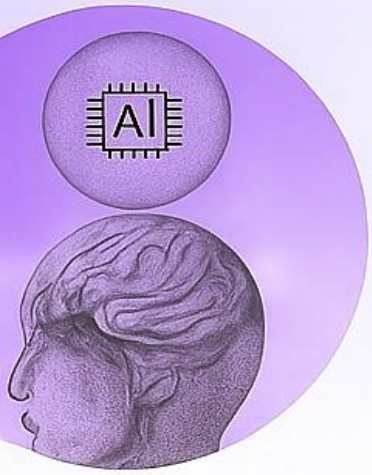
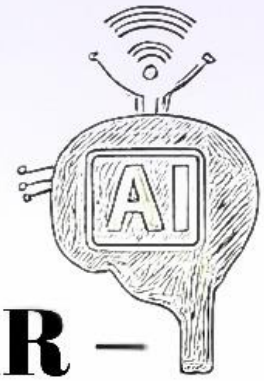
CASS

CENTRE for AEROSPACE & SECURITY STUDIES

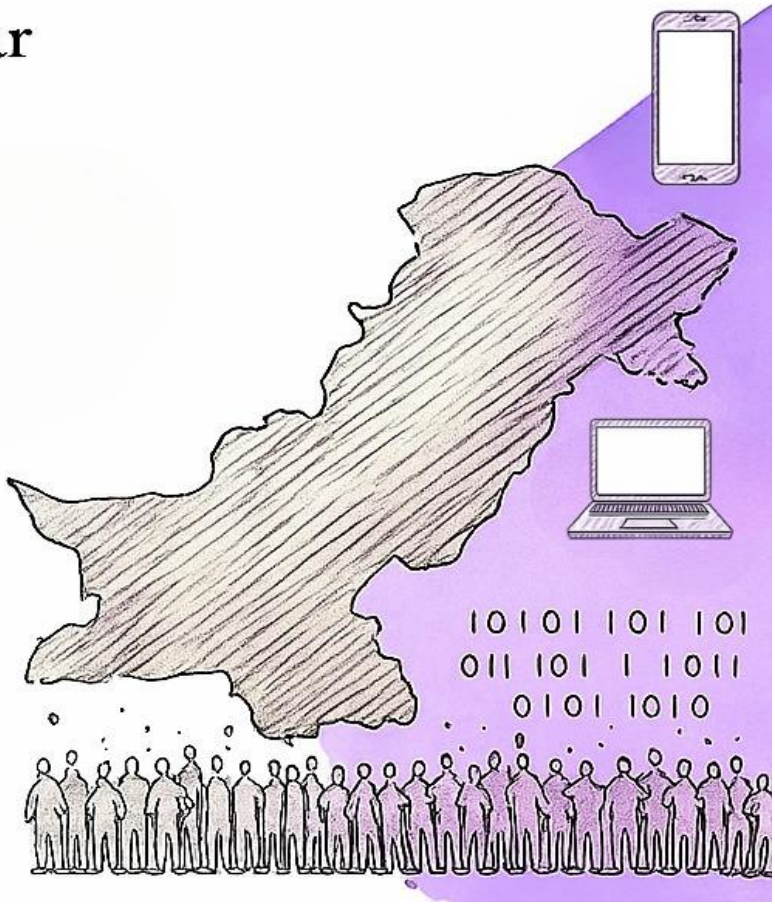




AI and PSYWAR – A Case Study of Pakistan

Muhammad Faizan Fakhar

Senior Research Associate



Working Paper

President
Air Marshal Javaid Ahmed (Retd)

Edited by:
Mashal Shahid

All correspondence pertaining to this publication should be addressed to CASS, Islamabad, through post or email at the following address:

Centre for Aerospace & Security Studies

+92 051 5405011
cass.thinkers@casstt.com
cass.thinkers
cassthinkers
@CassThinkers
Centre for Aerospace & Security Studies

CENTRE for AEROSPACE & SECURITY STUDIES

AI and PSYWAR – A Case Study of Pakistan

Working Paper

Muhammad Faizan Fakhar

Senior Research Associate

TABLE OF CONTENTS

Abstract

Psychological warfare (PSYWAR) has always been an integral part of armed conflicts. However, with advancements in the emerging technologies, particularly artificial intelligence (AI), the scale, scope and precision of PSYWAR have significantly grown. Information and communication technologies (ICT) are one of the key domains where the integration of AI has heralded noticeable shifts. This research paper analyses multiple dimensions of AI-enabled PSYWAR against Pakistan. To present contemporary and latest debates on the subject, this study does not examine the history of PSYWAR but rather discusses the AI-driven propaganda that Pakistan has been facing in recent times. Furthermore, the paper also discusses the response matrix of the Pakistani government to address this challenge. In addition, the study evaluates the adequacy of the responses, identifies related concerns, and examines the potential areas for improvement in the response mechanisms. Lastly, the paper concludes by offering recommendations for dealing with AI-enabled PSYWAR.

Keywords: Artificial Intelligence, Psychological Warfare, Pakistan, Propaganda

Introduction

Propaganda and misinformation are used to create a wedge between the state and its citizens, leading to internal turmoil and chaos within the targeted country. Such a campaign largely falls under the ambit of Psychological Warfare (PSYWAR). Since ancient times, PSYWAR has been a non-violent tool for achieving military goals against adversaries, as the psychological aspect of conflicts is as vital as its physical aspect. However, with advancements in the emerging technologies, particularly artificial intelligence (AI), the scale, scope and precision of psychological warfare have significantly grown. Information and communication technologies (ICT) are one of the key domains where the integration of AI has heralded noticeable shifts. This can be observed by examining the impact of AI on social media platforms. In contemporary societies, these platforms have become a critical tool of communication. Over the years, their role has undergone a rapid shift, from merely enabling social connections and idea-sharing to becoming an integral part of the global information ecosystem. Today, these platforms serve as the primary source of real-time information and news. With the introduction of AI, the ability to proliferate fake news and manipulate content on online platforms has increased at an unprecedented scale. AI-driven bots are now being used to circulate manipulated content on prominent social media sites such as X (former Twitter), Instagram, TikTok, and Facebook.[1] Non-state actors and groups have also been using AI tools to generate fake audio and video content.[2] On the external front, state-sponsored propaganda machinery is also using AI-generated content to malign Pakistan's image.[3]

Therefore, it is essential to examine the concept of AI-driven PSYWAR operations to underscore the forthcoming challenges for Pakistan. This research paper attempts to analyse multiple dimensions of AI-enabled PSYWAR against Pakistan. To present contemporary and latest debates on the subject, this study does not examine the history of PSYWAR but instead discusses the most recent AI-driven propaganda faced by Pakistan. Furthermore, the paper also discusses the response matrix of the state to deal with this challenge. In addition, the study evaluates the adequacy of the responses, identifies related concerns, and examines the potential areas for improvement in the response mechanisms. Lastly, the paper concludes by offering recommendations for dealing with AI-enabled PSYWAR.

