Information Operations and Social Media: Case Study of Indian Chronicles and Options for Pakistan

Maheen Shafeeq

Abstract
In the era of digital media, states have resorted to social media to pursue several agendas. In this regard, this paper sheds light on the evolving strategies of intelligence, surveillance and Information Operations (IO) conducted through social media sites. The paper examines various strategies of IO mentioned in U.S. military documents encompassing Military Deception (MILDEC), Computer Network Operations (CNO), Operations Security (OPSSEC), and Psychological Operations (PsyOps). The paper specifically evaluated the role of social media in PsyOps and coined the term Social Media PsyOps (SMPsyOps). It analyses how the Indian government employed these tactics to conduct IO against Pakistan unveiled in the Indian Chronicles by EU DisinfoLab. The paper argues that social media has become an open source of intelligence for conducting of IO by India and influencing opinions and perceptions of Pakistan in Western capitals. This has impacted Pakistan and therefore the paper recommends measures for the government of Pakistan on how to counter the growing Indian network of IO.

Keywords
Social Media, Information Operations, Psychological Operations, Intelligence, Surveillance, Indian Chronicles

Introduction
The advent of social media at the turn of the 21st century has revolutionized the conduct of communication in a way that the world has not witnessed before. Social media sites such as X (Twitter), Facebook, Instagram, TikTok and so on have unique features that have multiplied people’s ability to share and consume information and data in the form of videos, pictures and short statements. These social media sites hold significant...
relevance when it comes to connectivity with the masses and the presence of abundant data and information, making it an ideal ground for Information Operations (IO). Militaries and governments around the world are now depending on social media to carry out open-source surveillance and intelligence gathering for IO against adversaries (Fortin et al., 2021).

The Department of Defence characterizes Information Operations (IO) in Joint Publication 3-13 as “the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of potential adversaries while protecting our own” (Department of Defense, 2014, p. ix). The definition of IO identifies that any resourceful and actionable information gathered (during military operations) can be utilised in multiple ways against the adversary to gain or maintain a competitive edge (European Union Agency for Cybersecurity, 2020). Information has remained a key component during information operations in the past. Before the extensive use of digital technologies, this information was gathered through physical intelligence networks (Otis, 1991); however, since the advent of social media, the abundance of real-time information has become a component of IO due to the following reasons:

- Social media allows a readily available tool to reach the masses. It not only hosts the general public but also important officials holding positions of influence and decision-making powers (Ekwunife, 2020).

- Social media also allows cost-free sharing and gathering of exponential real-time information securely and at times anonymously, making it an ideal ground for IO (Shallcross, 2017). Social media can also act as an extended hand of transiting information from the physical world to the online world.

- Social media also complements IO by providing uninterrupted and direct access to information that discloses the perspectives, thoughts, and communications of a wide range of relevant audiences (Theohary, 2015). Likewise, social media can also be used to influence and alter beliefs, perceptions and understandings.

- IO through social media has reduced the time it would take to gather information as compared to traditional means. It only takes a second to upload a picture or post a comment on social media (Gery et al., 2017). With further advancements in technology such as 5G, these actions would become ten to a hundred times faster than 4G (Thales, 2022).

Due to the above-mentioned features of social media, it presents a fertile ground for hostile forces to conduct IO. This paper analyses the correlation of IO and social media and investigates the case study of Indian Chronicles to analyze the scope of IO conducted by the Indian government. It studies how various types of IO were employed by the Indian government to develop and run fake UN and EU-accredited organizations and how IO was amplified by the help of social media. Indian government for the past 15 years conducted IO primarily to influence and mold decision-making at the international level against Pakistan. From a security perspective, it is becoming essential for strategists and policymakers to study the influence of social media and its implications for the security of the state. In the end, the paper provides recommendations for the Government of Pakistan to address the growing sophisticated Indian IO campaigns to malign Pakistan.
Research Methodology
This paper employs qualitative research tools by analyzing unclassified U.S. military documents and reports on or related to Information Operations, Psychological Operations and Military Deception. Other secondary data sources of data include research articles, international and national reports by think tanks, media analysis and foreign office statements to understand the phenomenon of information operations and its relevance to social media.

