CASS

CENTRE for AEROSPACE & SECURITY STUDIES

Militarisation of Social Media

Research Team

Amna Tauhidi

&

Maheen Shafeeq

Research Directors

Air Vice Marshal Faheem Ullah Malik (Retd)

&

Air Vice Marshal Sohail Malik (Retd)

Working Paper

President
AIR MARSHAL FARHAT HUSSAIN KHAN (RETD)

Edited by:
SARAH SIDDIQ ANEEL

Layout
HIRA MUMTAZ

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

Centre for Aerospace & Security Studies

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

Old Airport Road, Islamabad, Pakistan
www.casstt.com

CENTRE for AEROSPACE & SECURITY STUDIES

Militarisation of Social Media

Working Paper

Research Team

Amna Tauhidi

&

Maheen Shafeeq

Research Directors

Air Vice Marshal Faheem Ullah Malik (Retd)

&

Air Vice Marshal Sohail Malik (Retd)

TABLE OF CONTENTS

Abstract

This Working Paper attempts to explore the militarisation aspect of social media and its impacts on national security. It finds that on the one hand, social media has revolutionised the conventions of socialisation and information sharing, while on the other, it has become an ideal platform for surveillance and intelligence. The militarisation aspect, in this study, covers Information Operations (IOs), PsyOps, propaganda, misinformation, fake news, and disinformation. To counter the threats emanating from these strategies, it is important to work towards joint efforts at individual, organisational and state level. The paper specifically provides a set of measures at the individual and state level and puts forth recommendations on how to counter the growing threat of misinformation, disinformation, hate speech, and false narratives. Lastly, the paper suggests that it is pertinent to study social media dynamics from a wider perspective and highlights the need for a dynamic and evolving Social Media Policy for Pakistan.

Keywords: National Security, Social Media, Information Operations, Propaganda, Misinformation, Fake News, Disinformation.

Introduction

No technology has been weaponised at such an unprecedented global scale as social media.

- *Jonathan Ong Jason Cabañes*

Social media networking sites such as Facebook, Google, YouTube, Instagram, TikTok, Snapchat, among others, have emerged as an easily accessible and readily available tool for virtual socialisation. These sites not only serve as platforms for socialising but also facilitate more connectivity and engagement. Likewise, these platforms have also provided a breeding ground to political parties to stay connected with their voters. While social media is supposed to have a progressive impact, it has also provided space for the spread of extremism, racism, violence, radicalisation, misinformation, disinformation, and fake news which have been adopted as methods of warfighting, otherwise called 'militarisation of social media.'

This evolution of social media has transformed the traditional methods of warfighting by introducing newer, non-violent, often more lethal tools and tactics of warfare. These non-violent means of warfighting employ social media and its burgeoning power to play mind games and alter the morals/values, thinking, and decision-making power of individuals. According to Clausewitz:

> *War is a trial of moral and physical forces using the latter….In the consequent analysis, it is a moral, not physical strength that all military action is directed….Moral factors, then, are the ultimate determinants in war.*

Social media is now serving as a tool of altering morals both during peace and war time.

The expanding scope of social media and its utility in military operations has made it a useful tool in the military kit of both state and non-state actors to achieve their economic, political, and strategic objectives. States and non-state actors are using social media networks as fertile ground to launch Information Operations (IOs).

According to a survey conducted by the Oxford Internet Institute, 81 countries are using social media to spread computational propaganda and disinformation about

politics.[1] The findings of the survey are evidence of the fact that misinformation has become more 'professionalised' to serve the interests of its initiators. Governments and political parties are investing heavily in building their 'private sector cyber troops'. The survey also showed that 'cyber troops' are affiliated with state agencies and assigned the task of shaping public perceptions and political attitudes.

The political manipulation of social media was also evident in the 'Cambridge Analytica scandal. The scandal revealed that the company working for the Trump campaign harvested user data from up to 87 million Facebook profiles before the 2016 election and used those data for social-media manipulation.[2] Such incidents provide an understanding of how modern-day social-media apps can be manipulated to amplify a particular political discourse' and achieve one's interests.

