption that any coordinated political campaign is illegal. Transparency of sponsorship and identity is frequently a more defensible policy goal than government judgment about viewpoint.

Table 2. Threat-response matrix

Threat method	Typical mechanism	Evidence-led response
False context / recycled media	Old or foreign footage is relabelled as current and local.	Publish original date, location, source, full clip, and visual comparison.
Forged notice / impersonation	Fake orders, alerts, or accounts borrow institutional authority.	Digitally signed notices, verified archives, rapid alerts, and platform impersonation channels.
Coordinated inauthentic behaviour	Hidden networks manufacture consensus or flood discussion.	Behavioural and network evidence, sponsorship disclosure, platform action, and confidence levels.
Extremist propaganda	Ideology, grievance, fear, operational claims, and selective imagery support recruitment.	Credible messengers, theological and constitutional rebuttal, victim support, inclusion, and governance response.
Deepfake / voice clone	Synthetic audio or video attributes false speech or conduct to a public figure.	Tiered forensics, provenance, human review, rapid authentication, and public explanation of uncertainty.
Hack-and-leak	Authentic stolen material is	Separate authenticity, completeness,

malinformation	selectively released and framed with false conclusions.	legality, and interpretation; acknowledge verified facts.
-----------------------	---	---

The characteristics of terrorist and violent-extremist propaganda are different. It includes ideology, selective reporting, martyrs narratives, successful claims of operations, criticism of government, and attempts to elicit a "too much" government reaction. May draw on local grievances relating to policing, development, displacement, sectarian discrimination or political exclusion. Theological rebuttal is not enough, then. While Paigham-e-Pakistan can challenge unapproved violence, counter-messaging needs to be effective in terms of service delivery, legalism, victim support, reintegration mechanisms, and political engagement. If the grievances are actually legitimate as they are here, then to deny them is to provide proof to the propagandists of the extreme right wing that official communication is not connected to reality.

In Pakistan's daily information landscape, the most common is not a completely created story, but fake context. A clip from an old event in another country is reframed as a current event; a question or statement is sliced out of a longer video; a fragment of a notification replaces the entire text; a photo of a dead or injured person is substituted; preliminary casualty statistics are provided as final; or a real data point is claimed as a conclusion it doesn't warrant. Firstly false context is effective because visual evidence looks self-evident; secondly, because the verification takes time. The proper answer is not just to mark a post as false, but to post the source, date, location, whole clip, document metadata, and an explanation of how the clip was manipulated.

Strategic effects that propaganda is able to create are cumulative. It may lead to a loss of confidence in elections, courts, security services, public-health guidance, economic statistics, and more; raise tensions between ethnic, sectarian, political, and/or provincial groups; make foreign investment and tourism difficult; make diplomatic bargaining more complicated; and drive institutions into a constant reactive communication cycle. Not always is the worst thing that happens believing one thing. It's the uncertainty that's generalized - the belief that no one can be trusted, and there is nothing but partisanship in every fact. Lazer et al. (2018) characterize misinformation as a system, comprised of technology, psychology, institutions, and incentives. The Pakistani reaction needs to be more comprehensive than just reacting to every viral claim as a media incident and needs to focus on the system.

Artificial Intelligence, Algorithms, Deepfakes and Digital Misinformation

AI alters the creation and identification of manipulative content. Generative systems can generate fluent text, realistic images, cloned voices, translated propaganda, fabricated personas and variations of the same claim at low cost. This enables an operator to customise narratives in Urdu and local language, mimic a local identity and engage and interact continuously with low manpower. The danger is nothing new for spectacular political deepfakes. Fake profile photos, fake screenshots, fake voice messages, fake comments might be more prevalent and harder for users to identify, due to their similarity to the platform's normal content.

There are two related harms caused by deepfakes. First, a convincing synthetic recording can claim that events or actions are the work of a political, military, judicial or religious entity. Second, there is now a way to discredit legitimate evidence: the liar's dividend suggested by Chesney and Citron (2019), the deepfake. Recent studies have indicated that even if the synthetic video doesn't convince the majority of viewers of the fictionalized fact, it can still cause uncertainty and distrust (Vaccari & Chadwick, 2020). Polarization in Pakistan means that doubt can sometimes be an effective device: it erodes consensus in the crisis, allows them to disbelieve inconvenient evidence, and places a burden on institutions to prove their authenticity in a hurry.

