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

NUST Journal of International Peace & Stability
2024, Vol. 7(2) Pages 42-52
njips.nust.edu.pk
DOI: http://doi.org/10.37540/njips.v7i2.173

***Maheen Shafeeq**[1]

Abstract
In the era of digital media, states have resorted to social media to pursue several agendas. In this regard, this paper focuses on the pivotal role of Social Media (SM) in the evolving strategies of intelligence, surveillance, and Information Operations (IO). The paper examines various strategies of IO mentioned in US military documents, encompassing Military Deception (MILDEC), Computer Network Operations (CNO), Operations Security (OPSSEC), and Psychological Operations (PsyOps). The paper specifically evaluated the role of SM 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 SM has become an open source of intelligence for conducting IO by India and influencing opinions and perceptions of Pakistan in Western capitals. This influence has had a significant impact on Pakistan, and therefore, the paper recommends urgent 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 (SM) at the turn of the 21st century has not just revolutionized but fundamentally altered the conduct of communication in a way that the world has not witnessed before. SM sites such as X (Twitter), Facebook, Instagram, TikTok, and so on have unique features that have exponentially multiplied people's ability to share and consume information and data in the form of videos, pictures, and short statements. These SM sites hold significant relevance when it comes to

[1] *****Corresponding Author: *Maheen Shafeeq is* a Research Associate at the Institute of Strategic Studies (ISSI), Islamabad, Pakistan
E-mail: maheenshafeeq246@gmail.com

Received 26 June 2023; **Revised** 10 May 2024; **Accepted** 25 May 2024; **Published online** 30 June 2024

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 realizing the potential of SM for carrying 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 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 utilized 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 SM, the abundance of real-time information has become a component of IO due to the following reasons:

- SM 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).
- SM 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). SM can also act as an extended hand in transiting information from the physical world to the online world.
- SM 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, SM can also be used to influence and alter beliefs, perceptions, and understandings.
- IO, through SM, has reduced the time it would take to gather information compared to traditional means. It only takes a second to upload a picture or post a comment on SM (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).

The features mentioned above of SM present a fertile ground for hostile forces to conduct IO. This paper analyses the correlation of IO and SM and investigates the case study of Indian Chronicles to analyze the scope of IO conducted by the Indian government. It studies how the Indian government employed various types of IOs to develop and run fake UN and EU-accredited organizations and how IOs were amplified with the help of SM. The 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 SM 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 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 SM.

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

The primary objective is to inform the readers about information operations, associated concepts, and consequences. The second key objective of this research is to assess the role of such IO campaigns, including SM 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 the Department of Defense (DoD), IO comprises four pillars: (i) Military Deception (MILDEC), (ii) Computer Network Operations (CNO), (iii) Operations Security (OPSEC), and (iv) Psychological Operations (PsyOps) (Theohary, 2021). The following points highlight the correlation between IO and SM:

- Military deception (MILDEC) employs SM sites to gain an advantage over adversaries and their leaders by misguiding and 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 available data. These independent networks also include SM and the use of data available on these SM sites. (Paul & Porche, 2017).
- Operations Security (OPSEC) uses SM in a disconnected manner to identify and protect data that could be grouped together to develop a bigger picture (Department of Army Headquarters, 2018).
- Psychological operations (PsyOps) use SM 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, and OPSEC play a vital role in misleading, collecting, and protecting information on SM, 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 SM. The relation between SM and PsyOps is further elaborated below.

Social Media Psychological Operations (SMPsyOps)

Psychological Operations (PsyOps) are utilized in peace and wartime activities (Mabima, 2018). This concept is not new; it is as old as the history of humanity and war (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, SM platforms have vastly increased the scope and capacity of PsyOps compared to these physical means (Mabima, 2018).