This *Working Paper* is an attempt to understand the evolving power of social media and its impacts on national security. The paper covers the militarisation aspect under the broad themes of Information Operations (IOs) and Psychological Operations (PsyOps), fake news, misinformation, and disinformation. The *Indian Chronicles* report by the EU DisinfoLab[3] and the objectives behind it, are worrisome both for national integration and national security. Keeping the above-mentioned scope and dynamics of social media in mind, the paper argues that it is becoming important for strategists and policymakers to study in detail the military aspect of social media and its implications for the security of the state. The paper concludes that to secure its digital space, it is of utmost importance that Pakistan develops a comprehensive 'Social Media Policy' at the national level and engage in dialogue with social media platforms to register her concerns.

---

1 Samantha Bradshaw, Hannah Bailey and Philip N. Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*, report (Oxford: Programme on Democracy & Technology, 2021), https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/#continue.

2 Alvin Chang, "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram," *Vox*, May 2, 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

3 Gary Machado, Alexandre Alaphilippee, Roman Adamczyk and Antonie Gregoire, "Indian Chronicles: Deep Dive into a 15-Year Operation Targeting the EU and UN to Serve Indian Interests," EU DisinfoLab, December 9, 2020, https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/.

Social Media: Tool for Surveillance Intelligence

Social media is now being utilised for surveillance intelligence and information gathering on people to whom propaganda, misinformation, and disinformation can be broadcasted. For this purpose, extensive data on citizens is being exchanged and analysed using data mining algorithms to spot persons of interest. In many state jurisdictions, social media companies are even bound by specifically framed laws to provide required information on citizens to intelligence agencies when needed.[4] The data gleaned from surveillance is also used for making future predictions by analysing user profiles. State agencies keep a record of online activities of users to get information regarding tactical, strategic, and operational interests to assess the effects of kinetic operations.[5] Once manipulatable individuals are identified through surveillance and data mining tactics, IOs and Psychological Operations (PsyOps) are employed against them to achieve the desired outcomes.

Social Media & Information Operations (IOs)

The United Department of Defense (DoD) defines IO as 'the integrated employment (during States military operations) of Information-Related Capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.'

Social media can prove to be a powerful instrument in IOs,[6] for retrieving information and getting insight into the military strengths and capabilities of an adversary, Military Information Support Operations (MISOs), public undertakings, or common military activities, along with 'different capacities that create impacts in and through the data climate.'[7] Other than this, social media can be used for political manipulation, especially during elections. The prime example of manipulation can be traced back to

---

4 Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," *New York Times*, April 4, 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

5 William Marcellino, Meagan L. Smith, Christopher Paul, and Lauren Skrabala, *Monitoring Social Media: Lessons for Future Department of Defence Social Media Analysis in Support of Information Operations*, report (Santa Monica: RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1742.html.

6 Christopher Whyte, "Protectors without Prerogative: The Challenge of Military Defense against Information Warfare," *Journal of Advanced Military Studies* 11, no. 1 (2020): 166-184. https://muse.jhu.edu/article/796248/pdf.

7 Rugge Fabio, *'Mind Hacking': Information Warfare in the Cyber Age*, paper (Italian Institute for International Political Studies, Analysis no. 319, 2018), https://www.ispionline.it/sites/default/files/pubblicazioni/analisi319_rugge_11.01.2018_0.pdf.

Russian IOs targeting the 2016 US Presidential Elections.[8] Social media holds immense potential to help IOs by giving access into the viewpoints, considerations, and mindsets of people of interest.[9] Social media platforms can give significant data on peoples' socioeconomic status, authoritative structure, zones of movement, and organisational reach. Such subtleties can amplify endeavors to target messages to select groups to impact their insights, choices, and practices.[10]

Social Media & Psychological Operations (PsyOps)

The concept of PsyOps is as old as the history of war. During the Vietnam War and Operation Desert Storm, and until the Second Gulf War, printed newspapers, pamphlets, and radio broadcasts were the tools of PsyOps.[11] However, in the digital age, the capability of PsyOps increased manifold due to the emergence of social media.[12] According to the US DoD:

> *PsyOps are 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, organisations, groups, and individuals.*[13]

The definition makes it clear that the primary objective of PsyOps is to alter the minds of its targeted audience and in present time, social media has provided an ideal platform for this. This has made social media an ideal location for the conduct of PsyOps.[14] Although historically, military and political strategy have included PsyOps

---

8 Camille Francois and Herb Lin, "The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping A Blind Spot," *Journal of Cyber Policy* 6, no. 1 (2021): 9-30, https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1950196.