The paper attempts to dissect information operations and its various types. It highlights how these information operations are increasing depending on social media and why this is the case. The paper specifically coins Social Media Psychological Operations (SMPsyOps) and underscores a growing trend of Social Media propaganda, misinformation and disinformation. It also analyses how disinformation campaigns can pose a significant risk to national security in Pakistan’s context and what is the associated consequences of disinformation campaigns in instigating internal instability and turmoil. The paper, at the end, looks into possible options available to Pakistan to counter such large-scale IO campaigns in future and what possible lessons can Pakistan derive from the launch of such campaigns.

The primary objective is to inform the readers about information operations and their associated concepts and their consequences. The second key objective of this research is to assess the role of such IO campaigns including social media psychological operations, in shaping perceptions and influencing decision-making processes in Pakistan. The third objective is to bring the impact of such IO campaigns into the eyes of government and security officials and magnify the need for a comprehensive security framework to counter Indian acts.

Pillars of Information Operations
The U.S. military has conducted significant research and analysis into IO. In the joint publication 3-13 by Department of Defense (DoD), IO comprises of four pillars (Theohary, 2021): that include:

- Military deception (MILDEC)
- Computer network operations (CNO)
- Operations security (OPSEC)
- Psychological Operations (PsyOps)

The following points highlight the correlation of IO and social media:

- Military deception (MILDEC) employs social media sites to gain an advantage over adversaries and/or their leaders by misleading, misguiding and/or diverting them into taking detrimental and consequential actions and decisions for a favorable conclusion. (Department of Defense, 2017).
- Computer network operations (CNO) are cyberspace operations conducted through interdependent networks of information technology infrastructures and the data available on them. These independent networks also include social media and use of data available on these social media sites. (Paul & Porche, 2017).
- Operations security (OPSEC) engages social media in a disconnected manner so that it identifies and protects pieces of data that could be clubbed together to develop a bigger picture (Department of Army Headquarters, 2018).
- Psychological operations (PsyOps) use social media to convey selected information to target the adversary’s value system, beliefs, emotions,
reasoning or behavior (Department of Army Headquarters, 2018; McKew, 2019).

While MILDEC, CNO, OPSEC play a vital role in misleading, collecting and protecting information on social media, PsyOps is the most critical of IO as it has the additional capacity to sway the opinions and actions of individuals, governments and groups. As PsyOps reflects a broader range and scope of IO activities to develop a desirable condition and environment, it needs particular attention in the age of social media. The relation between social media and PsyOps is further elaborated below.

**Social Media Psychological Operations (SMPsyOps)**

Psychological Operations (PsyOps) are utilized in both peace and wartime activities (Mabima, 2018). This concept is not new; rather, it is as old as the history of mankind and war itself (Chin, 2019). During Operation Desert Storm and the Vietnam War, printed newspapers, pamphlets, and radio broadcasts were the primary tools of PsyOps used to influence the opinions and emotions of people (Goldstein & Findley, 1996). However, in the digital age, social media platforms have vastly increased the scope and capacity of PsyOps compared to these physical means (Mabima, 2018).

According to the DoD, the aim of PsyOps is to conduct planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals (Cowan & Cook, 2018). This definition underscores that the primary objective of PsyOps is to persuade the minds of its target audience (Omand et al., 2012). Today, social media provides an ideal platform for such operations, as the minds that need to be persuaded are readily accessible (Farka & Neumayer, 2020).