According to the DoD, PsyOps aims 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, SM 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 SM Psychological Operations (SMPsyOps). The unique features of SM platforms make them an ideal environment for conducting SMPsyOps. SMPsyOps is supported by numerous research studies and analyses that have been conducted on the correlation between SM and PsyOps. Pakistan recently banned the SM platform X (Twitter) due 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, to promote a desired narrative, has become a routine practice in the age of SM to influence and malign adversarial states. This demonstrates the growing relevance of SM for states and civilian and military leaderships as they increasingly rely on SM to alter people's opinions and behaviors (Mlot, 2013). In addition, the US, Israeli, Russian, and British armed forces have developed a unique bridge that mainly focuses on PsyOps and SM in an attempt to 'master a new kind of warfare' (Flint, 2016, para 3). This indicates that SM and PsyOps are integral to contemporary intelligence and military strategies. The interplay of IO and PsyOps on SM has emerged as an imperative tool to harm the adversary's national security and wage irregular, asymmetric, and hybrid warfare (Mabima, 2018). Such 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 through strategically designed SM campaigns, which use the following methods to achieve their objectives.

- *Propaganda*: SM campaigns propagate an idea or narrative in the minds of its intended targets (Farka & Neumayer, 2020). The propaganda on SM can use truthful information, however, in a manner that is misleading and may include stolen information (Department of Defense, 2014).
- *Misinformation*: Unintentionally sharing false information or fake news on SM without counter-checking the information. Such false information is believed to

be accurate by the intended target under the influence of peers (Acemoğlu et al., 2021).

- *Disinformation*: Unlike misinformation, disinformation intentionally spreads false information (Department of Defense, 2014).

SM becomes the echo chamber for SMPsyOps through propaganda, misinformation, and disinformation. These tactics are propagated by manipulating algorithms using bots and 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 SM Psychological Operations (SMPsyOps). These operations utilize information available on SM or use SM to disseminate and amplify desired information and messages to a target audience. They are carried out against adversaries to intentionally damage their reputation among specific audiences. This was 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 ten 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).

Misleading depictions, with covert support from the state, evidently characterized the entire information operation (IO). 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 IO tactics could be identified. Military Deception (MILDEC) was employed, as misleading information was disseminated to international decision-making bodies such as the UN and EU and to the audience on SM 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 SM 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 SM accounts to disseminate misinformation and disinformation among decision-makers within the UN and EU. Notably, Twitter (now X) was observed to trend anti-Pakistan content through bot accounts, influencing a broad audience (Kausar et al., 2021). These online platforms served as honeypots, enticing members of Parliament to engage with and propagate anti-Pakistan content on SM.

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 SM 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 SM channels associated with fictitious news agencies to assess the impact of this psychologically manipulative content.

Additionally, the Indian government employed SM Psychological Operations (SMPsyOps) to effectively propagate its 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 to tarnish 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 IOs continued under the nose of Western capitals and on SM due to their anonymity and lack of direct association with the Indian government. The JP 13-3 document stated that the anonymity of cyberspace allows ideal ground for covert information operations, which can be carried out without association (Department of Defense, 2014). If government-sponsored covert IOs are exposed, the government usually denies 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. On the issue, Pakistan's Foreign Minister, Shah Mehmood Qureshi, stressed the notion that the Indian-funded network is manipulating the international system for its nefarious designs (Reuters, 2020). This highlights the urgent need to address the fasting-spreading trend of fake SM 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 is no denying that Pakistan has dramatically benefited from SM 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 SM platforms. Despite urging SM companies to establish local offices for better communication and coordination, Pakistan's influence in overregulating these platforms remains limited due to resistance from these companies.

In contrast, India wields significant influence over SM 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 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 SM demands a well-conceived and executed strategy involving multiple ministries working in coordination. Unfortunately, the absence of a national-level SM 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 SM. Pakistan should also contact governments and international institutions mentioned in the Indian Chronicles, urging a 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 SM 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 SM 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 SM and digital media in terms of IO, the Pakistani government should integrate these domains as elements of national power. Pakistan should convene relevant public and private stakeholders to assess and analyze SM and

IO trends, aiming to formulate 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 '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 industries to tailor their security approaches by covering these four key vectors (Alaphilippe, 2020).