Detection technology is required but not definitive. Forensic accuracy can be affected by the compression, reposting, using screen recording, language variation and quick changes in generation models. False positives could lead to serious falsification of the credibility of authentic journalism, while false negatives could cause false confidence. There is a need for a multistaged automated triage with metadata and provenance analysis of the media, reverse search, voice and visual forensics, source verification, and human experts' review of the synthetic media in Pakistan. Public statements need to convey the evidentiary basis and level of confidence: such as, verified manipulation, probable synthesis, inconsistent metadata, or still under assessment. Definitive labelling should not be done based on the score of one detector.

Algorithms are also a threat, regardless of whether they're made up artificially or not. Recommendation systems work on the basis of predicted engagement, and controversial content tends to attract comments, shares, and content watched time. Studies on out-group language, false news, and echo chambers demonstrate how novelty, polarization and hostility can be granted a structural advantage (Vosoughi et al., 2018; Cinelli et al., 2021; Rathje et al., 2021). The linguistic diversity of Pakistan also poses a challenge to moderation as that content and coded language in Urdu, Roman Urdu, Pashto, Punjabi, Sindhi, Balochi, Saraiki and mixed language formate may not be subject to the same degree of consistency in moderation as English content. There is another layer of encrypted or closed messaging channels where authorities have only limited visibility of the messages, but rumours are likely to spread fast in the family, work, religious, and neighborhood circle.

The National Artificial Intelligence Policy 2025 is also a policy to take note of since it has a strong policy base that connects AI adoption with ethics, security, awareness, data governance, human rights, and institutional capacity (Ministry of Information Technology and Telecommunication, 2025). These are the principles for information integrity that it needs Pakistan to invest in: Local language datasets, deep fake and voice clone research, provenance standards, content-authentication tools, and National CERT to university to media lab to platform to law enforcement connections. AI can also be employed in a defensive manner to perform multilingual transcription, claim clustering, anomaly detection, and quick comparison with authoritative data. These must be supervised, monitored, have privacy restrictions, include audit trails, and be tested for political and linguistic bias.

Beyond takedown requests is the platform-governance response. UNESCO's Guidelines for the Governance of Digital Platforms highlight human-rights due diligence, transparency, access to information, multistakeholder participation, and accountable processes (UNESCO, 2023). Pakistan should explore avenues for crisis escalation, transparency in disclosure of coordinated influence operations, researcher access to privacy protected data, governments' reporting of requests and consistency in enforcement against impersonation and covert coordination. Cooperation should be related to behaviour and harm and not to political alignment. It should also maintain legality of expression and notice and appeal, as it could be used as a proof of propaganda charges of censorship or institutional fear if it is removed without proper notice and appeal.

Assessment of current counter-propaganda measures

Monitoring of the rapid and coordinated hostile digital activity has improved, and there are reports of active responses to this activity. During cross-border tension, round the clock monitoring and action is taken on hostile digital assets, as mentioned in the Pakistan Economic Survey 2025-26 (Government of Pakistan, Finance Division, 2026). This sets up the state to be able to move technical and communication resources. The output measures – for monitored accounts, blocked assets, posts or impressions – are not measures of strategic effect, however. They do not indicate whether a false belief was reduced, whether neutral audiences believed Pakistan's evidence, whether public trust increased or whether enforcement had a negative impact on legitimate speech. Independent baseline and follow-up research is needed for effective evaluation.

The value and limitation of a national narrative is shown by Paigham-e-Pakistan. It is a cross-sect religious consensus that directly refutes claims of an extremist nature that violence towards the state or civilians is religiously sanctioned. It also links the rejection of terrorism with the Constitution and collective responsibility, in its language. However, Makki and Khan (2019) conclude that the program needs to be more targeted and localized, translated into the local language, disseminated widely, involve civil society, address governance and socioeconomic issues and have a more diverse group of credible messengers. The main lesson is that in all counter-propaganda a message from authority needs to be turned into products that resonate with the audience, communicated through trusted relationships and backed by policy.

In Pakistan, the evidence for media-literacy research is quite unique and practical. Ali and Qazi (2022) reported that digital skills were unevenly distributed amongst Facebook users in urban Pakistan and lower literacy levels were correlated with higher susceptibility to false content. They conducted a randomized experiment later, which revealed that the use of generic educational video was not found to have a significant effect on identification, but personalized feedback related to the engagement of the participants was found to have a significant effect on discernment (Ali & Qazi, 2023). This indicate that single campaigning for awareness and general slogans will not yield lasting resilience. Interventions should be repeated, interactive, culturally and linguistically adapted, and tailored to the problems of target populations.