9 Alexander Aguilastratt, Matthew Updike and Montigo White, "The Information Domain and Social Media: Part 1," *NCO Journal*, January, 2022, https://www.armyupress.army.mil/Portals/7/nco-journal/images/2022/January/Social-Media/The-Info-Domain-Part%201.pdf.

10 Marcellino, Smith, Paul, and Skrabala, *Monitoring Social Media*.

11 Frank L. Goldstein and Benjamin F. Findley, *Psychological Operations: Principles and Case Studies* (Alabama: Air University Press, 1996), https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0018_GOLDSTEIN_FINDLEY_PSYCHOLOGICAL_OPERATIONS.pdf.

12 Joseph Mabima, "Social Networking Sites as a Tool of Psychological Operations: A Case Study," (MA diss., London: King's College London, 2018), https://doi.org/10.2139/ssrn.3261039.

13 David Cowan and Chaveso Cook, "Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change," *Military Review,* March*,* 2018, https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/Cook-Cowan-PSYOP-v2.pdf.

14 Glenda Jakubowski, "What's Not to Like? Social Media as Information Operations Force Multiplier," *Joint Force Quarterly* 94, no. 3, (2019): 8-17, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-94/jfq-94_8-17_Jakubowski.pdf?ver=2019-07-25-162024-817.

but with the development of social media platforms, such ops has acquired a ready-made medium to amplify operational effectiveness. Research conducted at King's College London, there is a relatively greater use of Social Networking Services (SNS) in contemporary PsyOps to achieve an outcome with relative convenience.[15] According to the study, the infectious capabilities of social media and the vulnerability that PsyOps poses to alter narratives and opinions must be an integral part of contemporary intelligence and military strategies.[16]

The interplay of IOs and PsyOps with social media has emerged as an imperative tool to harm adversary's national security, wage irregular warfare, and be used as a virtual force multiplier in conventional warfare.

Propaganda, Misinformation & Disinformation

Backed with information gathered through IO and PsyOps, adversaries may become well equipped with the data regarding individuals and groups that constitute the desired audience. Social media then serves as a channel to further disseminate IOs and PsyOps into the minds and alter the behaviour of the target audience.[17] The financial model of social media is profit-driven; it, therefore, serves the business interests of social media service providers to provide links of people and communities to the highest bidder[18] for propaganda, misinformation, and disinformation.

Once misinformation and propaganda are disseminated through the social media business model, it can not only alter the truth and narrative of a state but also reduce an adversary's will to fight and discourage retaliatory aggressive actions.[19] Hence, IOs broadly aim to impact decision-making while PsyOps achieve behavioural change as the ultimate objective.[20]

---

15 Mabima, "Social Networking Sites as a Tool of Psychological Operations: A Case Study."

16 Anthony Seaboyer, *Influence Techniques Using Social Media*, report (Ontario: Royal Military College of Canada, 2018), https://cradpdf.drdc-rddc.gc.ca/PDFS/unc365/p807750_A1b.pdf.

17 Zachry Luab, "Hate Speech on Social Media: Global Comparisons," *Council on Foreign Relations*, June 7, 2019, https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons.

18 Dave Evans and Jake McKee, *Social Media Marketing* (Indianapolis: Wiley Publishing, Inc, 2021).

19 Linton Wells, "Cognitive-Emotional Conflict: Adversary Will and Social Resilience," *PRISM* 7, no. 2 (2017): 4-17, https://www.jstor.org/stable/26470514.

20 Christopher J Lamb and Paris Genalis, *Review of Psychological Operations Lessons Learned from Recent Operational Experience*, report (Washington, D.C.: National Defence University Press, 2005), https://irp.fas.org/eprint/lamb.pdf.

PsyOps in Pakistan pervades through interest groups which can be internal and external.[21] The upper crust of the society that holds greater influence on the public falls in the category of 'people of interest' while minorities or the neglected segments of the society fall under 'groups of interest'.[22] While sectarian and religious extremism is being exploited through social media to spread propaganda and misinformation,[23] of late, opposition against Pakistan's government institutions and the military has been growing on social media as well. Fake news and false info campaigns against the Army and its personnel have been on the rise. For instance, Amjad Shoaib, a retired Army General, and defense analyst believes, that there is a widespread smear campaign against the Army and other state institutions on social media. He was targeted by a social media user who accused him of acquiring land illegally. He denied such allegations as being baseless.[24] Additionally, fake news regarding the detention of various generals, who opposed the sitting Chief of Army Staff, have also been circulating on social media.[25]

While the spread of such propaganda, misinformation, disinformation, and fake news regarding the state and its institutions is regulated in Europe and US,[26] there is no effective mechanism to check the spread of anti-state propaganda in Pakistan. Such malicious falsehood is not only baseless but also hurts national integrity and poses a threat to national security.