---

1 Waleed Sami, "The Perilous Role of Artificial Intelligence and Social Media in Mass Protests," *Modern Diplomacy*, December 07, 2024, https://moderndiplomacy.eu/2024/12/07/the-perilous-role-of-artificial-intelligence-and-social-media-in-mass-protests/.

2 Clarisa Nelu, "Exploitation of Generative AI by Terrorist Groups," *International Centre for Counter-Terrorism*, June 10, 2024, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

3 Foresiet, "AI-Powered Propaganda Network Spreads Pro-India, Anti-Pakistan Content across Social Media," *Foresiet*, September 05, 2024, https://foresiet.com/blog/ai-powered-propaganda-network-spreads-pro-india-anti-pakistan-content-across-social-media.

Literature Review

Proroković and Parezanović (2023) highlight the way in which Psychological Operations (PsyOps) have been transformed into a strong tool of hybrid warfare by AI. The work is theoretically grounded in structural realism as it argues that international system remains anarchic and PsyOps are viewed by states as a tool to further their self-interests. The authors frame AI enabled PsyOps as a threat to the national security of any given state, as they can undermine societal cohesion and cause social unrest. Moreover, the authors also state that since AI is claimed to have its own logic, there is a possibility that AI could independently cause wars in the future by conducting unpredictable PsyOps.[4]

Moreover, Eleonore Pauwels (2024) argues that AI-driven disinformation has become industrialised in the modern world due to the onset of tools that have democratised the dual use of AI. As a result, AI-driven disinformation is no longer a fringe tactic as states and non-state actors can readily deploy AI-enabled propaganda, deepfakes and emotionally charged content. The author also highlights that the precision and personalisation of cognitive attacks are increasingly eroding public trust in societal structures and state institutions.[5]

To counter the rising threats associated with AI-enabled PSYWAR, Feldman, Dant, and Foulds (2024) highlight the urgent need to develop highly adaptable and multi-dimensional response mechanisms. The authors argue that AI-based PSYWAR is carried out through persistent and low visibility influence operations. The authors propose a detection mechanism for such influence operations, which includes provenance detection such as watermarks, use of trained 'guardian AIs' to flag harmful content and cross platform detection.[6]

In this respect, Van Diggelen et al. (2025) offer a unique understanding of how AI is being used to carry out psychological attacks online. The authors frame these attacks as results of man-machine integration where humans and AI work together as a team to influence the targets. The authors term these teams as Advanced Persistent Manipulators (APMs). The authors propose forming similar teams as a countermeasure against these attacks and name them Counter-Advanced Persistent Manipulators (C-APMs). The purpose of C-APMs would be to spot and stop the AI-enabled psychological attacks online. The paper stresses on the need for human control even in C-APMs in order to ensure transparency and user privacy.[7]

---

4 Dušan Proroković and Marko Parezanović, *Artificial Intelligence and Psychological–Propaganda Operations in the Context of Threat to National Security* (Belgrade: Institute of International Politics and Economics; National Security Academy, 2024).

5 Eleonore Pauwels, *Preparing for Next-Generation Information Warfare with Generative AI*, CIGI Paper No. 310 (Waterloo, ON: Centre for International Governance Innovation, December 11, 2024), https://www.cigionline.org/static/documents/Pauwels-Nov2024.pdf.

6 Daniel Feldman, Jesse Dant, and James R. Foulds, *Killer Apps: Low-Speed, Large-Scale AI Weapons*, February 2024, arXiv, https://arxiv.org/abs/2402.01663.

7 Jurriaan van Diggelen et al., "Designing AI-Enabled Countermeasures to Cognitive Warfare," *NATO Science and Technology Organization HFM-377 Symposium Proceedings*, April 14, 2025, https://arxiv.org/abs/2504.11486.

The existing literature offers comprehensive insights on how AI is enabling PSYWAR at scale in the contemporary world. Moreover, useful lessons for developing and deploying countermeasures can also be drawn from the existing literature. However, most of the studies focus on the Western or global context. Limited attention is given in the subject discourse to the unique geopolitical realities and sociopolitical dynamics of countries in South Asia, especially Pakistan. Therefore, this paper aims to fill this gap by investigating how AI is being leveraged to wage a PSYWAR against Pakistan along with an analysis of the aims of these campaigns. Furthermore, this paper examines the impacts of AI-enabled PSYWAR on national security of Pakistan. It critically assesses Pakistan's policy responses to these threats and identifies existing gaps. In addition, the study recommends locally driven counter-strategies to enhance national resilience against AI-enabled PSYWAR threats.

Methodology

This paper employs a qualitative research approach with an interpretive analysis of the collected data. The research is exploratory in nature, as prior research focusing specifically on AI-enabled PSYWAR in Pakistan is limited. Secondary sources, including books, peer-reviewed journal articles, credible newspaper articles, government, think tank, and watchdog reports, and social media content, are accessed and analysed for this study. The epistemological stance of this paper is interpretive in design as it endeavours to not only describe the AI-enabled PSYWAR against Pakistan but also attempts to understand the deeper motivations and impacts of this challenge. Therefore, while this study undertakes a thematic content analysis of the existing literature and the collected data, it also stresses on contextual application of localised countermeasures and strategies most relevant to Pakistan. Sources are selected using the technique of purposive sampling to keep a relevant and contemporary view of the subject matter. Therefore, focus of this study remains on the material published in the last five years.