Thus, this research introduces the concept of Social Media Psychological Operations (SMPsyOps). The unique features of social media platforms make them an ideal environment for conducting SMPsyOps. SMPsyOps is supported by numerous research and analysis conducted on the correlation of social media and PsyOps. Recently, Pakistan has banned the social media platform X (Twitter) owing to intelligence reports (Pakistan Observer, 2024). Similarly, a recent report by researchers at the Stanford Internet Observatory examined 150 removed bot accounts on X (formerly Twitter) and Meta. These accounts employed deceptive tactics to promote pro-Western narratives in the Middle East and Central Asia (Stanford Internet Observatory, 2022). Although the researchers did not attribute these online accounts to any specific entity, officials connected to the case believed they could be linked to the U.S. military (Nakashima, 2022).

SMPsyOps for the purpose of promoting a desired narrative has become a routine practice in the age of social media in order to influence and malign adversarial states. This demonstrates the growing relevance of social media for states and civilian and military leaderships as they are increasingly relying on social media to alter opinions and behaviors of people (Mlot, 2013). In addition to the US, Israeli, Russian and British, armed forces have developed a special bridge that particularly focuses on PsyOps and social media in an attempt to ‘master a new kind of warfare’ (Flint, 2016, para 3). This indicates that social media and PsyOps are integral components of contemporary intelligence and military strategies. The interplay of IO and PsyOps on social media has emerged as an imperative tool to harm the adversary’s national security and wage irregular, asymmetric and hybrid warfare (Mabima, 2018). Such type
of warfare is also quoted as a feature of hybrid warfare, non-contact warfare, 5th generation warfare and so on and is believed to be carried out through proper strategies. SMPsyOps is further promoted by carrying out strategically designed social media campaigns. These strategically designed social media campaigns use the following methods to obtain their objectives.

- **Propaganda**: Social media campaigns are used as a tool to propagate an idea or narrative in the minds of its intended targets (Farka & Neumayer, 2020). The propaganda on social media can use truthful information, however, in a manner that is misleading and may include stolen information (Department of Defense, 2014).

- **Misinformation**: The sharing of false information or fake news on social media unintentionally without counter-checking the information. Such false information is believed to be true by the intended target under the influence of peers (Acemoğlu et al., 2021).

- **Disinformation**: Unlike misinformation, disinformation has the intentional purpose of spreading false information (Department of Defense, 2014).

Through propaganda, misinformation, and disinformation, social media becomes the echo chamber for SMPsyOps. The propagation of these tactics is facilitated by manipulating algorithms using bots in addition to real accounts (Fournier, 2021). An investigation by the BBC revealed that this manipulation involves fake and bot accounts that can create and boost trends within a few hours. Furthermore, the investigation reported that companies offer trending services through bot accounts for approximately USD $200 (Abdulrahman, & Subedar, 2018).

This clarifies that Information Operations (IO) employ Military Deception (MILDEC), Computer Network Operations (CNO), Security Operations (SECOPS), Psychological Operations (PsyOps), and Social Media Psychological Operations (SMPsyOps). These operations utilize information available on social media or use social media to disseminate and amplify desired information and messages to a target audience. They are carried out against adversaries to intentionally damage their reputation among certain audiences. This was clearly demonstrated in the EU DisinfoLab's report "Indian Chronicles," which exposed a highly sophisticated disinformation campaign by the Indian government targeting decision-makers primarily in Brussels and Geneva.

**Case Study of Indian Chronicles**
The Indian government and its security establishment have remained fixated on humiliating, degrading, and maligning Pakistan since the partition of the subcontinent in 1947. India has frequently engaged in Information Operations (IO) through various political and diplomatic activities. These IOs not only threaten Pakistan's national security but also create obstacles for Pakistan in achieving its foreign policy objectives.

