



Vivekananda
International
Foundation

Information Warfare

The Evolving Role of Social Media
Against India's Security Apparatus



VIVEK PURI

VIF BRIEF

**Information Warfare:
The Evolving Role of Social Media
Against India's Security Apparatus**

VIVEK PURI

© Vivekananda International Foundation

Published in 2026 by

Vivekananda International Foundation
3, San Martin Marg | Chanakyapuri | New Delhi - 110021
Tel: 011-24121764 | Fax: 011-66173415

E-mail: info@vifindia.org
Website: www.vifindia.org

Follow us on:
Twitter | [@vifindia](https://twitter.com/vifindia)
Facebook | [/vifindia](https://facebook.com/vifindia)

Disclaimer: The paper is the author's individual scholastic articulation. The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to be correct. Views expressed by the author are personal in nature.

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording or otherwise without the prior permission of the publisher.

Information Warfare: The Evolving Role of Social Media Against India's Security Apparatus

Vivek Puri

Abstract

The digital technology by its very own nature is constantly evolving and thus generating novel challenges for the Indian security agencies to monitor and maintain the safety and security of its citizens as well as to keep a track of current advances made by trans-border state and non-state actors vis-à-vis misinformation and disinformation campaigns as a tool of Information Warfare. Lately, it has been witnessed that, the misuse of social media to spread misinformation and disinformation with a purpose to destabilise the social fabric and security apparatus of India is steadily increasing. Henceforth, in order to dive deep into the perils of information warfare, this article elucidates the misuse of social media to spread fake information and narrative warfare as well as counter measures taken by the government of the day to combat fake narratives. The paper also recommends a way forward to address these evolving national security challenges, which is a prerequisite to maintain the social fabric as well as strengthening the security apparatus of India, that is Bharat.

Introduction

The ground breaking and progressive advent of digital technology has made exceptional evolutions and countless contributions in the present day world, from the task to uplift the humanity via digitally backed Jan Dhan, Adhaar, Mobile connectivity led financial inclusion programme to digitising public services such as; online passport services, CoWIN platform for vaccination during Covid-19, Direct Benefit Transfer of subsidies and weather as well as soil nutrition updates to the agriculturalists in the cities and hinterlands of the country. India has covered a major milestone and has left no stone unturned to establish India's digital footprint across the world in real time through digital platforms such as; Google (search engine) YouTube (video sharing platform) Facebook, X (Formerly twitter), Instagram, WhatsApp and Telegram (social media platforms) in the form of news, diplomatic outreach programmes or messages, showcasing soft power skills, managing stress and conveying safety protocols as well as advisories, audio files, videos, live events, documents and pictures. This advent of digital technology (a double-edged sword) has not only proved to be a productive instrument qualifying for its optimistic usage but has also fetched a wave of internal and external disturbances, grey zone warfare and a weapon of national security threat to maintain the law and order in the respective states, particularly those sharing international borders. The disruptive practice of using digital technologies, particularly social media has activated an alarming state for the government agencies to handle this national security challenge emitting in the form of information warfare (IW).

The Penetration of Social Media in India

In the past decade and a half, the internet has emerged as a last mile connectivity tool to connect people through various mediums. However, social media has emerged as one of the most convenient instruments to connect people even in the hinterlands of the world. As per a report, a substantial increase has been witnessed in the last ten years vis-à-vis Indians using the internet. The data demonstrates that the number of internet users has increased from 250 million in 2014 to approximately 1.02 billion in September 2025¹. Additionally, the penetration of the internet has also made India a base of staggering 491 million social media users², which further means that at least one in every three Indians have now created a social media identity for her/himself.

The driving force underlining this massive increase is the penetration of internet, accessibility of economically viable smartphones and affordable data costs which positions India as the world's second-largest smartphone market, with around 750 million devices in 2025³. The colossal dissemination of internet has proved to be a boon for students, researchers, teachers and institutional functionaries as irrespective of place, distance, language, time and day they now have uninterrupted access to quality education content, continuity in learning practices, authentic information via government portals on programmes and policies as well as broader engagement. However, a survey conducted by ASER (Annual Status of Education Report) in 2024, elucidates that approximately 82.2 percent⁴ of teenagers in the age group of 14 to 16 years are well versed in the use of a smartphone, however, only 57 percent use it for educational purposes, while 76 percent primarily use it to access social media⁵. Going forward, according to the data from

Sensor Tower, a (digital intelligence provider) the average user base of Meta's WhatsApp in India is close to 837 million which includes; Instagram 501 million and Facebook 362 million in 2026⁶. Moreover, the user base of Google's YouTube had 646 million ⁷and X had 15 million⁸ which makes Meta a dominant social media establishment in India.