In 2020, the EU DisinfoLab, a European Non-Government Organisation (NGO) tackling global disinformation practices, published its findings that unveiled a vast Indian network of more than 750+ fake news sites and 550+ domain names expanding over 119 countries entangling over 10 resurrected NGOs accredited by United Nations

---

21 International Crisis Group, *The State of Sectarianism in Pakistan*, report (Brussels: International Crisis Group, 2005), https://www.crisisgroup.org/asia/south-asia/pakistan/state-sectarianism-pakistan.

22 Ansar Abbasi, "BLA Has Known Indian Connection," *News International*, July 1, 2020, https://www.thenews.com.pk/print/680356-bla-has-known-indian-connection.

23 International Crisis Group, *The State of Sectarianism in Pakistan*.

24 "Pakistan Seeks to 'Control Digital Media' amid Anti-Government Protests," *Deutsche Welle,* December 26, 2020, https://www.dw.com/en/pakistan-seeks-to-control-digital-media-amid-anti-government-protests/a-55422291.

25 "Pakistanis Poke Fun at Indian Media's 'Civil War' Hyperbole, Ministers Ask Twitter to Take Action," *Dawn*, October 22, 2020, https://www.dawn.com/news/1586438.

26 Sophia Ignatidou, "EU–US Cooperation on Tackling Disinformation," (paper, Chatham House, London, 2019), https://www.chathamhouse.org/sites/default/files/2019-10-03-EU-US-TacklingDisinformation.pdf; Joris v. Hoboken and Ronan Ó Fathaigh, "Regulating Disinformation in Europe: Implications for Speech and Privacy," *UC Irvine Journal of International, Transnational, and Comparative Law* 6, no. 9 (2021): 9-36, https://scholarship.law.uci.edu/ucijil/vol6/iss1/3.

Human Rights Council (UNHRC) to spread anti-Pakistan propaganda, misinformation, and disinformation.[27] Pakistan has maintained that India uses various methods of IOs and PsyOps to spread propaganda, misinformation, and disinformation to damage its reputation within the international community.[28] It is also believed that India is targeting minorities and people affected by state policies in Pakistan to spread anti-state agenda. There are fake social media accounts created outside Pakistan (with fake IDs/locations) to influence the public inside the country.[29] There have also been reports of banning accounts from Pakistan that raise voices against Indian oppression in the Indian Illegally Occupied Jammu & Kashmir.[30] This is all being done under Indian State influence.

Hence, social media is not only affecting the psychological, social, and political fabric of Pakistan but also heavily impacting its national security and reputation at the international level. There is no doubt that Pakistan has benefitted from social media in terms of connectivity and communication. However, social media in the country is still unregulated and unmanaged which is fuelling its negative potential. Since the adverse effects of social media can be regulated, there is a greater need to take this initiative now before it is too late.

---

27 Machado, Alaphilippee, Adamczyk and Gregoire, *Indian Chronicles.*

28 "FM Qureshi Urges UN, EU to Investigate Report on Indian Propaganda Network," *Dawn*, December 11, 2020, https://www.dawn.com/news/1595195/fm-qureshi-urges-un-eu-to-investigate-report-on-indian-propaganda-network.

29 Ramsha Jahangir, "Indian Network Lobbying against Pakistan Exposed," *Dawn*, December 10, 2020, https://www.dawn.com/news/1594928/indian-network-lobbying-against-pakistan-exposed; "400 Fake Social Media Accounts being Reported Daily, PTA tells PAC," *Pakistan Today*, June 8, 2022, https://www.pakistantoday.com.pk/2022/06/08/192834/.

30 "One Year of India's Clampdown in Occupied Kashmir – Here's Everything You Need to Know," *Dawn*, August 13, 2020, https://www.dawn.com/news/1514652.

Countering Militarisation of Social Media

To counter militarisation of social media, state regulations are necessary, however, these may not be enough to have an impact alone. Therefore, it is the responsibility of individuals alongside the state to take the initiative of countering militarisation of social media. This section discusses the measures that can be taken at the individual level followed by recommendations for the state to combat and counter the militarisation trends of social media.