One example of such an IO, aimed at promoting an anti-Pakistan narrative in Western countries, was revealed in the report "Indian Chronicles" by EU DisinfoLab. This report exposed a network of over 750 fake news sites and more than 550 domain names spanning 119 countries (Alaphilippe et al., 2020). This network included over 10 resurrected NGOs accredited by the United Nations Human Rights Council (UNHRC) to reinforce anti-Pakistan propaganda, misinformation, and disinformation. The task of amplifying fake news and propaganda was carried out by Asian News International, a leading news agency in India (Javed, 2021).
The entire information operation (IO) was evidently characterized by misleading depictions, with covert support from the state. Conducting such an operation for 15 years would have been impossible without the resources and perseverance afforded by state backing. While Pakistan has frequently pointed out instances of such IO by India, it was first exposed in 2019 by an EU DisinfoLab report titled "Indian Chronicles" (Alaphilippe et al., 2020). This report uncovered a network of UN-accredited NGOs working in coordination to promote Indian interests while repeatedly criticizing Pakistan. Within the Indian Chronicles case study, various tactics of IO could be identified. Military Deception (MILDEC) was employed, as misleading information was disseminated to international decision-making bodies such as the UN and EU, as well as to the audience on social media platforms. The Indian government effectively circulated images and videos depicting fake lobbying, staged demonstrations, and fabricated speeches during press conferences and UN side events, orchestrated by fictitious or hijacked NGOs and their members. The report highlighted three informal groups in the European Parliament, namely the "South Asia Peace Forum," the "Baloch Forum," and "Friends of Gilgit-Baltistan," which actively shared these activities online and staged events in front of the European Parliament to propagate pro-India and anti-Pakistani narratives among the members of Parliament. The impact of these deceptive activities was amplified through repeated posting and sharing on social media platforms, ultimately misleading the target audience away from reality.

Furthermore, Computer Network Operations (CNO) utilized a network comprising over 750 fake media outlets, 550 fake news websites, and associated social media accounts to disseminate misinformation and disinformation among decision-makers within the UN and EU. Particularly, Twitter (now X) was observed to trend anti-Pakistan content through the use of bot accounts, influencing a wide audience (Kausar et al., 2021). These online platforms served as honeypots, enticing members of Parliament to engage with and propagate anti-Pakistan content on social media.

Elements of Operations Security (OPSEC) are also apparent. In addition to the tactics outlined in Indian Chronicles, the Indian government employed other strategies to discredit Pakistan. For instance, the Financial Action Task Force (FATF) and allegations of cross-border terrorism were leveraged to tarnish Pakistan's reputation by disseminating false information linking Pakistan to terrorist funding (Khan, 2021). Moreover, the Balochistan separatist movement was instigated using similar platforms (Khetran, 2017), alongside other incidents. These disparate operations were simultaneously promoted on social media through Indian platforms to achieve a broader objective: influencing and reshaping perceptions of Pakistan in Geneva, Brussels, and other Western capitals.

Psychological Operations (PsyOps) overshadowed these operations as the most crucial factor. As highlighted in the Indian Chronicles report, the primary objective was to propagate an anti-Pakistan narrative in Western capitals by circulating fabricated images and posters depicting violence and atrocities committed by Pakistan against its nationals. These staged protests were then disseminated via social media channels associated with fictitious news agencies to assess the impact of this psychologically manipulative content.

Additionally, Social Media Psychological Operations (SMPsyOps) were employed by the Indian government to effectively propagate their anti-Pakistan narrative to Western leaders and the general populace, aiming to influence and manipulate their perceptions. The intention, as revealed in the Indian Chronicles, was to systematically alter international perceptions of Pakistan, ensuring that it is
consistently viewed in a negative light. These SMPsyOps, documented by researchers (Hafeez, 2021; Rehman, 2021), were executed with the explicit aim of tarnishing Pakistan's international standing.

This demonstrates that a detailed and thoroughly planned IO, carried out by the Indian government, was unveiled in the Indian Chronicles. These IO continued under the nose of Western capitals and on social media due to their anonymity and lack of direct association to the Indian government. The JP 13-3 document stated that the anonymity of cyberspace allows ideal ground for covert information operations, due to which they can be carried out without association (Department of Defense, 2014). If government-sponsored covert IO are exposed, the government would usually deny it.