Understanding Misinformation and Disinformation

The term misinformation refers to inaccurate information or sharing false, misleading and incorrect information unintentionally to deceive others. This inaccurate or misleading information is referred to as actual facts or accurate stories which may include misinterpreted facts, contextually irrelevant content or genuine errors in reporting. For instance; a person named X sharing a picture/video of a partially opened road during monsoon season to her/his traveller friend Y. The message conveyed that the road or path is partially open for traffic. However, person X believes in the authenticity of the picture/video because it has been made viral on the social media and has forwarded it without cross verifying the facts, road, place and location mentioned in the picture/video circulating on the social media which of course is not true. Often people with an intention to help others pass on the information usually believing it to be true but never cross check the validation of the facts which are usually incorrect. Thus, spreading wrong and factually incorrect information unintentionally can cause grave administrative and security issues for the government of the day. On the other hand, the term disinformation refers to spreading of false or misinformation with a purpose to manipulate mindsets, cause damage, to sow seeds of discontent and disharmony, social unrest as well as misguide people,

organizations and countries in the wrong direction. The intention behind this motive is to create law and order disturbance and distort the social fabric of the nation as a whole. As described by the United Nations, “Disinformation can be spread by state or non-state actors. It can affect a broad range of human rights, undermining responses to public policies or amplifying tensions in times of emergency or armed conflict. Disinformation is not only inaccurate, but intends to deceive and is spread in order to do serious harm⁹” The person or group sharing the disinformation is cognizant of the facts and knows that the prime purpose of spreading factually incorrect information is to promote an agenda, create conflicts and to confuse people vis-à-vis empirical reality. It has been witnessed that disinformation campaigns have been used to propagate political campaigns, interfere in elections and scams¹⁰.

The Role of Social Media in Information Warfare

The unparalleled rise of internet access has given social media platforms a voice to express views on subjects that are of utmost importance in the public domain. However, there are certain groups and entities who take advantage of these platforms to spread misinformation and disinformation to distort the social fabric and create hatred among the general population. The spreading of misinformation and disinformation campaigns in the form of fake news through regular social media accounts often result in IW against the state. The people who follow these regular or conventional social media handles/accounts never try to cross check or verify the information received and forward it without even considering the consequences of spreading the news which is fake. IW is conducted through intentional, harmful and manipulative as well as misinformation and disinformation campaigns

via traditional and social media handles/accounts by foreign state and non-state actors with an intention to create misperception, develop social divisions, destabilise societies, create disturbances and ultimately weaken the state as a whole.

IW is a technical strategy deployed through social media platforms to manipulate and influence public opinions, create confusion about programmes and policies of the government of the day, spread disinformation about government and private sector investments, distort political discourses and create discontent among the general population. The weapons used in IW includes; disseminating false or misleading information, disinformation, political propaganda and manipulating social media algorithms to either amplify or overwhelm certain messages or opinions. In the recent past, it has been witnessed that two of India's neighbours i.e. China and Pakistan have persistently used IW against India via social media platforms to amplify their propaganda, the case in point is; a social media platform known as (X) removed almost 23,750 accounts from an organised network with 1,50,000 accounts propagating disinformation in June 2020¹¹ during COVID-19 pandemic. The accounts were propagating false news and spreading geopolitical narratives favourable to the Chinese Communist Party¹². Likewise, other social media platforms, for instance; Facebook, Instagram and YouTube have exposed similar comprehensive coordinated initiatives to propagate misinformation and disinformation campaigns in the form of IW to propagate fake narrative warfare with India. Additionally, India's western neighbour and a close ally of China, Pakistan has consistently made an attempt to fuel anti-India sentiments with an aim to destabilise the nation and Indian information space by pushing propaganda messages,

spreading fake or fabricated information and disinformation via verified social media accounts, YouTube channels and bots. Pakistani propaganda campaigns have oriented towards India-Pakistan military establishments, accusation of mistreatment of the Muslim communities in India and the Kashmir issue. For instance; Pakistan-backed terror groups such as the Kashmir Tigers, the Resistance Front (TRF) and the People's Anti-Fascist Front (PAFF) ¹³as well as global groups like the Popular Front of India and the Islamic State (IS) ¹⁴have used social media accounts to spread their fake propaganda. Here, the case in point is; the TRF, a proxy of Lashkar-e-Taiba, celebrated the attacks in Anantnag (2023) and Ganderbal (2024)¹⁵ through propaganda posts that glorified martyrs and projected the group's power. Similarly, another example is of the PAFF, a proxy of Jaish-e-Mohammed¹⁶, the group during the Poonch attack deliberately disseminated messages and images designed to elicit a reaction from the Indian security forces. These terror groups deploy a calculated, adaptive and tactical strategy to spread misinformation or disinformation through social media in order to garner public sympathy, undermine the credibility of the state and its forces to pursue their strategic objectives.

Misinformation and Disinformation: Instruments of Information Warfare

The evolution of digital technology and particularly social media platforms over the past decade have created a space for spreading misinformation and disinformation campaigns which has outpaced innovation. Unfortunately, in the present times, due to massive news content, the recipient is not able to identify or differentiate if the content S/he is engaging with is genuine or an artificially-propelled narrative,