Individual Level Measures: Combatting Misinformation & Fake News

There is an increasing trend in news outlets to publish fake news and disseminate it through social media to increase readership and generate profits. According to research conducted by the Massachusetts Institute of Technology, true stories take six times longer to reach 1500 people as compared to fake news to reach the same number.[31] This is because, the research found that false news is 70% more likely to be retweeted than true stories.[32] There is also a wide use of fake news and misinformation as part of psychological warfare. Fake news and misinformation gather attention because of their flashy headlines, often referred to as 'clickbait', which lure users by creating curiosity while factual news does not usually employ this technique. As more people depend on social media as a source of information, the dissemination of fake news and misinformation, becomes easy. According to the Reuters Institute for the Study of Journalism, about 51% of people surveyed reported that they received news from online sources.[33]

Fake news and misinformation is spreading because of the way people consume information. This indicates that the long-standing institutional defences against such ploys are eroding. This is not only making the security of institutions weak, but also impacting the security of states. In fact, this has emerged as a global problem.[34]

---

31 Peter Dizikes, "On Twitter, False News Travels Faster than True Stories," *MIT News*, March 8, 2018, https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

32 Dizikes, "On Twitter, False News Travels Faster than True Stories."

33 Nic Newman, Richard Fletcher, Anne Schulz, Simge Andı and Rasmus Kleis Nielsen, *Reuters Institute Digital News Report 2020*, report (Oxford, UK: Reuters Institute for the Study of Journalism, 2020), https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf.

34 Claire Wardle, "Misinformation Has Created a New World Disorder," *Scientific American*, September 1, 2019, https://www.scientificamerican.com/article/misinformation-has-created-a-new-world-disorder/.

To tackle the issue of fake news and misinformation, it is foremost the duty of individuals to evaluate the authenticity of the news before sharing it. According to a Harvard University blog, the following activities can help spot fake news and misinformation at the individual level:[35]

1. Vetting Credibility of Publisher

To evaluate the credibility of the source, one must assess if the publishing site meets the academic citation criteria. Does the source mention the name of the author, date of publication? Has a trustworthy reputation. For instance, who is the author of the article? Does he or she have any other publications? Or is there a bio-line of the author? It is also important to read the 'About Us' section of the website which usually mentions the publisher's mission statement and the nature of its publication. An unusual domain name of the website also shows whether it is authentic or not.

2. Quality of Publication

To analyse the quality of publication, it is important to read past the headlines. The publishers that use a lot of CAPS, dramatic punctuation, flashy headlines, or headlines that create curiosity are usually an indication of false news or misinformation. The purpose of such attention-grabbing statements is profit generation through click baits. The quality of the publication can also be judged by noticing editing and spelling errors. Moreover, the quality of the publisher is also undermined if the story narrates biased information and fails to provide contradictory claims.

3. Citations & Source Review

If the content appears on social media and is promoted by a source known for click baits, it is best to proceed with caution. Even if shared by a trustworthy acquaintance, one should vet the credibility of the publisher. If the news lacks a source, particularly on a complex issue, that means research is missing and there is less fact-based information. Additionally, if similar information is not available on other authentic sites, then it is likely that journalists do not have valid or thoughtful information on the subject. Moreover, in the era of deep fakes and Photoshop software, it is important not to fall victim to false news, misinformation, and disinformation.

---

[35] Christina Nagler, "4 Tips for Spotting a Fake News Story," *Harvard Summer School*, January 23, 2017, https://summer.harvard.edu/blog/4-tips-for-spotting-a-fake-news-story.

4. Fact-Checking Websites

If the above-mentioned steps have been taken, and one is still doubtful, professional help may be sought. Fact-checking websites verify facts and dismiss false information. An increasing number of fact-checking websites evaluate the truth of claims and judge them based on authentic information from credible sources.[36]

Figure 1 is also a useful infographic generated by the Cornell to spot fake news.

Figure 1: How to Spot Fake News

Source: "Fake News, Propaganda, and Misinformation: Learning to Critically Evaluate Media Sources: Infographic: Spot Fake News," Cornell University (2020), https://guides.library.cornell.edu/evaluate_news/infographic.