Defining PSYWAR

PSYWAR has emerged as a vital aspect of military strategy, employing non-combat methods to influence perceptions, behaviours, and decision-making processes. PsyOps include tactics such as media dissemination, deception, and strategic threats to undermine the adversary's resolve, instigate dissent, and accomplish objectives with minimal actual engagement. PSYWAR can be traced back to the ideas of Sun Tzu, but the tools and techniques have consistently evolved depending on the technological advancements and changing geopolitical dynamics. The term PSYWAR was first coined in 1920 by J.F.C. Fuller.[8] It is defined as 'the strategic deployment of disinformation

[8] Sunil Narula, "Psychological Operations (PSYOPs): A Conceptual Overview," *Strategic Analysis 28*, no. 1 (2004): 177-192.

and associated informational tactics by an actor to manipulate the views, feelings, mindset, and behaviour of the adversary.'[9] In the contemporary world, PSYWAR has become an integral part of day-to-day operations conducted by both state and non-state actors to attain their political objectives. The most common ones are mentioned below:[10]

1. Facilitating the subjugation of an adversary's resolve to fight.
2. Maintaining morale and securing the allegiance of supportive factions in targeted states.
3. Shaping the morale and dispositions of individuals in hostile countries.

Artificial Intelligence (AI): A New Source of Fake News

Historically, propaganda operations have depended on organised and concerted efforts by human resource. However, AI is now facilitating the creation of fake content without the requirement of elaborate human resource, resulting in the generation of fake content at an unmatched pace. Therefore, AI has automated the production of fake news, resulting in a proliferation of misinformation around elections, wars, and natural disasters.[11]

AI can be viewed as the interaction between big data and learning algorithms that can mimic real-life activities.[12] In other words, it entails the utilisation of machines and bots to replicate human intelligence. AI has assumed a bigger role in assisting the dissemination of fake news in recent times. The advancement of AI-generated material has resulted in a proliferation of fake news that may readily deceive the audience. The most prominent AI-generated fake content is known as the deepfake. When AI tools generate fake material such as video and audio content, the result is termed a deepfake.[13] It is difficult to identify deepfake content from authentic content without professional tools, making it readily accepted among the masses. As far as detection by software is concerned, it is also challenging due to the rapid advancements in the field of AI. This has raised concerns about the detrimental effects of AI-generated misinformation, including the capacity to subvert political processes and disseminate false information.

---

9 Nesya Rubinstein-Shemer, "Close but No Cigar': Hamas's Psychological Warfare against Israel between 2014 and 2023," *Middle Eastern Studies* 61, no. 1 (2024): 1–17, doi: 10.1080/00263206.2024.2355159.

10 Bela Szunyogh, *Psychological Warfare: An Introduction to Ideological Propaganda and the Technique of Psychological Warfare* (New York: William-Frederick Press, 1955).

11 Pranshu Verma, "The Rise of AI Fake News is Creating a 'Misinformation Superspreader," *Washington Post*, December 13, 2023, https://www.washingtonpost.com/technology/2023/12/17/ai-fake-news-misinformation/.

12 Haleema Zia, "The Evolution of Artificial Intelligence: Implications for Cybersecurity and Hybrid Warfare," *Pakistan Journal of Terrorism Research* 03, no.1 (2021): 59-86.

13 Noémi Bontridder, and Yves Poullet, "The Role of Artificial Intelligence in Disinformation," *Data & Policy* 3, (2021): 1-21, doi: https://doi.org/10.1017/dap.2021.20.

Social Media and AI-Driven PSYWAR

In the contemporary era, social media has emerged as a crucial component of everyday lives. It has become the primary medium through which individuals seek information regarding local and global events. On the other hand, the proliferation of misinformation on social media has become a global concern. With the advent of AI-generated content, its ability to influence the minds of ordinary people worldwide has increased, and Pakistan is no exception. Pakistan is grappling with the issue of widespread proliferation of AI-generated misinformation, resulting in significant societal and political consequences.[14] In case of Pakistan, the country has been subject to PSYWAR from both internal and external actors for decades.[15] However, the rapid rise and deep penetration of social media in the last decade have provided an additional and potent medium for adversary states to launch their disinformation campaigns against Pakistan. The rapid rise of AI has led to the emergence of deepfakes. They have garnered international attention for their capacity to disseminate falsehoods, damage reputations, and even sway public opinion. In Pakistan, deepfake content is now a new security challenge.[16] These deepfakes are being used to generate compromising videos of renowned government officials, resulting in harm to institutions' reputation and public trust, as evident in the case of a senior government official from the country's apex court.[17] Likewise, the adversaries of Pakistan have also used AI-generated fake content to malign the military leadership, which is evident from the artificially generated video of Pakistan's military leaders. [18] The potential of AI-generated fake content to undermine the national security of Pakistan became pronounced during the four-day conflict of Pakistan and India in 2025. During this time, AI AI-generated deepfake video of Inter Services Public Relations (ISPR) Director General (DG) surfaced.[19] In this doctored video, DG ISPR appeared to be admitting losses, and it was widely circulated on different social media platforms.

Social media is a key medium used to conduct PSYWAR because it provides an accessible means to engage with a wide audience. It accommodates both the general people and significant officials with influence and decision-making authority. Social

---

14 Federico Fusco, "Artificial Intelligence and Fake News: Criminal Aspects in Pakistan and Saudi Arabia," *Pakistan Journal of Criminology* 14, no.4, (October-December 2022): 19-33.

15 Rubina Waseem and Muhammad Sajjad, "Conceptualizing New Avenues of the Indo-Pak Hostilities: An Analysis of the Invisible PsyWar Operations and Challenges," *Liberal Arts & Social Sciences International Journal 6*, no.2 (2022): 161-174, doi: https://doi.org/10.47264/idea.lassij/6.2.9.

16 Asif Chaudhry, "Punjab Police File Three Cases under PECA for Deepfake Content," *Dawn News*, February 21, 2025, https://www.dawn.com/news/1893349.