all they are exposed to is selected content based on similar themes on top of their feeds. In 2024, the UN's Global Risk Report ¹⁷categorised misinformation and disinformation campaigns as the highest and gravest global threat. Furthermore, around 1,100 experts from 136 countries¹⁸ placed it in the category of severe risk. Misinformation and Disinformation campaigns are strategically planned operations by state and non-state actors through social media platforms to create conflict among communities, distort social fabric, disturb economy, manage recruitment for terror operations, manipulate public opinion, post fabricated stories online to disturb law and order and radicalise people for personal and political motives. These campaigns pose a grave national security threat which has the potential to create serious harm particularly when the penetration of internet and social media usage is substantial in countries like India. This is exemplified by; in 2019, a coordinated system being administered by Pakistan's ISPR¹⁹ (Inter-Services Public Relations) was identified as a source of posting derogatory activities against India on social media platforms, another example is from The Washington Post²⁰ which exposed the usage of bots to conduct misinformation operations against the Indian government and appeals for violence by the Khalistani groups²¹. The misinformation campaigns present dangers to our society and democracy as a whole and it targets children and elderly the most as well as the section which is not digitally literate to identify or cross check the incorrect information on the social media accounts.

Misinformation cannot be left unrestricted as it is becoming a weapon with an intention to challenge law enforcement and public order by certain organised groups to promote their propaganda driven vested interests against India. Considering the grave consequences germinating

from misinformation and disinformation campaigns the G20 Leaders Bali Declaration of 2022²² emphasised that the need of the hour is to counter disinformation campaigns as a prerequisite in order to prevent online threats and promote cyber security. According to a survey conducted by the Indian School of Business, it was noticed that social media retains 77.4 percent²³ share and has emerged as the principal source of spreading misinformation as compared to mainstream media which stands at 23 percent²⁴. Going forward, amongst the various social media platforms, X accounting for 61 percent²⁵ is found to be the foremost contributor to spreading false news followed by Facebook constituting 34 percent²⁶. The findings of the survey further underscores that almost 74.89 percent of Indian consumers²⁷ rely primarily on social media for consumption of news via video content which represents a massive 68.21 percent²⁸ share.

The implications of disseminating fake news and fake propaganda declines public confidence in the mainstream media and government institutions. The misinformation and disinformation campaigns have the potential to grossly impact electoral outcomes, people's point of views, political outcomes, economic and cultural aspects of life, beliefs, ideology, social fabric as well as specify issues such as climate change, pandemics, medication etc. Even well-educated people who are aware of these fake narratives are at times deceived by their rapid dissemination. Such manipulative narratives feeds polarisation²⁹ and have the capacity to adversely affect and have grave consequences on the society as well as national security of India. Indeed, misinformation campaigns were listed as one of the global risks by the World Economic Forum in 2024³⁰.

Deepfake Technology

Another challenge to security agencies vis-à-vis misinformation is the emergence of deepfake technology which incorporates deep learning algorithms. A pertinent case in point is Generative Adversarial Networks {GAN}³¹. The GAN is composed of two components, one is the generator and the other is the discriminator. The generator is accountable for generating final recording vis-à-vis video or audio while the purpose of the discriminator is to extract the features containing genuine images of the person concerned from an online source. As the training progresses, the discriminator becomes capable of extracting relevant features of the target person, whereas, the generator learns to generate realistic output. The training process comprises a large collection of images and videos of the target individual which is being used by the encoders and decoders to extract exact facial features which are subsequently used to generate actual pictures. The knowledge acquired by these encoders and decoders facilitate the transfer of facial features, expressions and vocal sound from one individual to another.

The deepfake technology is composed of two principal components; 1. Face Swapping, this technique enables the face of a person (X) to be superimposed onto the body of person (Y). The technology flawlessly replicates the face of individual (X) on the body of individual (Y) making it difficult for the viewers to distinguish whether the actions performed by individual (X) are genuine or fake. 2. Voice Synthesis; in this technique, the speech of the individual (X) can be replicated by capturing voice characteristics such as; modulation, tone and pitch to generate a synthetic voice that closely resembles the voice of (X). These voice notes are then extensively disseminated over social media³² to spread misinformation and disinformation campaigns.

Case Studies

Burhan Wani

Burhan Wani was a 22-year-old social media literate militant and had a substantial following among the Kashmiri youth. From the age of 15 he was turned into a militant and motivated a significant number of Kashmiri youths to join militancy. It was on 8th July in 2016, that he was killed by the Indian security forces during an encounter, following which thousands of people were reportedly gathered for his funeral. Wani created a Twitter handle @Gazi_Burhan2³³ to garner support for the separatist movement through his social media presence by exhibiting photographs of violence and anti-India content. His appeal to join the Jihad via video and (X) twitter messages emphasised his fight against the government of the day. Not only this, he also started a recruitment drive with a remuneration of Rs 35,000³⁴ to enthrall the young and often unemployed population who were hyperactive on the social media thus giving Wani an established audience base. The effective use of social media fuelled Wani's rise to prominence and with digital skills he left no stone unturned to radicalise the Kashmiri youth in large numbers as compared to conventional methods. By 2013, he was described as the poster boy of insurgency in Kashmir by both the national and international media, owing to his dedicated fan following in the Valley and in Pakistan-occupied Kashmir³⁵. Wani attracted significant media attention in 2014 for the pictures he had posted on social media depicting himself and other militants dressed in military uniforms and carrying Kalashnikovs³⁶. The magnitude of online/social media radicalisation was so widespread that, in July 2016, a statement was made by Hansraj Ahir, Minister of State for Home

and he remarked that; “This year, Pakistan strategy has been to try and promote radicalisation through vested groups and social media so that this can be given the shape of a civil resistance³⁷”. This clearly depicts that; a strategy was crafted by Pakistan to radicalise the Indian youth through social media platforms.