A similar scenario was witnessed in the case of Indian Chronicles, as the Indian Ministry of External Affairs (MEA) denied the claims made by the EU DisinfoLab report and the MEA spokesperson Anurag Srivastava said that India does not practice disinformation campaigns as it is a responsible democracy (Mohan, 2020, para 2). On this denial, Pakistan reiterated the involvement of the Indian government in such dubious campaigns. Pakistan’s Foreign Minister Shah Mehmood Qureshi, on the issue, stressed on the notion that Indian-funded network is manipulating the international system for its nefarious designs (Reuters, 2020). This highlights the urgent need to address the fast-spreading trend of fake social media campaigns to malign and discredit states. In this regard Pakistan must take firm and proactive measures to counter this trend.

**Countering Information Operations on Social Media**

There’s no denying that Pakistan has greatly benefited from social media in terms of connectivity and communication, facilitating strong ties with the global community. However, Pakistan has faltered in constructing a robust counter-narrative against harmful content on social media platforms. Despite urging social media companies to establish local offices for better communication and coordination, Pakistan's influence overregulating these platforms remains limited due to resistance from these companies.

In contrast, India wields significant influence over social media platforms, giving it an advantage in shaping perceptions and narratives. India has effectively propagated pro-Indian and anti-Pakistani narratives in Western capitals, including the United States, diverting attention from its own nefarious activities. Despite the revelations in the EU DisinfoLab report, Pakistan has yet to take concrete steps to identify, address, and counter such malicious agendas.

Effectively countering IO through social media demands a well-conceived and executed strategy involving multiple ministries working in coordination. Unfortunately, the absence of a national-level social media strategy and its implementation remains Pakistan's weakest link, leaving it vulnerable to exploitation by adversaries. To mitigate this vulnerability and counter militarization effectively, Pakistan's decision-makers must prioritize enhancing the security of its weakest link through the following measures:

**Diplomatic Efforts**

Pakistan must prioritize addressing Indian Information Operations (IO) and disinformation campaigns, such as the Indian Chronicles, in its discussions with Indian counterparts. It should aim to tackle the issue at its root by engaging with the Indian government and related factions, urging them to take action to alienate and cease such IO campaigns, particularly on social media. Pakistan should also reach out to
governments and international institutions mentioned in the Indian Chronicles, urging joint investigation into the staged activities in their respective cities and meetings. The Pakistani foreign minister should ensure that the topic of Indian IOs and strategies for dealing with them remains on the agenda during diplomatic meetings.

Cooperation with Social Media Companies
The Pakistani government should formally request social media companies to conduct thorough reviews of the authenticity of staged anti-Pakistan protests, especially in Western capitals, and seek their cooperation in removing such content from their platforms. Pakistan should actively engage with social media platforms to address the increasing prevalence of Indian IO campaigns on their sites.

Treating Social Media and Digital Media as Components of National Power
Recognizing the significance of social media and digital media in terms of IO, the Pakistani government should integrate these domains as elements of national power. Pakistan should convene relevant stakeholders from both the public and private sectors to assess and analyze social media and IO trends, with the aim of formulating policies to counter Indian IO campaigns and highlight their weaknesses.

Understanding ABCD of Disinformation
To tackle online propaganda, disinformation, and misinformation, Camille François, Graphika’s chief innovation officer, presented a framework titled as “ABC Framework to Address Disinformation”. The framework presents a three-tier framework to identify manipulative actors, deceptive behaviors, and harmful content (François, 2019).

Adding another element of D that deals with information distribution can make this framework an effective tool for government agencies and industry to tailor their security approaches by covering these four key vectors (Alaphilippe, 2020).