It is imperative to move beyond narratives that are spread through popular social media channels and strive to be skeptical of virtual information; however, that is usually not a common practice due to ignorance. There is an increasing need to inform the general population of the means to counter-check information as well as a collateral need for vigorous awareness campaigns on social media against this trend. Daniel Kahneman, a psychologist, in his book 'Thinking, Fast and Slow' introduces the

[36] Nagler, "4 Tips for Spotting a Fake News Story."

concept 'WYSIATI' that stands for 'What You See Is All There Is' – which means that humans tend to not look for what they do not see, rather they only rely on available information without being completely aware of what they do not know.[37] This was famously elaborated by Donald Rumsfeld:

> *There are known knowns, the things that we are aware of; and there are known unknowns; the things that we know we do not know. But there are also unknown unknowns; the things that we do not know.*

'Unknown knowns' and 'unknown unknowns' are where false news and misinformation lies, and humans tend not to fill in the gaps. They tend to rely on elements of the story that are known and construct the unknowns from it, often relying on cognitive biases. This behavior can overlook facts and mislead one into consuming false news and information.

The vast network of social media has broadened the sources of false news and misinformation and assisted the spread of propaganda, altering narratives and veiling the truth. This is as much applicable to Pakistan. Measures such as fact-checking websites and general awareness campaigns against false news and misinformation are, therefore, necessary to deal with the challenge. There are numerous fact-checking websites operational around the world that are pursuing journalistic rigor to counter false news and misinformation. Models of such websites can be introduced in Pakistan to cater to the growing need for authentic information. Examples of fact-checking websites include PolitiFact, FactCheck.org, Washington Post Fact Checker, Snopes, Fact Check from Duke Reporters' Lab, SciCheck, Hoax Slyer, International Fact-Checking Network, and NPR FactCheck, among others.

State Level Measures: Countering Militarisation on Social Media

The use of social media by state and non-state actors for spreading propaganda, misinformation, and disinformation makes regulating social media a challenging task for any state. It is widely argued that use of social media by terrorists and extremists is a global problem and calls for a collective response both at the national and international level. Put forth are some recommendations for the Government of

[37] Daniel Kahneman, *Thinking, Fast and Slow* (New York: CreateSpace Independent Publishing Platform, 2014).

Pakistan (GoP) that can help minimise the militarisation of social media by state and non-state actors:

1. *National Social Media Cell (NSMC)*

A National Social Media Cell should be formed with multiple stakeholders and staff from diverse fields such as national security, cyber, Information Technology, and intelligence to analyse social media from multiple angles. The purpose of this Cell would be to propose measures to prevent and counter the militarisation of social media. It should be accountable to the government and must submit and publish its annual progress report in order to ensure transparency.

2. *Social Media Guidelines for Government Institutions*

The government, along with relevant stakeholders, should stipulate elaborate guidelines for engagement on social media by state and Law Enforcement Agencies (LEAs). The guidelines must highlight objectives, engagement protocol, types of platforms, communication strategy, response criteria, and legal limitations for agencies to formulate their respective strategies for engaging on social media. The guidelines, once framed, should be institutionalised without delay.[38]

3. *Countering Misinformation & Propaganda through Social Media*

Keeping in view the force-multiplying ability of social media, efforts must be launched to use this media as an empowering tool for public and government officials to engage proactively and maintain channels of communication. An online active presence will not only weaken false claims and misinformation but also function as a Confidence-Building Measure and a trust-enhancing factor, especially during national security emergencies.

4. *Redirecting Users towards De-Radicalising Content*

Jigsaw, Google's idea lab, introduced a data-driven approach to counter extremism-promoting content online. It developed an application that assists the US government in overcoming hurdles to counter online extremist activities. Instead of relying on government personnel to counter online extremism, the application redirects

---

[38] Shruti Pandalai, "The Social Media Challenge to National Security: Impact and Opportunities: A Conceptual Overview," *Institute for Defense Studies & Analyses Monograph* no.55 (2016), https://www.idsa.in/monograph/social-media-challenge-to-national-security.

YouTube users away from such content. A similar approach can be adopted in Pakistan by joining hands with the tech industry to follow a data-driven approach that redirects Pakistani youth away from online content instigating radicalisation. Policymakers, along with key stakeholders, can decide with consent as to what type of content promotes extremism and is harmful to national security.[39]

5. Shared Database of Digital Fingerprints of Extremist Content

Exploitation of social media by terrorists and extremists is a global problem, so the solution should transcend borders as well. One such solution has been undertaken by the 'Global Internet Forum for Counter Terrorism (GIFCT)' which has developed a shared database where companies and states can create 'digital fingerprints of terrorist content' and share it with each other.[40] GoP should also study this initiative.