Op. SINDOOR

On the intervening night of 6th and 7th May, 2025, the Indian Armed Forces, launched Operation SINDOOR to target terror launch pads and infrastructural camps across the border in Pakistan and Pakistan-occupied Jammu and Kashmir subsequent to the terror attack at Pahalgam in Jammu and Kashmir on 22nd April, 2025³⁸ in which 26 innocent civilians and mostly Hindu tourists³⁹ were assassinated. The moment Operation SINDOOR was launched, security agencies witnessed a massive wave of fake news dispersal in India from numerous sources. The escalation of disinformation on social media was purportedly targeted against India in order to disrupt the security apparatus, for instance; Maj Gen Fazlur's (ret'd) from Bangladesh⁴⁰ disseminated a fake news implying that Bangladesh would attack the northeast region with China's support if India launched a war against Pakistan. However, after corroboration, the Bangladesh Ministry of Foreign Affairs firmly refuted Maj Gen Fazlur's (ret'd) statement. Moreover, according to The Guardian⁴¹, the Pakistani government revoked the ban on X shortly before the conflict broke out which immediately became the root cause of spreading misinformation and disinformation. This is illustrated by; 1. AI-generated material purportedly displaying military success achieved by Pakistan was shared extensively on social media platforms which was then amplified

by its mainstream media, 2. Government ministers made false claims of capturing an Indian pilot, 3. A coup in the Indian army and 4. Pakistani strikes have severely damaged India's defence. Furthermore, a fake news circulated that a cyber-attack by Pakistanis has devastated most of the Indian power grid⁴².

COVID-19

During COVID-19 pandemic, numerous India based YouTube channels⁴³ had published unverified news, for instance; news of false claims of a pan-India lockdown due to COVID-19 was circulating which threatened the migrant workers and fabricated claims alleging threats to certain religious communities in order to create panic, distort the social fabric and public order in India. Additionally, during the same COVID-19 pandemic, China was accused of engaging in a disinformation campaign⁴⁴ to undermine the effectiveness of Made in India vaccines and spreading misinformation about the origin of the virus. China through social media platforms attempted to frame narratives that reshape perceptions of its response to the pandemic and emphasise the efficacy of Chinese vaccines while questioning India's vaccine efforts. China's state-owned media outlets, "Global Times"⁴⁵ have repeatedly carried fake news and ambiguous reports on India's alleged failure to tackle the pandemic effectively. Going further, COVID-19 related fake news which began rising in the third week of March took a massive rise in early April, particularly after the Tablighi Jamaat incident in Delhi. Out of 178 fact checks⁴⁶ conducted since the onset of COVID-19 in the country, as much as 35 percent of them were fake videos, 29 percent images⁴⁷ highlighting fake diagnosis, treatment, incorrect statements as well as false lockdown rules. Going forward,

to counter the fake narrative of misinformation and disinformation campaigns. In his inaugural address to the Non-Aligned Movement (NAM) Prime Minister Narendra Modi highlighted the issue of “terrorism” and “fake news”, by calling them “deadly viruses” when the world is fighting the novel coronavirus. The PM remarked⁴⁸ that; “Even as the world fights COVID-19, some people are busy spreading other deadly viruses. Such as terrorism. Such as fake news, and doctored videos to divide communities and countries,”.

Demonetisation

There was an extensive and widespread panic witnessed owing to circulation of incorrect news claiming that the government of the day had intended to demonetise other denominations as well along with certain other additional banking restrictions. The spread of inappropriate information created confusion and fear among the general population exacerbating the disruptions caused by demonetisation. Going further, the fake news suggested that the government of the day would take hold of individual's valuable gold assets which resulted in panic selling⁴⁹, hoarding and getting people engaged in unintended monetary activities which further strained the already stressed fiscal status of the country. Finally, the competent authority intervened and came forward with explanations and also initiated an awareness campaign to combat the wild spread of misinformation.

Disinformation Campaigns During Elections

Social media has been misused during various polling periods with an aim to propagate disinformation and manipulate public opinion vis-

à-vis elections. One such instance is during the general elections of 2024⁵⁰ in India. Some deepfake videos presenting political figures were circulated to deceive voters and Artificial Intelligence was used to create a fake video of PM Modi⁵¹ dancing as well as false videos of Bollywood celebrities using Hindu extremist⁵² language. Another case in point is; a news article published in The Diplomat highlighted that researchers at the nonprofits Global Witness and Access Now created 48 fake ads⁵³ in English, Hindi and Telugu with false voting information or calls for violence. One claimed India raised its voting age to 21, though it remains 18⁵⁴, while another said women could vote by text message and a third called for the use of force at polling places.