Nevertheless, threats, impersonation, fraud, coordinated criminality and unlawful access to data will require regulation and criminal investigation, but these are not alternatives to communication. Broad and opaque enforcement can create a chilling effect, and diminish the desire of journalists, researchers, and citizens to share information with authorities. The vague definitions, institutional independence, due process and impact on expression are key points raised by national human rights bodies against the 2025 amendments to the PECA (Human Rights Commission of Pakistan, 2025; National Commission for Human Rights, 2026). When action is legally permitted, the state shall provide a factual basis, states law, scope, duration and avenue of appeal. This transparency in procedure is also a counter-propaganda tool as it lessens the chances of bringing all moderation into the frame of mind of arbitrary suppression.

One remaining deficiency is that rebuttal is more prevalent than pre-emption. Once a narrative has gone viral, often the institutions will respond after it has been repeated and thus partisan. This disadvantage can be minimized by providing audiences with prescriptive warnings about common manipulation techniques before exposure (prebunking). The strategy is especially effective during certain known events, like elections, high-security anniversaries, budget decisions, sectarian events, public-health crises, and border issues. Prebunking should not be a way to inform citizens of which political conclusion to take. It should inform users how notices may be forged, how to use the old footage, how to listen to anonymous voice notes, how to use the selective clips, how the fake surveys might be operated and how to go to fast verification channels.

Strategic and institutional gaps

The first is fragmentation. Pakistan doesn't have a publicly-adopted doctrine defining strategic communication, explaining the difference between strategic communication and propaganda and censorship, assigning responsibilities during the routine and crisis phases, and providing a standard process on how to deal with information incidents. Agencies then keep their own watch on various domains, have varying labels, and issue sometimes conflicting reports. The second is credibility management. In particular, officials are pressured to convey a sense of certainty and success, and message discipline, even when the facts remain incomplete. This can result in untimely claims, delayed corrections, or no correction. A system that admits and fixes mistakes publicly will tend to retain more trust than a system which looks like it knows the right answer and then gets it wrong.

The third gap is related to the evidence and attribution. Often, in the case of public accusations, there is no intermediate evidence but a leap from a hostile narrative to a foreign sponsorship claim. The next rung up the attribution ladder should be verification of the content, followed by analysis of coordinated behaviour, technical infrastructure, and organizational links, and then responsibility should be attributed. Confidence level and alternative explanations should be documented. The fourth one is inclusion. The national messaging is very often created in Islamabad, in formal Urdu or English and then shared in elite media. Rural people, young people, women with unequal access to digital tools, people with disabilities, and speakers of regional languages might only be able to receive information late, or via less trusted channels.

The fifth gap is measurement. Press releases, posts, followers, views, takedowns, seminars, or hashtags can easily be counted, but lack strong measures of resilience. There is a need for indicators of response time, factual response, belief change, the trust of sources, the reach of the audience to vulnerable communities, uptake by international media, reversals in enforcement, false positives, and overall performance in time in Pakistan. Limited institutionalisation of independent expertise is the 6th gap. The role of universities, professional factcheckers, investigative journalists, behavioural scientists, technologists and civil-society organisations should not be treated as that of the mere message multiplier. They must have access to data, clear access to grants, editorial independence and formal challenge of official assessments.

An Integrated National Strategic Communication Framework

Pakistan needs an integrated national strategic communication policy with a goal of maintaining the integrity of public decision making while ensuring the constitutional freedoms and political pluralism. The policy should clearly define that the main tools of credibility are truthful communication, disclosure of uncertainties, and consistency of policy and performance. It should refuse to collude in covert domestic manipulation, to fabricate evidence, to adopt state personae, to counter-inform against legitimate criticism. This normative limit does not impede security, but sets a difference between what is being opposed and legal state communication.

The government should first set up a National Strategic Communication Council, with civilian supervision, and have a permanent professional secretariat. The council should consist of representatives from the National Security Division, Ministry of Information and Broadcasting and PID, Ministry of Foreign Affairs, Interior Ministry and NACTA, Defence/ISPR liaison, Ministry of Information Technology and Telecommunication, National CERT, PTA, PEMRA (when available), election and emergency-management institutions, and provincial representatives. The council should approve doctrine, priorities, safeguards and annual assessments. It should not be used to approve all messages or to be used for routine departmental communication. It would be important, if it existed, for policy coherence, authority to act on mandate conflicts and accountability for national level performance.