6. Need for Public-Private Partnerships to Tackle Social Media

There is significant participation by the private sector in critical infrastructure. The government needs to partner and utilise the services of the private sector to deliver auxiliary services and seek cooperation where it believes the latter has a comparative advantage.[41]

7. Critical Data Securing Software

To ensure the protection and regulation of critical data and information, intelligence agencies can collaborate with cyber experts to design data protection software that can be installed on mobiles and computers. The US Air Force has adopted a similar approach to secure airmen working in the US Department of Defense. USAF has teamed up with 'Good Technology' to provide a secure 'software container' approach that can keep official data separate and secure. The app ensures that employees can access both work-related and personal applications on their devices.[42]

---

39 Thomas H. Kean, Lee H. Hamilton, Blaise Misztal, Nicholas Danforth, Michael Hurley and Jessica Michek, *Digital Counterterrorism: Fighting Jihadists Online*, report (Washington, D.C.: Bipartisan Policy Center, 2018), https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/BPC-National-Security-Digital-Counterterrorism.pdf.

40 Mehmet Nesip Ogun, "Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes," *Journal of Applied Security Research* 7, no. 2 (2012): 203-217, https://sci-hub.hkvisa.net/10.1080/19361610.2012.656252.

41 Graeme A. Hodge, Carsten Greve and Anthony Boardman, *International Handbook on Public–Private Partnerships* (Cheltenham: Edward Elgar Publishing, 2010).

42 Scott E. Solomon, *Social Media the Fastest Growing Vulnerability to the Air Force Mission* (Air Force Research Institute: Air University Press, 2017).

8. Use of Artificial Intelligence

Another promising approach is the development of tools driven by Artificial Intelligence (AI) that could ultimately enable platforms to identify and remove propaganda, misinformation, and disinformation, faster than its creators can put it up. All countries are progressing and investing heavily in the field of AI. Pakistan should also devote attention and resources to the development of expertise in this domain.[43]

9. Layered Cyber Security System

To secure critical information in the digital realm, Pakistan's policymakers and strategic community should look toward implementing a 'layered cyber defence approach.' Layered cyber defense involves multiple security controls in a way that cyber-defense is back by several additional layers of defense to ensure security. It is argued that this multi-layered approach would entail making each stage less hospitable to the launched PsyOps and IOs by the adversary.

10. Provision of Funds

Governments and private companies are making efforts to secure social media in isolation by framing regulations to protect their privacy. There is a need to nationalise this effort, and this will require the allocation of specific budgets, standardisation of tools, and provision of technology.[44]

11. Awareness Campaigns

One of the existing gaps identified is the lack of awareness amongst citizens regarding social media threats and vulnerabilities. Social media is increasingly being used to spread propaganda, misinformation, cybercrimes, and cyber theft, to mention a few. These threats proliferate through careless behaviour while using social media. To make citizens responsible and safe, awareness campaigns should be initiated on how these tools can be used safely from the school till government level.[45]