Galwan Clash of 2020

During the Galwan valley and post 2020 clash between India and China, around 400 to 500 fake X accounts⁵⁵ were activated to spread disinformation campaigns. Most of these fake accounts were either of Chinese or Pakistani origin⁵⁶ and were created to spread fake narratives supporting China's opinions and false propaganda. For instance; a video was circulated on YouTube depicting a real fight between Indian army and Chinese PLA soldiers at the site of the Galwan clash and this fake video garnered more than 21,000 views⁵⁷. Additionally, subtitles claimed that this video has been confirmed by the Indian government. However, the Indian government had never claimed any such video. Furthermore, the video was recorded during the day time whereas the 2020 Galwan clash took place at night⁵⁸. The same video was posted in August 2017 and September 2019 and claimed to show combat between the Indian Army and Chinese troops. Similarly, an article was published on 18th June, 2020⁵⁹ on China's Weixin (Chinese name

for the messaging app, WeChat) highlighting why the Indian Army suffered so many casualties against the PLA in Galwan. The article used an image trying to depict as in how many Indian Army personnel had been killed by the PLA in the Galwan Valley clash. By the end of 2020, the article had been read more than 100,000 times⁶⁰, and the same image depicting the apparent death of Indian Army personnel in Galwan, also cropped up on social media in India. However, a reverse image search exhibited that the image was from Nigeria and depicts the aftermath of an incident in 2015 when Boko Haram militants had killed Nigerian soldiers. The image was also used on a Pakistani news website called Baaghitiv⁶¹.

Not only Galwan clash but China's misinformation engineering units had manufactured numerous fake news campaigns against India during India's G20 presidency, Manipur conflict, Buddhism and the Dalai Lama⁶² as well as even spreading lies to gaslight relations between India and Canada. China has also made persistent efforts of spreading false claims about the Manipur conflict and accusing India of running concentration camps for minorities, as well as suggesting, that states in the North-East should secede from India. Going further, Pakistan has also been involved in numerous disinformation campaigns by spreading fake news and divisive content against India, for instance; Channels and websites from Pakistan, such as; the Naya Pakistan Group⁶³ has been posting divisive content on sensitive topics. The websites hold a subscription of over 3.5 million people with 5.5 billion⁶⁴ views with an attempt to spread discontent in Kashmir, the Indian Army and minority communities⁶⁵. Going further, these players also aim to undermine the electoral process in India by highlighting issues such as; the farmers protest and the Citizenship Amendment Act. Kashmir

has witnessed a massive spike in disinformation campaigns especially after the abrogation of Article 370 in 2019⁶⁶. These campaigns involve false claims about resource crunch and administrative issues in the valley post the abrogation of Art. 370. Considering the gravity of this fake narrative, the Ministry of Information and Broadcasting in 2021 had ordered to block twenty YouTube channels and 02 websites for spreading anti-India propaganda and fake news by Pakistan⁶⁷.

Countermeasures Adopted by India

The Government of the day is cognizant and well aware of the nature and level of the threats posed by false narratives, misinformation, disinformation and deepfakes powered by Artificial Intelligence, including synthetic audio, video and text. Such fake content has the potential to impact a person's dignity, reputation and right to privacy as well as further raises concerns about platform accountability. Taking the cognisance of this grave threat to the nation as a whole, the Ministry of Information & Broadcasting on 22nd April, 2022⁶⁸ utilised its emergency powers under the IT Rules, 2021 and issued instructions to block sixteen YouTube based news channels which includes 01 Facebook account⁶⁹ as well. The blocked social media accounts include 06 Pakistan based and ten India based YouTube news channels⁷⁰ with a tentative viewership of around 68 crores⁷¹. These channels were accused of spreading disinformation related to India's national security, foreign relations, communal harmony and public order in the country. The content published by some of the India based YouTube channels referred to a community as terrorists and incited hatred among the members of various religious communities with the potential to create communal disharmony and disrupt public

order. Pakistan based YouTube channels were reportedly used in a coordinated manner to disseminate fabricated narratives vis-à-vis the Indian Army, Jammu and Kashmir and India's foreign relations in the light of the situation in Ukraine. The content disseminated through these channels were found to be false with potential implications for national security, sovereignty and integrity of India and its diplomatic relations with foreign countries. Additionally, none of the digital news publishers had furnished information to the respective Ministry as it is mandatorily required under rule 18 of the IT Rules, 2021⁷². Likewise, in 2024, the Ministry of Electronics and Information Technology (MeitY)⁷³ under Section 69A of the Information Technology Act blocked websites, URLs, WhatsApp accounts, Instagram, Facebook, and YouTube channels related to, linked to or owned by extremists and terrorist groups such as; Kashmir Fights, Resistance Media, TRF and Jhelum Media⁷⁴.