17 Muhammad Binyameen Iqbal, "Fact-check: AI-generated Video of Justice Mansoor Ali Shah goes Viral Online," *Geo News*, October 29, 2024, https://www.geo.tv/latest/571499-fact-check-ai-generated-video-of-justice-mansoor-ali-shah-goes-viral-online.

18 "Fact Check: Video of Army Chief Talking to US Lawmakers is Dubbed," *Dawn News*, April 24, 2025, https://www.dawn.com/news/1904426.

19 Zeeshan Ahmad, "Fact Check: No, DG ISPR did Not Admit Loss of JF-17 Jets," *The Express Tribune*, May 8, 2025, https://tribune.com.pk/story/2544743/fact-check-no-dg-ispr-did-not-admit-loss-of-jf-17-jets.

media facilitates cost-free dissemination and collection of extensive real-time information safely and, at times, anonymously, rendering it an optimal platform for PSYWARS. Social media can serve as a conduit for transferring information from the physical realm to the digital sphere. It also enhances the scope of PSYWAR by offering continuous and direct access to information that reveals various pertinent audiences' viewpoints, thoughts, and communications. Similarly, it can shape and modify beliefs, perceptions, and understandings. Moreover, PSYWAR via social media has significantly decreased the duration required to collect information in contrast to conventional methods. Lastly, posting a picture or a comment on social media requires only a second. With continued technological developments, like 5G, these actions would occur much faster than 4G.

State-Sponsored Actors and AI-Generated Content

Organisations sponsored by adversarial states remain one of the primary actors using online tools and digital space to sabotage the trust between the people of Pakistan and its leadership.[20] In the last five years, the online campaign against Pakistan has become intense, which involves the use of accounts spreading fake AI-generated content against Pakistan and its institutions. In this regard, three key examples are discussed below, reaffirming AI's use to disseminate propaganda against Pakistan.

A 2022 report by Stanford University exposed an organised campaign against Pakistan and its military, which was being run by a X handle that belonged to the Chinar Corps (15 Corps) of the Indian army based in Srinagar.[21] The report argued that the account run by the Indian army accused Pakistan's troops of violating the rudimentary human rights of citizens and harbouring terrorists.[22] Tweets from the official account asserted that Pakistan was unsafe for Hindus, Muslims, as well as women. The report also stated that AI-driven bots were used to maximise the reach of the fake content.

Following this, in 2024, an internet watchdog, renowned for exposing AI-driven sites and accounts spreading propaganda, exposed another campaign run by India against Pakistan.[23] The network included approximately 1,409 social media handles from X and Facebook, which were operating since September 2021.[24] Of the 1,409 accounts, 500 belonged to Facebook, while the remaining 904 were operating on X.[25] This has

---

20 Minahil Shawal Afridi, "India's Strategic Information Warfare: Challenges and Policy Options for Pakistan," *NDU Journal 38*, no.1 (2024): 77-93.

21 Shelby Grossman, Emily Tianshi, David Thiel, and Renée DiResta, "My Heart Belongs to Kashmir: An Analysis of a Pro-Indian Army Covert Influence Operation on Twitter," *Stanford Internet Observatory*, 2022, https://stacks.stanford.edu/file/zs105tw7107/20220921%20India%20takedown.pdf.

22 Ibid.

23 Dimitris Dimitriadis, "News Guard Uncovers Massive India-Aligned Network Using AI and Fake Accounts to Target Country's Foes Operating without Detection for Three Years," *News Guard*, September 04, 2024, https://www.newsguardtech.com/special-reports/india-ai-fake-accounts-network/.

24 Ibid.

25 Shahzad Masood Roomi, "Indian Anti-Pakistan AI-Generated Fake Social Media," *Voice of Khyber Pakhtunkhwa*, September 26, 2024, https://voiceofkp.org/en/indian-anti-pakistan-ai-generated-fake-social-media-propaganda-project/

been one of the largest coordinated efforts against Pakistan since the EU DisinfoLab, which exposed India's long-term efforts to malign Pakistan.[26] Although the direct involvement of India was not independently verified but the content analysis of the network reveals its affiliations.[27] For instance, one Facebook page, JK News Network, consistently disseminated content in support of the Indian Army. This content frequently included glorifying images of military personnel along with pro-Indian Army news and commentary. Moreover, the content of this account was further shared and amplified by other anonymous accounts with similar discourse.

Most recently, in the aftermath of the Pahalgam attack, Indian state-sponsored accounts began to circulate a fake letter on social media platforms.[28] The letter titled, 'Massive surge in resignations amid rising tensions with India', which was allegedly written to inform about the morale of the Pakistan army formations.[29] The letter cited that as of April 26, 2025, approximately 250 officers and around 1,250 enlisted men of the Pakistan army had resigned from their positions due to different reasons such as mental fatigue, illness, and family issues. The fake letter claimed that resigning personnel belonged to the Pakistan Army 10 Corps, 1 Corps, and XII Corps. AI-driven bots were also employed to boost the reach of this fake letter aiming to ensure its widespread dissemination in Pakistan before authorities could lodge official complaints with social media sites. The letter's carefully crafted design and the language suggested that it was AI-generated. In addition, the text and the background color scheme of the letter depicted a glowing reflection and enhanced colors, which affirms that the letter is AI-generated. Media sources in Pakistan debunked this letter, along with another letter, as fake.[30] This is a classic example of how an AI-generated fake letter was fabricated and then disseminated on social media handles as part of India's AI-enabled PSYWAR against Pakistan. The objective was to influence the minds of Pakistani public. This was part of India's broader plan to malign the Pakistan's defences and to negatively influence the perception of the masses in a time of crisis.

Non-State Actors and AI-Generated Content

Easy and cost-effective accessibility of social media has made it the platform of choice for non-state actors in Pakistan to disseminate and publicise their anti-state

---

26 Maheen Shafeeq, "Information Operations and Social Media: Case Study of Indian Chronicles and Options for Pakistan," *NUST Journal of International Peace & Stability 7*, no.2 (2024): 42-52, http://doi.org/10.37540/njips.v7i2.173.

27 Nate Nelson, "Indian Army Propaganda Spread by 1.4K AI-Powered Social Media Accounts," *Dark Reading*, September 05, 2024, https://www.darkreading.com/threat-intelligence/indian-army-propaganda-ai-powered-social-media-accounts.