Secondly, there should be a permanent Information Environment Fusion and Response Centre to support shared situational awareness. The centre's monitoring, analysis and reporting should be mixed, including open-source monitoring, media analysis, cyber indicators, diplomatic reporting, local-government inputs, public complaints and research partnerships. It should adopt the common taxonomy of incidents that includes misinformation, disinformation, malinformation, impersonation, coordinated inauthentic behaviour, extremist propaganda, synthetic media, hack-and-leak activity and public-safety rumour. The following information should be specified for each incident record: Claim, Status of Evidence, Audiences Affected, Potential For Harm, Lead Agency Responsible, Agencies Supporting, Legal Considerations, Communications Plan. Access control and confidentiality regulations are allotted not to let the centre be a device for the monitoring of legal political opinion.

Thirdly, Pakistan needs to adopt national standard of evidence and attribution. Public findings should categorize by verified, probable, possible, under assessment. An evidence package of a manipulated video may contain the original video, the earliest known source, evidence of the date and location, a frame-by-frame comparison, evidence of metadata, evidence of witness confirmation, and technical analysis. A coordinated-network assessment should be a statement of the behaviour difficulties that are being observed and should not indicate sensitive investigative methods. Any mention of an organisation or state should include a documented chain of infrastructure, behaviour, control and/or direction. If possible, within operational time, high consequence public attributions should be assessed by an independent review panel of technical, legal, diplomatic and subject experts.

Fourth, there must be a multilingual rapid response protocol for the government available at all times. The first goal in the initial stages of a crisis is to take up much of the information space by providing verified minimum facts: (1) What occurred on Saturday, (2) What is known, (3) What is not known, (4) Who is leading, (5) Where updates can be verified, and (6) When the next briefing will take place. A single incident brief should be shared with among agencies, with the specialized spokespersons still on hand. Any corrections must be made in the logbook that can be seen, not silently edited. Document products should be provided in English, Urdu, Roman Urdu and in the relevant region language, with captions, audio, accessible formats and low bandwidth versions. The high-risk notices should be signed with digital signatures or verification codes that are used to reference an official archive.

Fifth, there should be an independent federated fact-checking and research environment in Pakistan. A common claim registry could be developed by universities, newsrooms, professional associations, and civil-society groups, to track common false claims, sources, evidence, corrections, and geographic distribution. Public funding may be warranted, but it should be provided by an open and competitive process, with the obligation to disclose the funding source, and no power to dictate the findings. There is a need to rapidly provide documents and subject experts by government institutions and external partners should make their own conclusion whether an official claim is backed or not. This mutual accountability would increase the persuasive impact of the neutral audience for which the state responds in a verifiable way.

Sixth, National CERT and its partner universities should set up a Synthetic Media and Information Forensics Laboratory. It should include voice cloning of Urdu and regional languages, detection of deepfakes, image provenance, document forensics, bot and coordination analysis, and secure preservation of digital evidence as its priorities. Methods, limitations, and benchmark results should be published by the lab and they should participate in international proficiency testing. It should also have a triage system to assist journalists and provincial authorities. Automated tools should be used as guidelines; the final assessments should include the technical results in addition to source and context and human verification. Acquisition should be subject to auditing and safeguard against vendor claims not subject to independent testing.

Seventh, the media and information literacy should not be a slogan, it should be a continuing public competence. Core skills need to be part of the curriculum at school, in universities, and the civil service academies as well as in police and military education, and public broadcasting. Community programmes should rely on trusted voices in the community, and should include practical exercises to help people: verify the origin of a forwarded message on WhatsApp, locate the original image, compare a clip to the full speech, check for emotionally manipulative language, and take a moment before sharing. The case studies in Pakistan show that personalized feedback is more effective than general teaching (Ali & Qazi, 2023). Programmes should therefore consider age, gender, education, language, disability and previous digital experience, and should measure changes in behaviour after several months not on the number of visitors at one event.