Similarly, during Op. SINDOOR "the government found that massive fake news, misinformation and propaganda campaigns were being run, mostly from outside India". Thus, the Information & Broadcasting Ministry issued directions to block more than 1,400 URLs⁷⁵ for circulating "false, misleading, anti-India, and communally sensitive contents, primarily through Pakistan-based accounts⁷⁶", Moreover, a 24x7 centralised control room⁷⁷ was established to facilitate real-time information dissemination to all media stakeholders. This control room encompassed nodal representatives from the Indian Army, Navy and Air Force along with public officials from Government media units and Press Information Bureau (PIB). The PIB's Fact Check Unit⁷⁸ monitored social media and online news sources in real time to detect fake images, edited videos, misleading narratives and any manipulated

content targeting the operation's objectives, government agencies and security forces. The PIB Unit debunked Pakistani propaganda against India and Indian Armed Forces and fact-checked many posts countering such content. Another case in point is; when The Ministry of Information & Broadcasting under rule 16 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ordered to block Thirty-Five YouTube based news channels and 02 websites⁷⁹ which were involved in spreading anti-India fake news over digital media. The YouTube accounts blocked by the Ministry had a total subscriber base of over 1 crore 20 lakh, and their videos had over 130 crore views⁸⁰. Additionally, 02 (X) Twitter accounts, 02 Instagram accounts, and 01 Facebook account⁸¹ were also blocked by the Government for being involved in spreading coordinated anti-India disinformation over the internet. The Thirty-Five accounts blocked⁸² by the Ministry were operating from Pakistan⁸³ and were part of four coordinated disinformation networks. The accounts include the Apni Duniya Network operating Fourteen YouTube channels, and Talha Films Network operating Thirteen YouTube channels⁸⁴.

All these social media accounts and YouTube channels were operating with a single agenda to disseminate fake narratives via news vis-à-vis sensitive subjects related to India. These YouTube channels were also found posting content to undermine the democratic process with respect to the forthcoming elections in the five states, encourage separatism, create a gulf on the lines of religion and generate animosity among the various sections of the Indian society. The respective information was feared to have the potential to incite riots and disturb public order in the country. The channels used common hashtags and editing styles and some of the YouTube channels were being operated by the anchors

of Pakistani TV news channels⁸⁵. To verify the fake narratives and fake news in circulation and misinformation and disinformation in India. A Fact Check Unit (FCU) which functions under the Press Information Bureau, Ministry of Information and Broadcasting⁸⁶ identifies fake news and misinformation relating to the Central Government. After verifying the authenticity of news from authorised sources, FCU publishes correct information on its social media platforms. Additionally, it encourages citizens to report suspicious content for verification, thereby strengthening public participation in combating misinformation campaigns by both state and non-state actors. FCU has been able to identify various fake news vis-à-vis Government of the day such as; deepfakes, AI-generated and misleading videos, false notifications, deceiving letters and websites. PIB has published almost 2913 factchecks⁸⁷ across its official social media platforms, including X, Facebook, Instagram, Telegram, Threads and WhatsApp Channel so far.

However, despite these evolving challenges and growing discontent, India, that is Bharat, is very well-equipped to tackle IW campaigns. India's multi-layered cyber response ecosystem includes institutional, regulatory, reporting, and public awareness mechanisms to address cybercrimes, user grievances, and unlawful content, including deepfakes, for instance; 1. The Indian Cyber Crime Coordination Centre (I4C) Coordinates ⁸⁸ actions related to cyber-crimes across States. It empowers agencies to issue notices for removal or disabling access to unlawful content including deepfakes under the IT Rules, 2021. 2. Similarly, the SAHYOG Portal (managed by I4C) enables automated, centralized removal notices to intermediaries and all authorised agencies across India use it to request removal of unlawful

content. 3. Citizens can report incidents through the National Cyber Crime Reporting Portal via <https://cybercrime.gov.in> which focuses on cyber-crimes against women and children as well as Deepfakes and financial frauds. 4. The Indian Computer Emergency Response Team (CERT-In) frequently issues guidelines regarding threats related to AI and suggest countermeasures, for instance; in November 2024⁸⁹, CERT-In published an advisory vis-à-vis deepfake threats and measures to stay protected. 5. Lastly, The Ministry of Electronics and Information Technology of India annually observes the Cyber Security Awareness campaigns during October, Safer Internet Day on 2nd Tuesday of February every year⁹⁰, Swachhta Pakhwada from 1st to 15th February of every year and Cyber Jagrookta Diwas on 1st Wednesday of every month with various events and activities for citizens as well as the technical cyber community in India.

India's Challenges

Misinformation and disinformation campaigns are the nutrition for feeding polarised content and eroding the trust of people of India within the institutional framework of the nation. The prime reason that makes India vulnerable is its diverse social, cultural, historical and political fabric vis-à-vis exploitation by terror networks, separatists and extremist groups via social media platforms such as; Facebook, WhatsApp, Telegram, X and YouTube. These platforms are extensively used for spreading propaganda, fake narratives, and false news during Op. SINDOOR to discredit Indian Armed forces and mobilising individuals to distort communal harmony as well as law and order in the country. Another major challenge is digital literacy where people both residing in the metro cities and hinterlands are at times unable

to identify the reason behind spreading fake narratives, false news, AI generated content to malign the image of the country and deep fake videos to promote propaganda to serve their vested interests. Therefore, the misinformation and disinformation campaigns with an agenda to spread incorrect news becomes a challenge for the Indian security agencies who are tasked to counter this narrative warfare as national security threat by incessantly monitoring the social media posts, YouTube channels and X handles to flag detrimental content as and when it is sighted. However, the rapidly evolving and decentralised nature of digital platforms necessitates robust strategies and proactive actions to counter the threats. Considering the gravity of the situation Union Minister for Information and Broadcasting Sh. Ashwini Vaishnaw⁹¹ pointed to the issue of social media and fake news and stated that “fake news poses a threat to India’s democracy and emphasised the need for strict action on social media platforms, misinformation and AI-generated deepfakes⁹²”. He further emphasised that the use of social media has created ecosystems whose actors do not want to comply with the rule book of the nation i.e. the Constitution of India.