Nullifying Misinformation and Propaganda Through Social Media

Countering misinformation and propaganda, especially on SM, is essential to preventing falsehoods from gaining traction and evolving into perceived truths (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 SM as a force multiplier, Pakistan should initiate comprehensive efforts to harness these platforms as tools for empowerment. Instead of merely observing SM dynamics, 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 misinformation and reinforce Pakistan's narrative on various issues.

Building Counter Narrative

Pakistan should craft its national narrative to combat India's disinformation campaigns effectively. 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) targets specific segments of Pakistani society, Pakistan needs 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 SM 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 SM 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), mainly Psychological Operations (PsyOps).

By implementing the recommendations above, the government and state institutions can significantly bolster their capacity for managing SM against Indian IO. This proactive approach combats IO on SM and 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 SM in the last two decades has had an astounding influence on social, economic, and political life worldwide. It has created a new space for trade wars, political campaigns, information, and military operations. In the 21st century, SM 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 that the Indian government has been actively exploiting SM, so it has become more of a national security concern to preserve one's security and frame its own IO strategy to counter its adversary. Since there is no unanimous regulatory and security model at the international level 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 national narrative and security. To prevent Indian IO, the paper makes essential 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

Acemoğlu, D., Ozdaglar, A., & Siderius, J. (2021, June 30). *Misinformation: Strategic Sharing, homophily, and endogenous echo chambers.* VOX EU. https://voxeu.org/article/misinformation-social-media

Alaphilippe, A. (2020). Adding a D to the ABC disinformation framework. *Brookings Institution.* https://policycommons.net/artifacts/4139892/adding-a-d-to-the-abc-disinformation-framework/4948112/

Abdulrahman, F., & Subedar, A. (2020). How much can you fake a trend on Twitter? in one country, about £150. *BBC News*, *29*. https://www.bbc.com/news/blogs-trending-43218939

Chin, W. (2019). Technology, war and the state: past, present and future. *International Affairs*, *95*(4), 765-783. https://doi.org/10.1093/ia/iiz106

Cowan, M. D., & Cook, M. C. (2018). Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change. *Military Review*, *1*. https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/Cook-Cowan-PSYOP-v2.pdf

Department of Army Headquarters. (2018). *The Conduct of Information Operations.* Washington D.C.: Army Publishing Directorate.

Department of Defense. (2014, Nov 20). *Joint Publication 3-13 Information Operations.* Joint Staff US Armed Forces. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Department of Defense. (2017). *Military Deception Joint Publication 3-13.4.*

Ekwunife, N. (2020). National security intelligence through social network data mining. In *2020 IEEE International Conference on Big Data (Big Data)* (pp. 2270-2273). IEEE. https://ieeexplore.ieee.org/document/9377940

European Union Agency for Cybersecurity. (2020). *Information Operations – Active Defence and Offensive Countermeasures*. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/information-operations-2013-active-defence-and-offensive-countermeasures

Farka, J., & Neumayer, C. (2020). Disguised Propaganda from Digital to Social Media. In J. Hunsinger, M. M. Allen, & L. Klastrup, *Second International Handbook of Internet Research* (pp. 707-723). Berlin: Springer.

Flint, J. (2016, Feb 6). Army joins the social media war with psy-ops brigade. *The Conversation.* https://theconversation.com/army-joins-the-social-media-war-with-psy-ops-brigade-37125

Fortin, F., Delle Donne, J., & Knop, J. (2021). The Use of Social Media in Intelligence and Its Impact on Police Work. In J. J. Nolan, F. Crispino, & T. Parsons, *Policing in an Age of Reform* (pp. 213-231). Switzerland: Palgrave Macmillan.

Fournier, J. (2021). How algorithms are amplifying misinformation and driving a wedge between people. *The Hill.* https://thehill.com/changing-america/opinion/581002-how-algorithms-are-amplifying-misinformation-and-driving-a-wedge

François, C. (2020). Actors, behaviors, content: A disinformation ABC. *Algorithms*. https://policycommons.net/artifacts/8986429/untitled/9875484/

Goldstein, F. L., & Findley, B. F. (Eds.). (1996). *Psychological operations: Principles and case studies* (p. 351). Maxwell Air Force Base, AL: Air University Press.