Nullifying Misinformation and Propaganda Through Social Media
To prevent falsehoods from gaining traction and evolving into perceived truths, it's essential to counter misinformation and propaganda, especially on social media (Trottier, 2015). Establishing a dedicated unit within Pakistan's Ministry of Foreign Affairs to identify and combat anti-Pakistan misinformation and propaganda online is crucial. This specialized team would actively monitor online platforms, promptly respond to false claims, and provide accurate information to debunk misinformation.

Recognizing the influential role of social media as a force multiplier, Pakistan should initiate comprehensive efforts to harness these platforms as tools for empowerment. Instead of merely observing social media dynamics, both government officials and the public should be encouraged to engage proactively. By maintaining an active online presence and communication channels, Pakistan can not only debunk false narratives but also foster confidence and trust, particularly during instances of anti-Pakistan trends online. This proactive approach can effectively neutralize the spread of misinformation and reinforce Pakistan's narrative on various issues.

Building Counter Narrative
Pakistan should craft its own national narrative to effectively combat disinformation campaigns by India. Regular impact assessments of current information practices are crucial for policymakers to grasp the evolving landscape of misinformation. Pakistan should establish a dedicated department, through public-private partnerships, to conduct frequent assessments of anti-Pakistan events and narratives online. The primary objective of this effort would be to construct a robust counter-narrative.
In cases where Indian Information Operations (IO) target specific segments of Pakistani society, it's vital for Pakistan to ensure that strong rebuttals originate from those particular segments. This approach would not only highlight Pakistan's authentic narrative but also effectively counter misinformation, disinformation, and IO orchestrated by India. By proactively addressing targeted campaigns with tailored responses, Pakistan can reinforce its narrative and mitigate the impact of false information spread by adversaries.

**Shared Database of Digital and Physical Fingerprints of Indian IO**

The exploitation of social media by India has escalated into a global concern, impacting institutions such as the UN and EU. Therefore, a collaborative effort to establish a shared database encompassing NGOs, news outlets, domain names, and social media presence is imperative. This initiative would enable targeted UN and EU members to recognize and thwart future misinformation campaigns by India. Additionally, it would safeguard the digital realms of the UN and EU, minimizing susceptibility to Information Operations (IO), particularly Psychological Operations (PsyOps).

By implementing the aforementioned recommendations, the government and state institutions can significantly bolster their capacity for managing social media against Indian IO. This proactive approach not only combats IO on social media but also erects a robust defense against such activities. Moreover, it facilitates secure engagement between the government, state institutions, and the public. Furthermore, it educates Western capitals to discern and resist India's anti-Pakistan agendas, preserving the authenticity and integrity of the Indian government.

**Conclusion**

The development and expansion of social media in the last two decades has had an astounding influence on social, economic, and political life across the world. It has created a new space for trade wars, political campaigns, information and military operations. In the 21st century, social media is utilized as a tool of surveillance and intelligence that in some way is responsible for undermining the territorial sovereignty and integrity of states. As believed, the findings of the paper prove Indian government has been actively involved in exploiting social media so it becomes more of a national security concern to preserve one's own security and frame its own IO strategy to counter its adversary. Since there is no unanimous regulatory and security model at the international to control the flow and distribution of information at social networking sites states should take precautionary measures and strengthen their digital security to ensure their own national narrative and security. To prevent Indian IO, the paper makes important recommendations for the government of Pakistan to ensure the security of digital space from anti-Pakistan content.

**Conflict of Interest:** The authors declare no conflict of interest.

**Funding:** This research received no external funding.

**References**


Khan, I. A. (2021, November 5) FATF asked to probe India’s role in keeping Pakistan on grey list. *Dawn.* https://www.dawn.com/news/1656024


Pakistan Observer. (2024). ‘X’ banned on basis of intelligence reports, says official. https://pakobserver.net/x-banned-on-basis-of-intelligence-reports-says-official/


Stanford Internet Observatory. (August 24, 2022). *Unheard Voice: Evaluating five years of pro-Western covert influence operations*. Cyber Policy Center