28 Chandan "Leaked Documents Expose Chaos in Pakistan Army: Over 250 Officers and 1,200 Soldiers Resign Amid Rising Tensions with India," *X*, April 27, 2025, 05:42 P.M., https://x.com/chandan_stp/status/1916473070165885151.

29 Ibid.

30 "Fact Check: Debunking Fake Resignation Letters of Pakistan Army Officers Amid War Tensions," *Pakistan Today,* April 28, 2025, https://pakobserver.net/fact-check-debunking-fake-resignation-letters-of-pakistan-army-officers-amid-war-tensions/.

propaganda.[31] Experts note that terrorist networks have shifted from relying on leaflets, amateur videos, and sporadic internet posts to employing strategies involving AI-generated content, digitally manipulated footage, and falsified documents. These organisations use AI-driven chat programs to craft sophisticated messages that mimic human conversation, generating responses in multiple tones and styles to manipulate audiences. They issue fabricated statements in the names of political leaders, clerics, and community figures, and create convincing deepfake images and videos depicting staged atrocities, rallies, and endorsements from influential personalities.

Terrorist organisations such as Tehreek-e-Taliban Pakistan (TTP) and Baloch Liberation Army (BLA) have proficiently utilised social media networks and video-sharing websites such as YouTube, Facebook, and Twitter to propagate their ideology and attract potential followers.[32] Due to the easily accessible nature of these platforms, there has been a rapid increase in content promoting extremism and hate. The online dissemination has significantly intensified the challenges faced by Pakistan's officials in addressing the rise of violent extremism. The availability of AI-driven tools such as voice cloning software, deepfake generators, and AI-powered video generators—often accessible for nominal fees or as open-source—has empowered extremist groups to create incredibly realistic propaganda on an unprecedented scale.

With the assistance of these tools, terrorist groups operating in Pakistan find it easy to disseminate their propaganda. For example, in 2023, TTP disseminated a deepfake video depicting a key religious leader advocating sectarian violence, which became successful in influencing the masses of Khyber Pakhtunkhwa (KPK) province. Consequently, sectarian clashes broke out before it was deemed as fake by the government authorities.[33] Recent posts on social media indicate that counter-terrorism operations in areas such as KPK have discovered electronic devices carrying AI-driven data-sifting tools, sophisticated chatbots, and editing software capable of generating highly realistic audio and video. Instances of these manipulations are evident in brief videos disseminated through Twitter and Telegram, as well as in declarations and press releases issued in Pashto and Urdu. The primary target of the TTP remains the Pashtun population. TTP is using social media to articulate this goal by portraying the Pakistan's government working on behalf of the US government while failing to implement Shariah in the country.[34]

---

31 Nimra Javed, "Combating Online Violent Extremism through AI: Avenues for Pakistan," *Pakistan Journal of Terrorism Research 05*, no.2 (2023): 1-23.

32 Sameer Patil and Soumya Awasthi, "Pakistan Taliban's Evolving Social Media Propaganda," *Observer Research Foundation*, January 18, 2025, https://www.orfonline.org/expert-speak/pakistan-taliban-s-evolving-social-media-propaganda; Jehanzeb Iqbal, "Decoding Bots of Terrorism in Balochistan," *Margalla Papers 28*, no. 2 (2024): 63-77, doi: https://doi.org/10.54690/margallapapers.28.2.277.

33 Muhammad Irfan, "AI as a Weapon: How Militant Groups in Pakistan Exploit Latest Tools for Recruitment and Extremism," *Khabar Kada*, February 26, 2025, https://khabarkada.com/ai-as-a-weapon-how-militant-groups-in-pakistan-exploit-latest-tools-for-recruitment-and-extremism/.

34 Saad Al Abd, "Social Media as a Threat to National Security: A Case Study of Twitter in Pakistan," *Margalla Papers* 26, no. 2 (2022): 96-107, doi: https://doi.org/10.54690/margallapapers.26.2.117.

Likewise, BLA has enhanced its reach through social media outlets to engage with its target audience.[35] BLA is recognised as a terrorist organisation by the US.[36] Therefore, American-based tech companies generally comply with Pakistani authorities' requests to remove pages and accounts run by BLA on sites such as Facebook and X. Nevertheless, BLA is still operating thousands of fake accounts as it is easy to create new accounts on social media platforms under different names.[37] However, despite this ban on most social media sites, BLA has successfully propagated its narrative via messaging and calling apps such as WhatsApp and Telegram.[38]

For instance, BLA's social media team consistently updates its Twitter and Facebook accounts disseminating fake news, videos, and photographs peddling separatist agenda in Balochistan. It has been relentless in garnering support for the cause among the Baloch diaspora and global sympathisers. The BLA social media team employs hashtags to enhance the visibility of its messaging. As of September 2021, the hashtag #FreeBalochistan accumulated more than 101,000 tweets on Twitter.[39] The hashtag #Balochistan garnered more than 222,000 tweets, while the hashtag #Baloch accumulated over 142,000 tweets.[40] These figures illustrate the reach of the BLA's social media communication and its capacity to engage a substantial audience. The BLA's social media presence has raised concerns among Pakistani officials, prompting them to implement measures to thwart the group's internet propaganda. The Pakistan Telecommunication Authority (PTA) has prohibited access to numerous websites and social media accounts associated with the BLA. Nevertheless, the BLA has maintained its social media presence by constantly making new fake accounts.

Conclusively, groups associated with TTP and BLA have demonstrated their capability to generate online social media content with the assistance of AI. This is a serious challenge for the security agencies of Pakistan and the organisations in the country responsible for countering such propaganda, as AI-generated propaganda can be easily created and disseminated. Besides, the social media platforms coupled with encrypted messaging services such as WhatsApp and Telegram have enhanced the

---

35 Abeera Haider, Saqib Khan Warraich, and Dr. Alishba Mukhtar, "Use of Facebook and Twitter by Terrorist Organizations to Radicalize the Youth: A Case Study of TTP, BLA and ISIS in Pakistan," *Bulletin of Business and Economics 12*, no. 2 (2023): 171-177. https://doi.org/10.5281/zenodo.8348303.