Gery, W. R., Lee, S., & Ninas, J. (2017). Information Warfare in an Information Age. *Joint Force Quarterly, 85*(2), 22-29.

Hafeez, M. (2021). Indian Chronicles: An Eye Opener for the World Community. *Institute of Strategic Studies Islamabad*. http://issi.org.pk/wp-content/uploads/2021/01/IB_Mahwish_Jan_14_2021.pdf

Javed, Z. (2021). Analysis of the Indian Chronicles. *Islamabad Policy Research Institute. https://ipripak.org/wp-content/uploads/2021/05/Indian-Chronicles-Policy-Brief.pdf*

Kausar, S., Tahir, B., & Mehmood, M. (2021). Towards Understanding Trends Manipulation in Pakistan Twitter. *arXiv:2109.14872*. https://arxiv.org/abs/2109.14872

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

Khetran, M. S. (2017). Indian Interference in Balochistan. *Strategic Studies, 37*(3), 112-125. https://issi.org.pk/wp-content/uploads/2017/10/7-SS_Mir_sherbaz_Khetran_No-3_2017.pdf

Mabima, J. (2018, Oct 29). *Social Networking Sites as a Tool of Psychological Operations: A Case Study.* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3261039

Alaphilippe, M., G., Adamczyk, R., & Grégoire, A. (2020, Dec 9). *Indian Chronicles.* EU Disinfo Lab. https://www.disinfo.eu/wp-content/uploads/2020/12/Indian-chronicles_FULLREPORT.pdf

McKew, M. K. (2019, Feb 8). *Rules of Engagement for Social Media Influence Operations.* Defusing Disinfo. https://defusingdis.info/2019/02/08/rules-of-engagement-for-social-media-influence-operations/

Mlot, S. (2013, February 12). Raytheon Riot Software Predicts Behavior Based on Social Media. *PCMag*. https://www.pcmag.com/news/raytheon-riot-software-predicts-behavior-based-on-social-media

Mohan, G. (2020, December 12). India Clarifies on Fake News Report. *India Today* https://www.indiatoday.in/india/story/india-clarifies-on-fake-news-report-blames-pakistan-1748892-2020-12-12

Nakashima, E. (2022, September 19). Pentagon opens sweeping review of clandestine psychological operations. *The Washington Post.* https://www.washingtonpost.com/national-security/2022/09/19/pentagon-psychological-operations-facebook-twitter/

Omand, S., Bartlett, J., & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823.

Otis, G. (1991). *Information Operations*. FAS. https://irp.fas.org/doddir/army/fm34-1/ch7.htm

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

Paul, C., & Porche, I. (2017). *Cyber Forces and U.S. Cyber Command.* Santa Monica, CA: RAND Corporation.

Rehman, A. (2021, January 18). Indian Chronicle: Exposing the Indian Hybrid warfare against Pakistan. *Modern Diplomacy*. https://moderndiplomacy.eu/2021/01/18/indian-chronicle-exposing-the-indian-hybrid-warfare-against-pakistan/

Reuters. (2020, December 12). *Pakistan accuses India of funding disinformation campaign in EU.* https://www.reuters.com/article/pakistan-india-idUSKBN28M022

Shallcross, N. (2017). Social Media and Information Operations in the 21st Century. *Journal of Information Warfare*, *16*(1), 1-12. https://www.jstor.org/stable/26502873

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

Thales. (2022, Jan 25). *5G technology and networks (speed, use cases, rollout)*. Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G

Theohary, C. A. (2015, March 4). *Information Warfare: The Role of Social Media in Conflict.* FAS. https://sgp.fas.org/crs/misc/IN10240.pdf

Theohary, C. A. (2021). *Defense Primer: Information Operations.* Congressional Research Service (CRS).

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies*, *18*(4-5), 530-547. https://doi.org/10.1177/13675494155773