Eighth, the Foreign Office's verification should be linked with the public diplomacy. In international crises, missions should be given a standardised evidence package, with timelines, maps, primary documents, imagery with provenance, legal positions, humanitarian information and brief answers to expected questions. Availability of foreign journalists, researchers, diaspora organizations and multilateral officials should be engaged regularly before crises through briefings and data access. Public diplomacy is relationally effective, a foreign editor is more inclined to consider Pakistan's evidence quickly if the relationship between Pakistan and the foreign editor is professional and credible. Information should also be localized and geared towards local issues and concerns, not be sent out as a one-size-fits-all social-media card globally.

Cooperation between platforms should be formalized with clear protocols, 9th. Pakistan needs to identify specific crisis contacts, streamline impersonation and credible threats procedures, ensure the preservation of evidence, reveal coordinated influence networks, and provide researcher (privacy protected) access. Requests should be made to government to specify the legal basis and type of harm, and platforms should provide transparency regarding compliance, rejection and appeals, on an aggregate basis. The arrangements for trusted flaggers must incorporate oversight and regular accuracy checks. If and when there is a dispute over content, but it is not illegal, platforms and authorities should perform in a manner that prioritizes context, provenance labels, minimizing recommendations of content that can be shown to be misleading, and providing links to authoritative information rather than automatic removal.

10th, the law should be limited and protected. Offences and regulatory powers against false information should be defined, show actual harm, include defences for journalism, satire, research, whistleblowing and good faith error, and have a demonstrable purpose. Independent authorization, reasoned written decisions, giving notice, granting appeals, time limits and public reporting should be applied to intrusive investigation and emergency restrictions. Oversight institutions shall publish the number and type of requests, results, processing time, reversals and complaints. These protections are designed to ensure security action is in line with constitutional rights and minimise reputational damages from security action perceived as politically selective.

Eleventh, there should be a link between communication and governance response. A narrative on security cannot replace protection of civilians; a narrative on inclusion cannot replace fair

treatment; and a narrative on economic stability cannot replace accessible and consistent data. A policy-performance matrix should therefore be a component of every major strategic communication plan that specifies the action to support each policy claim, the institution who is responsible for the action, what evidence will be shared with the public, and what feedback process will be in place for those impacted. If the state is not yet achieving an objective, then a credible and explanatory communication should outline the limitations, intermediate steps and timeline, not an aspiration as achievement.

Twelfth, Pakistan needs to have an evaluation and exercise program. KPIs should encompass median time to first verified update; time to the correction of claims by official sources; percentage of priority content in the language(s) available; reach to identified vulnerable groups; change in belief before and after the correction; public trust by institution/issue; pickup of evidence by credible international media; proportion of enforcement decisions reversed on appeal; false positive rate in synthetic media evaluation; and recurrence of previously corrected claims. A yearly independent information-integrity reporting should provide trends and lessons, while not revealing any sensitive operations. National exercises should involve simulating an election deep fake, a terrorist attack with conflicting casualty reports and a border incident, a disaster rumour and a hack-and-leak campaign. Red teams should challenge not just attacks, but also the delays, overclaims, rights violations and conflicting statements that may result from official procedures.

Conclusion

Trust should be the focus of an effective national strategic communication policy. Institutions should communicate early but with no over-excessive claims of certainty, disclose evidence that is proportionate to claims, correct errors on a visible basis, distinguish foreign manipulation from domestic criticism, and apply standards consistently, Pakistan should build up its capacity in local-language and synthetic-media technology, independent verification, public digital literacy, public diplomacy, and rights protecting regulation. Most importantly, communication must be tied to the performance of the policy, credible action is the best story.

A State that respects the constitution must not turn counter-propaganda into propaganda. It seeks to safeguard citizens' capacity to choose truthful information, build together while preserving pluralism, and give institutions a way to communicate on a lawful policy in an adversarial information context. Building resilience through a system of verifiable truth, coordination, technology, and accountable power – not through a reactive rebuttal or through a system of message control.

References

- Ali, A., & Qazi, I. A. (2022). Digital literacy and vulnerability to misinformation: Evidence from Facebook users in Pakistan. *Journal of Quantitative Description: Digital Media*, 2. <https://doi.org/10.51685/jqd.2022.025>