36 "Designation of Balochistan Liberation Army by the US Administration as Specially Designated Global Terrorist (SDGT)," *Ministry of Foreign Affairs*, https://mofa.gov.pk/designation-of-balochistan-liberation-army-by-the-us-administration-as-specially-designated-global-terrorist-sdgt. (accessed April 20, 2025).

37 Jehanzeb Iqbal, "Decoding Bots of Terrorism in Balochistan," *Margalla Papers 28*, no. 2 (2024): 63-77, doi: https://doi.org/10.54690/margallapapers.28.2.277.

38 Sajid Aziz, "Digital Warfare: The Baloch Liberation Army's Tactical Use of Social Media in the Hereof Attack," *Global Network on Extremism and Technology*, November 08, 2024, https://gnet-research.org/2024/11/08/digital-warfare-the-baloch-liberation-armys-tactical-use-of-social-media-in-the-herof-attack/.

39 Abeera Haider, Saqib Khan Warraich, and Dr. Alishba Mukhtar, "Use of Facebook and Twitter by Terrorist Organizations to Radicalize the Youth: A Case Study of TTP, BLA and ISIS in Pakistan," *Bulletin of Business and Economics 12*, no. 2 (2023): 171-177. https://doi.org/10.5281/zenodo.8348303.

40 Ibid.

terrorists' capability to disseminate fake news on a larger scale with just one click. For instance, the simplicity of producing, enhancing, and disseminating propaganda has created unprecedented challenges for counter-terrorism authorities to keep a vigilant eye on the massive flow of disinformation.

Pakistan's Counter Measures

This section evaluates the state's existing legal, technical, and operational responses to the challenge of PSYWAR in general and AI-driven PSYWAR in particular. A thorough examination of these responses is necessary to evaluate their efficacy and identify potential gaps particularly within the framework of Pakistan's primary cybercrime legislation, the Prevention of Electronic Crimes Act (PECA).

Prevention of Electronic Crimes Act (PECA)

The principal legislative framework for countering PSYWAR operations in the digital domain is the 2016 Prevention of Electronic Crimes Act (PECA). The PECA has clauses that criminalise several cybercrimes, including unauthorised access to data systems, spreading of fake news on digital platforms, online stalking, and cyber-terrorism. Section 9 of the act pertains to the act of glorifying an offence, whereas Article 18 addresses offences against the honour of an individual. These clauses may be utilised to prosecute anyone accountable for the development and distribution of AI-generated misinformation if it incites violence or hatred.

The government has recently amended the Prevention of Electronic Crimes Act (PECA) in 2025.[41] The act has now been amended to hold individuals and organisations, operating from within Pakistan accountable for proliferating fake news and misinformation against the state. The amendments in PECA have been made to deter individuals and groups from spreading harmful content through the threat of imprisonment and fines. However, it raises concerns about the removal requests of the content without the inclusion of explicit legal justifications. Moreover, explictit assurance about the autonomy of the Social Media Protection Tribunal is also missing.[42]

PECA's Ethical Concerns

The due process of law is a constitutional assurance that pertains to fair treatment within the standard judicial framework. This pertains to a citizen's right to get notification of an accusation and a hearing before an unbiased court. Pakistan's 1973

41 Kamran Adil, "2025 Amendments to The Prevention of Electronic Crimes Act, 2016: An Introduction," *Research Society of International Law*, February 25, 2025, https://rsilpak.org/2025/2025-amendments-to-the-prevention-of-electronic-crimes-act-2016-an-introduction/.

42 Maham Naweed and Khadija Almus Khanum, "PECA 2025: A Dispassionate Analysis," *Islamabad Policy Research Institute*, https://ipripak.org/wp-content/uploads/2025/02/Final-PECA-2025-1.pdf.

constitution, Article 4, guarantees that every citizen is entitled to legal treatment.[43] Any infringement upon a citizen's rights, irrespective of an individual or government entity, must be substantiated by applicable national legislation. Article 10-A is another crucial clause granting citizens the right to an impartial trial and the due process of law.[44] This provision pertains exclusively to charges of crime.

Concerning PECA, it might be asserted that it violates the country's Constitution's inalienable protections granted to an individual. The law's formulation renders it challenging to ascertain precisely what constitutes criminal activity. For instance, specific terms have been delineated in the definitions section as highly subjective. The term 'act' is defined in the Act as 'a succession of acts,' without more clarification of what constitutes an 'act' under this section. 'Dishonest intention'is described as the intention to inflict injury, obtain wrongful gain, cause unjust damage or suffering to any individual, or incite hatred. This meaning has become highly subjective due to the incorporation of the phrase "to create hatred."

Similarly, Section 10 delineates the definition of cyber-terrorism, a vital term for the objectives of this Act. Nonetheless, this idea has faced criticism for having broad interpretations. Critics assert that cyber-terrorism offences must be explicitly connected to violence and the potential for harm and injury. Section 10 (b) stipulates that the promotion of inter-faith, sectarian, or ethnic hatred is a criterion for cyber-terrorism. Consequently, the wording of the clause sometimes conflates terrorism with acts associated with the promotion of violence or hate. This is an effort to increase control over information access and restrict speech under the pretext of combating fake news. Another concern revolves around the broad and often unambiguous powers granted to under PECA. Notably, Section 37 of the Act, which pertains to the regulation of online content, authorizes authority to block or remove internet content deemed unauthorised, thereby impinging upon the right to freedom of expression. Moreover, PECA has encountered significant criticism for potentially infringing upon the basic rights, particularly the right to freedom of speech as enshrined in Article 19 of Pakistan's Constitution.

Deep Packet Inspection (DPI)

As a substitute approach to address the challenges of online propaganda and PSYWAR, the state of Pakistan had reportedly started to rely on Deep Packet Inspection (DPI). DPI enables the network owner to conduct a deep analysis of the online content and traffic in real time. This technique of filtering and blocking unwanted content was erroneously referred to as *the firewall* in the public discourse.[45] The government argued that the rationale for enforcing a firewall is to control the proliferation of hateful and violent content while also restricting the use of platforms, which are facilitating

[43] Eesha Arshad Khan, "The Prevention of Electronic Crimes Act 2016: An Analysis," *LUMS Law Journal 6*, (2019): 117-126.