Going forward, A thoughtful and deep understanding of how these platforms are exploited by state and non-state actors is extremely crucial to address the challenges and hit the targets. Extremist, separatists and terror groups rely on the susceptibility of spectators to uncorroborated information, disseminating intended propaganda to shape fake narratives and transform public opinions as well as excavate ideological gulfs. The purpose of narrative warfare is to create disrupted law-and-order situation in the country, further hampering the daily life of citizens who unfortunately have less faith in Indian media as compared to foreign media.

Way Forward

As India continues to embrace digital technologies and social media platforms, the need of the hours is to foster a culture of responsible digital citizenship, critical thinking, digital literacy to the last person standing in the last line especially in the hinterlands of the country where digital and internet awareness is limited and ethical online practices needs to be highlighted. Given the massive user base, awareness campaigns shall be organised whether online or onsite by respective stakeholders such as; government institutions, respective agencies, educational institutes, financial institutions, social media influencers, media organisations and civil society as a whole to address key issues such as digital literacy, online safety, data privacy, and the spread of fake narratives. People of this nation shall be sensitised about the dangers and repercussions of information warfare, misinformation and disinformation campaigns being penetrated in India to destabilise the nation and distort the very own population of this country against the ethical institutions which are the foundational pillars of this society. The 1.4 billion people of India, that is Bharat shall maintain the trust in the respective institutions and this will be possible only when the entire population comes together against this fake narrative war we as citizens of India are fighting in the present era. Monitoring the authenticity of the sources and verifying the intention behind the reels, social media campaigns, YouTube videos, fake narratives carrying false messages, thought provoking messages, demeaning armed forces shall be thoroughly read and be able to identify the thought process and the real purpose of spreading such fabricated stories and distorted facts in the public domain. Every citizen of this country shall act and think like an intelligence agent whose foremost duty is to validate

any information received thrice before forwarding or believing in the content shared or uploaded on the social media platforms such as X, Facebook, Instagram, WhatsApp and other messaging services, YouTube channels as well as other such sources which act as a medium to spread information warfare in the country.

Technology giants, employers, social media influencers, financial institutions and security agencies shall leverage the positive power of the internet for progressive and optimistic social, economic, cultural and political awareness as well as development as a grassroots policy in India. The need of the hour is to instil confidence and trust especially in the vulnerable sections of the society residing in the hinterlands and border areas of the nation about the strategic investments and practices of state and non-state actors in creating law and order issues and distorting social fabric of the country by deploying unethical, unwarranted, undesirable and unsolicited information warfare campaigns in a nation whose people are strong enough to fight any battle that targets the social harmony of India. Educating users, promoting responsible online behaviour and implementing effective regulatory frameworks are indispensable steps to harness the potential benefits of the digital ecosystem while mitigating the risks associated with misinformation. Strategy and tactics are required to tackle the menace of misinformation and disinformation owing to their velocity of disseminating information. Defence forces also need to strategise their plan of action to influence people across the border and AI can be deployed to counter narrative warfare as AI will prove to be the turning point in the game in the times to come. Our determined efforts to deny misinformation continue without ever diminishing our constitutional values and fundamental rights to ensure the internet never becomes

a safe haven for those who seek to misuse it for their own personal agenda.

Keywords; Information Warfare, Social Media, Misinformation, Disinformation, National Security

Endnotes

- 1 <https://www.orfonline.org/expert-speak/students-screens-and-human-capital-formation-in-india>.
- 2 <https://indianexpress.com/article/fresh-take/young-edge-doomscroll-de-tox-young-logging-off-virtually-10074679/>.
- 3 <https://www.orfonline.org/expert-speak/students-screens-and-human-capital-formation-in-india>.
- 4 *'Ibid'*.
- 5 *'Ibid'*.
- 6 <https://www.cnbc.com/2026/07/30/india-meta-democracy-protest-boost-instagram-meta.html>.
- 7 *'Ibid'*.
- 8 *'Ibid'*.
- 9 <https://www.un.org/en/countering-disinformation>.
- 10 <https://ischool.syracuse.edu/what-is-misinformation/>.
- 11 <https://www.orfonline.org/expert-speak/indias-two-front-information-war>.
- 12 *'Ibid'*.
- 13 *'Ibid'*.
- 14 *'Ibid'*.
- 15 *'Ibid'*.
- 16 *'Ibid'*.
- 17 <https://un-dco.org/stories/disinformation-global-risk-so-why-are-we-still-treating-it-tech-problem>.
- 18 *'Ibid'*.
- 19 <https://indianexpress.com/article/opinion/columns/it-rules-step-towards-denying-misinformation-space-on-internet-8555000/>.
- 20 *'Ibid'*.