- Ali, A., & Qazi, I. A. (2023). Countering misinformation on social media through educational interventions: Evidence from a randomized experiment in Pakistan. *Journal of Development Economics*, 163, 103108. <https://doi.org/10.1016/j.jdeveco.2023.103108>
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753-1819.
- Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrocioni, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9), e2023301118. <https://doi.org/10.1073/pnas.2023301118>
- Constitution of the Islamic Republic of Pakistan. (1973, as amended).
- EU DisinfoLab. (2020). Indian chronicles: Deep dive into a 15-year operation targeting the EU and UN to serve Indian interests. <https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/>
- Government of Pakistan. (2025). Prevention of Electronic Crimes (Amendment) Act, 2025 (Act II of 2025). *Gazette of Pakistan*.
- Government of Pakistan, Finance Division. (2026). Pakistan Economic Survey 2025-26: Information technology and telecommunication. https://www.finance.gov.pk/survey_2026.html
- Government of Pakistan, National Security Division. (2022). National Security Policy of Pakistan 2022-2026. <https://www.nsd.gov.pk/>
- Hallahan, K., Holtzhausen, D., van Ruler, B., Vercic, D., & Sriramesh, K. (2007). Defining strategic communication. *International Journal of Strategic Communication*, 1(1), 3-35. <https://doi.org/10.1080/15531180701285244>
- Human Rights Commission of Pakistan. (2025). Prevention of Electronic Crimes (Amendment) Act 2025: Human-rights concerns and recommendations. <https://hrcp-web.org/>
- Jowett, G. S., & O'Donnell, V. (2019). *Propaganda & persuasion* (7th ed.). SAGE Publications.
- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094-1096. <https://doi.org/10.1126/science.aao2998>
- Makki, M., & Khan, N. (2019). Critical appraisal of Pakistan's efforts in (re)constructing a national narrative to violent extremism and terrorism: A case of Paigham-e-Pakistan. *Pakistan Journal of Terrorism Research*, 1(2), 1-32.
- Meta. (2019). Removing coordinated inauthentic behavior from India and Pakistan. <https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/>
- Meta. (2020). August 2020 coordinated inauthentic behavior report. <https://about.fb.com/news/2020/09/august-2020-cib-report/>
- Meta. (2021). May 2021 coordinated inauthentic behavior report. <https://about.fb.com/news/2021/06/may-2021-coordinated-inauthentic-behavior-report/>
- Ministry of Foreign Affairs, Government of Pakistan. (n.d.). Public diplomacy. <https://mofa.gov.pk/public-diplomacy>

- Ministry of Information Technology and Telecommunication. (2021). National Cyber Security Policy 2021. Government of Pakistan. <https://moitt.gov.pk/>
- Ministry of Information Technology and Telecommunication. (2025). National Artificial Intelligence Policy. Government of Pakistan. <https://moitt.gov.pk/>
- Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). Strategic narratives: Communication power and the new world order. Routledge.
- National Commission for Human Rights. (2026). PECA and the 2025 Amendments Act: An NCHR report. <https://nchr.gov.pk/>
- National Counter Terrorism Authority. (2014). National Action Plan. Government of Pakistan. <https://nacta.gov.pk/>
- National Counter Terrorism Authority. (2021). Revised National Action Plan 2021. Government of Pakistan. <https://nacta.gov.pk/>
- National Counter Terrorism Authority. (2024). National Prevention of Violent Extremism Policy 2024. Government of Pakistan. <https://nacta.gov.pk/>
- Nye, J. S., Jr. (2008). Public diplomacy and soft power. The ANNALS of the American Academy of Political and Social Science, 616(1), 94-109. <https://doi.org/10.1177/0002716207311699>
- Pakistan Electronic Media Regulatory Authority. (n.d.). About PEMRA. <https://pemra.gov.pk/>
- Pakistan Telecommunication Authority. (2023). Cyber security strategy for telecom sector 2023-2028. <https://www.pta.gov.pk/>
- Paul, C. (2011). Strategic communication: Origins, concepts, and current debates. Praeger.
- Press Information Department. (n.d.). About Press Information Department. Government of Pakistan. <https://pid.gov.pk/about>
- Rathje, S., Van Bavel, J. J., & van der Linden, S. (2021). Out-group animosity drives engagement on social media. Proceedings of the National Academy of Sciences, 118(26), e2024292118. <https://doi.org/10.1073/pnas.2024292118>
- UNESCO. (2023). Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach. <https://unesdoc.unesco.org/ark:/48223/pf0000387339>
- United Nations. (2024). United Nations Global Principles for Information Integrity. <https://www.un.org/en/information-integrity/global-principles>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media + Society, 6(1). <https://doi.org/10.1177/2056305120903408>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146-1151. <https://doi.org/10.1126/science.aap9559>
- Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe. <https://rm.coe.int/information-disorder-report/1680764666>