[44] Ibid.

[45] Sindhu Abassi, "Pakistan's Firewall: Explained," *Express Tribune*, September 08, 2024, https://tribune.com.pk/story/2494442/pakistans-firewall-explained.

the rapid spread of such content. The previous firewall had the potential to impede internet speed, whereas the new one is significantly more sophisticated.[46] However, the new firewall has a geo-fencing capability, which allows it to track data in real time. Such a firewall regulates and limits traffic that comes in and leaves by establishing geographical constraints. These constraints obstruct access to Facebook, YouTube, and various other websites and applications.

Besides, the firewall also has financial risks attached to it. According to a report, Pakistan lost $1.34bn as a result of the government's decision to ban 'X' last year.[47] 'Pakistan Software Houses Association' warned the government to stop internet blackouts, as for every hour without internet, losses of the information technology (IT) sector account for approximately USD 2.21 million.[48] Moreover, the Pakistan Institute of Development Economics found that cumulative financial losses due to 24-hour internet outages stand at USD 15.6 million.[49]

Pakistan has become a significant participant in the worldwide freelancing industry, with several specialists providing services in diverse areas. Freelancing has offered an alternate career trajectory for some individuals, particularly in a nation where conventional work prospects are constrained. The capacity to serve clients globally, devoid of territorial limitations, has facilitated individuals earning while sitting at home and boosted the economy by bringing international trade currency, US dollar, into the country. State restrictions on digital communication through firewalls has reduced internet speed, which presents a substantial risk to remote workers. They significantly depend on high-speed internet for customer communication, task submission, and project collaboration. Inadequate or inconsistent internet connection can result in missed deadlines, ineffective communication, and, eventually, client attrition.

Furthermore, firewalls frequently obstruct access to prominent freelancing platforms, including Fiverr and Upwork.[50] These platforms are crucial for digital nomads to secure employment, develop portfolios, and process payments. Limited access to these platforms can significantly constrain freelancers' employment choices, compelling them to pursue alternative, frequently less profitable options. The effects on freelancers are both economic and social. The repercussions are catastrophic for numerous freelancers who serve as their families' exclusive providers. The uncertainty generated by these measures may compel competent workers to contemplate

46 Sindhu Abassi, "Pakistan's Firewall: Explained," *Express Tribune*, September 08, 2024, https://tribune.com.pk/story/2494442/pakistans-firewall-explained.

47 Abdul Moiz Malik, "Pakistan tops world in economic losses due to internet shutdowns," *Dawn News*, January 04, 2025, https://www.dawn.com/news/1882972.

48 Kalbe Ali, "IT industry 'loses $1m' due to one hour of net outage," *Dawn News*, December 04, 2024, https://www.dawn.com/news/1876517.

49 Ramsha Jahangir, "Internet: Pakistan's new political battleground," *Aljazeera*, February 22, 2024, https://www.aljazeera.com/opinions/2024/2/22/internet-pakistans-new-political-battleground.

50 Faraz Ahmed, "Firewalls: threat to digital ecosystem," *Express Tribune*, August 26, 2024, https://tribune.com.pk/story/2491018/firewalls-threat-to-digital-ecosystem.

immigrating to countries with more advantageous digital ecosystems, intensifying the prevailing trend of brain drain that has reached a concerning magnitude.

Digital Rights Protection Authority (DRPA)

The newly established regulatory authority was proposed by the government in 2024.[51] Under the new legislative amendment, the Digital Rights Protection Authority (DRPA) will determine the authenticity of news.[52] It will serve as a tool for the government to block platforms promoting content that is illegal as per the new PECA Act.[53] The DRPA possesses the authority to investigate grievances, eliminate content, and uphold digital ethics. The authority will secure compliance from social media corporations, potentially necessitating registration and the appointment of local representatives.[54] DRPA shall possess the authority to eliminate, obstruct, and access indecent or forbidden content online. Furthermore, it has the authority to impose a penalty of imprisonment for a maximum of three years, a fine of up to PKR 2 million, or both on individuals disseminating false information.[55] In addition, DRPA will guarantee the removal of unlawful videos, photos, audio, and texts from online media platforms promptly, and also hold accountable those individuals and groups, propagating disinformation.

Although this body has members from the journalism and legal communities, it functions under the Ministry of Information, which has a history of suppressing content.[56] Therefore, under the PECA framework, there are concerns about the DRPA labelling authentic news as fake if it does not align with a certain narrative. Similarly, firewalls have also raised concerns about access to information and national security. Such systems often rely on foreign firms and services, which carry the risk of exposure and dependency. Consequently, Pakistan's national security could be compromised by the use of unreliable systems. Moreover, these actions undermine Pakistan's digital economy and negatively impact investors' trust in the IT sector.

---

51 Pakistan Today, "PM Shehbaz approves Peca law amendments to regulate social media," https://www.pakistantoday.com.pk/2024/05/09/pm-shehbaz-approves-peca-law-amendments-to-regulate-social-media/. (accessed April 24, 2025)

52 Usman Khan, "Fake news to be punishable with 3-year jail, Rs2m fine or both," *Samaa News,* January 22, 2025, https://www.samaa.tv/2087327755-fake-news-to-be-punishable-with-3-year-jail-rs2m-fine-or-both.

53 "NA approves amendments to PECA law without opposition," *Express Tribune*, January 23, 2025, https://tribune.com.pk/story/2524015/na-approves-amendments-to-peca-law-without-opposition.

54 Irfan Sadozai, "NA passes controversial PECA amendment bill amid walkout by PTI, journalists," *Dawn News*, January 23, 2025, https://www.dawn.com/news/1887195.

55 "President Zardari signs controversial PECA amendment bill," *Express Tribune*, January 29, 2025, https://tribune.com.pk/story/2525281/president-zardari-delays-peca-act-signing-over-journalists-concerns.

56 Shakeel Ahmed, "State of Media in Pakistan," *International Journalists*, September 26, 2022, September 26, 2022, https://internationaljournalists.org/en/state-of-media-in-pakistan/.