- 21 *'Ibid'*.
- 22 *'Ibid'*.
- 23 <https://procd.isb.edu/media/5phbz2nd/fact-checkingindia-23-01-24.pdf>.
- 24 *'Ibid'*.
- 25 *'Ibid'*.
- 26 *'Ibid'*.
- 27 *'Ibid'*.
- 28 *'Ibid'*.
- 29 [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU\(2021\)653635_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf).
- 30 <https://deakin.libguides.com/misinformation/impact>.
- 31 https://cenjows.in/wp-content/uploads/2025/12/Wg-Cdr-Anand-R-Na-varatna_-Article.pdf.
- 32 *'Ibid'*.
- 33 https://idsa.in/system/files/issuebrief/ib_online-radicalisation.pdf.
- 34 *'Ibid'*.
- 35 *'Ibid'*.
- 36 <https://indianexpress.com/article/india/india-news-india/jk-valley-on-boil-after-face-of-new-militancy-burhan-wani-is-shot-dead-hizbul-muja-hideen-2902395/>.
- 37 <https://www.ndtv.com/india-news/pak-promoting-radicalisation-in-india-via-social-media-rajya-sabha-told-1434041>.
- 38 <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2128747®=3&lang=2>.
- 39 *'Ibid'*.
- 40 https://cenjows.in/wp-content/uploads/2025/12/Chander-Sekhar_-IB.pdf.

- 41 <https://www.theguardian.com/media/2025/may/28/how-social-media-lies-fuelled-a-rush-to-war-between-india-and-pakistan>.
- 42 *'Ibid'*.
- 43 <https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1819892®=48&lang=2>.
- 44 <https://www.orfonline.org/expert-speak/indias-two-front-information-war>.
- 45 *'Ibid'*.
- 46 <https://www.orfonline.org/expert-speak/how-fake-news-complicating-india-war-against-covid19-66052>.
- 47 *'Ibid'*.
- 48 <https://indianexpress.com/article/india/pm-modi-at-nam-summit-terrorism-fake-news-deadly-viruses-6394202/>.
- 49 <https://procd.isb.edu/media/5phbz2nd/fact-checkingindia-23-01-24.pdf>.
- 50 https://www.orfonline.org/research/extremist-propaganda-on-social-media-impact-challenges-and-countermeasures#_edn2.
- 51 *'Ibid'*.
- 52 *'Ibid'*.
- 53 <https://thediplomat.com/2024/05/as-india-votes-misinformation-surges-on-social-media/>.
- 54 *'Ibid'*.
- 55 https://cenjows.in/wp-content/uploads/2025/12/Dr_Sriparna_Pathak_Web_Article_April_2025_CENJOWS.pdf.
- 56 *'Ibid'*.
- 57 *'Ibid'*.
- 58 *'Ibid'*.
- 59 *'Ibid'*.
- 60 *'Ibid'*.

61 *'Ibid'.*

62 https://cenjows.in/wp-content/uploads/2025/12/Maj-Vishnu-RJ_-Article.pdf.

63 *'Ibid'.*

64 *'Ibid'.*

65 *'Ibid'.*

66 *'Ibid'.*

67 *'Ibid'.*

68 <https://www.pib.gov.in/Pressreleashare.aspx?PRID=1819892®=48&clang=2>.

69 *'Ibid'.*

70 *'Ibid'.*

71 *'Ibid'.*

72 *'Ibid'.*

73 https://www.orfonline.org/research/extremist-propaganda-on-social-media-impact-challenges-and-countermeasures#_edn2.

74 *'Ibid'.*

75 <https://www.thehindu.com/news/national/blocked-1400-anti-india-urls-during-operation-sindoor-says-governement/article69874844.ece>.

76 *'Ibid'.*

77 *'Ibid'.*

78 *'Ibid'.*

79 <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1791547®=48&clang=2>.

80 *'Ibid'.*

81 *'Ibid'.*

82 *'Ibid'.*

83 *'Ibid'.*

84 *'Ibid'.*

85 *'Ibid'.*

86 https://sansad.in/getFile/loksabhaquestions/annex/187/AU6139_TmP-mGG.pdf?source=pqals.

87 *'Ibid'.*

88 <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268®=48&lang=2>.

89 *'Ibid'.*

90 *'Ibid'.*

91 <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198117®=3&lang=1>.

92 *'Ibid'.*

About the Author

Vivek Puri is an independent research analyst and educator based in India. He holds a master's degree in International Relations and Strategic Studies and another degree in Public Administration. His areas of interest focus on India's evolving strategic partnerships, national security and diplomatic engagements across the **Indian Ocean Region and Africa**.

Email: vivekp0108@gmail.com

I Vivek Puri (author) certifies that: -

The article is original in content, unpublished elsewhere and it has not been submitted for publication/web upload elsewhere.

Facts and figures quoted in the article are duly referenced, as needed, and are believed to be correct.

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.



VIVEKANANDA INTERNATIONAL FOUNDATION

3, San Martin Marg, Chanakyapuri, New Delhi – 110021

Phone: +91-11-24121764, 24106698

Email: info@vifindia.org,

Website: <https://www.vifindia.org>

Follow us on [twitter@vifindia](https://twitter.com/vifindia)