Freedom of Speech Concerns

The government of Pakistan has faced challenges in regulating information dissemination and countering the proliferation of misinformation on social media platforms. The proliferation of AI-generated disinformation has intensified these issues, therefore making it difficult for the regulatory agencies to distinguish between authentic news and propaganda. Sometimes, through error and a bad judgment call, an innocent citizen could be punished. In addition, PECA subjects journalists and content creators to potential persecution for an investigative report critical of governmental institutions, a humorous tweet, or an attempt to exposé corruption. Furthermore, empowering authorities to terminate news channels, restricting access to encrypted communications, and penalising whistleblowers under the pretext of curbing 'false information' implies that there is little room left for freedom of speech. PECA restricts little room for a free press, which is the foundation of any democratic society. It is therefore essential to preserve avenues through which individuals can voice dissent and expose governmental corruption to ensure transparency.

To address these concerns, it is essential to introduce safeguards that prevent the misuse of laws like PECA while maintaining national security. One potential remedy is to establish independent oversight mechanisms that are free from political influence, ensuring that decisions about content moderation and intent assessment are transparent, consistent, and accountable. Moreover, instead of solely relying on punitive measures, the state should invest in fostering a more open and informed digital environment. This includes providing platforms for dialogue and debate among the internal populace and political forces, where differing perspectives can be expressed and contested through democratic means rather than being censored. Encouraging such engagement strengthens public trust and creates resilience against AI-driven PSYWAR by promoting critical thinking and inclusivity in national discourse.

Recommendations

In view of the findings pf this study, it is pertinent for Pakistan to adopt a comprehensive and forward looking response to the emerging nexus of AI and PSWAR. Following recommendations are proposed:

Cooperation with Social Media Platforms

Pakistan should seek cooperation from social media platforms for better moderation of online content. Harmful and hateful content based on local languages and local context often gets overlooked by the digital platforms' content moderation policy. This can only be addressed through better collaboration between stakeholders from Pakistan and the social media platforms.

Prevention of Legal Misuse

To prevent the misuse of laws such as PECA, there is a need to establish an independent oversight body. Such a body should be free from any political influence in order to ensure an objective and fair assessment of content and its intent.

Positive Utilisation of Social Media

The government should recognise the positive role played by social media platforms in different capacities; therefore, these platforms must be utilised in a better way instead of blanket bans. The state needs to invest in creating an open and informed digital ecosystem. This would include digital platforms for debate and discussion among the population and political forces of the country, where views are heard and debated in a democratic manner, rather than through censorship.

Institutionalising Narrative Response

Pakistan must develop its national narrative to effectively counter disinformation campaigns. The government should establish a specialised unit under the Ministry of Information, through public-private partnerships, to monitor, assess and counter anti-state narratives in cyberspace.

Adoption of ABC Framework

To tackle online propaganda, disinformation, and misinformation, Camille François, Graphika's chief innovation officer, presented a framework titled 'ABC Framework to Address Disinformation'. This framework focuses on manipulative actors, deceptive behaviours, and harmful content. Pakistan authorities should seek assistance from this model while crafting anti-propaganda strategy.

Social Welfare Programs

Merely disabling accounts or deleting videos might not be enough to deal with the colossal challenge of citizens falling prey to online PSYWAR. There is a need for social welfare programs aimed at job creation and improved education to address the root causes of radicalization.

Conclusion

The evolution and proliferation of social media over the past decade have significantly impacted the socio-political landscape of the world. It has provided a novel arena for the dissemination of psychological operations. With the introduction of AI, the scope and scale of PSYWAR has reached a new level. The paper's findings indicate that AI and social media sites are a perfect duo to wage PSYWAR against any target. Pakistan has been subject to this sort of warfare for many years, both from internal and external actors. However, with the introduction of AI, the generation, dissemination and proliferation of fake content with the intent of conducting PSYWAR against Pakistan

has become much more pronounced. The key objective of such campaigns is to create mistrust between the state of Pakistan and its citizens. Amid this, Pakistan's government has proposed amendments to PECA law. Moreover, there have been reports of employing Deep Packet Inspection (DPI). DPI enables a deep analysis of the online content and traffic in real time to filter and block unwanted content. However, there are certain concerns and reservations which require careful consideration by the government of Pakistan such as the digital privacy of citizens and negative impacts on digital economy. Government should address the online propaganda, however, at the same time, it needs to ensure that citizen's rights are guarded and respected.

ABOUT THE AUTHOR

Muhammad Faizan Fakhar *is a Senior Research Associate at the Centre for Aerospace & Security Studies (CASS), Islamabad. He is a researcher, academic, and content producer specialising in strategic affairs, emerging technologies, and public policy. With Master's in Strategic Studies from the National Defence University and Bachelor's in Electrical Engineering, he brings a multidisciplinary approach to analysing complex issues at the intersection of technology, security, and society.*

ABOUT CASS

The Centre for Aerospace & Security Studies (CASS), Islamabad, was established in 2018 to engage with policymakers and inform the public on issues related to aerospace and security from an independent, non-partisan and future-centric analytical lens. The Centre produces information through evidence-based research to exert national, regional and global impact on issues of airpower, emerging technologies and security.

VISION

To serve as a thought leader in the aerospace and security domains globally, providing thinkers and policymakers with independent, comprehensive and multifaceted insight on aerospace and security issues.

MISSION

To provide independent insight and analysis on aerospace and international security issues, of both an immediate and long-term concern; and to inform the discourse of policymakers, academics, and practitioners through a diverse range of detailed research outputs disseminated through both direct and indirect engagement on a regular basis.

CORE AREAS OF RESEARCH

Aerospace

Emerging Technologies

Security

Strategic Foresight

CASS www.casstt.com
CENTRE FOR AEROSPACE & SECURITY STUDIES, ISLAMABAD
Independence | Analytical Rigour | Foresight

Old Airport Road, Islamabad, Pakistan
+92 051 5405011
cass.thinkers@casstt.com
www.casstt.com
@CassThinkers
Centre for Aerospace & Security Studies
cassthinkers
cass.thinkers