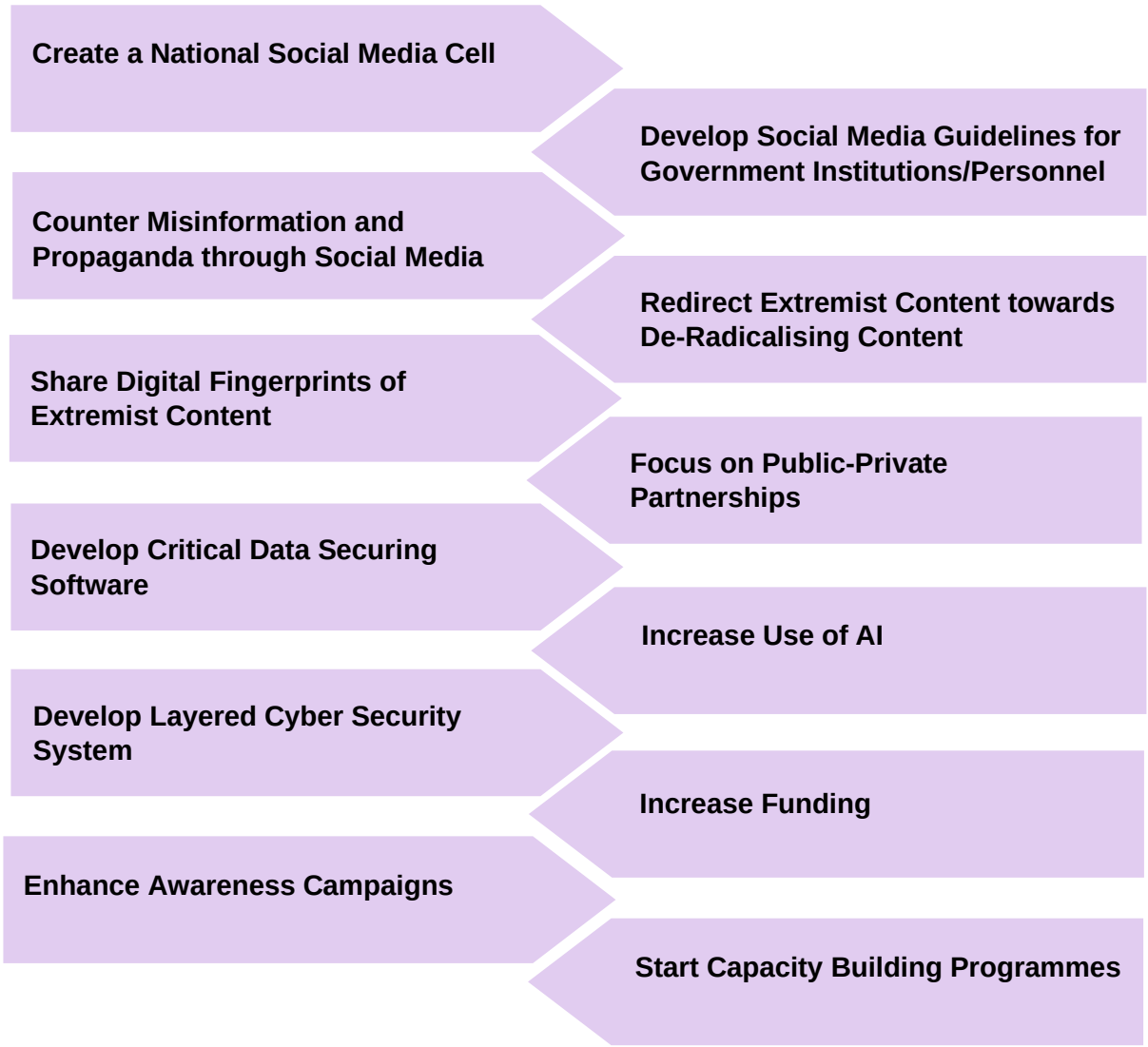
---

43 Solomon, "Social Media the Fastest Growing Vulnerability to the Air Force Mission."
44 Pandalai, "The Social Media Challenge to National Security: Impact and Opportunities."
45 Ibid.

12. Capacity Building Programmes

The framework to deal with social media challenges requires building capacity at local levels since issues begin at this stage. However, development of databases and sharing of information should use existing mechanisms between provincial and federal agencies. For example, intelligence gathered locally on specific physical and cyber-crimes, using social media platforms, should supplement the information in national databases.[46]

Figure 2: Recommendations on Countering Militarisation of Social Media for Government of Pakistan



Source: Authors' own.

[46] Pandalai, "The Social Media Challenge to National Security."

By implementing and practicing the above-mentioned recommendations, along with suggested individual level measures, the social media management capacity of the people, government, and state institutions can be enhanced immensely. Such a multi-pronged approach would not only counter the militarisation of social media but also build a strong and united defence against disinformation/misinformation activities. It will also help the government and state institutions to connect with the public safely in a holistic manner. Moreover, it will educate the general population to not fall prey to anti-state agendas that weaken the cohesion, solidarity, integrity, and security of the state.

Conclusion

The general unreliability of all information presents a special problem in war: all action takes place, so to speak, in a kind of twilight, which like fog or moonlight tends to make things seem grotesque and larger than they really are.

\- CARL VON CLAUSEWITZ

The development and expansion of social media in the last three decades have had an astounding influence on social, economic, and political life across the world. It has provided a new space for trade wars, tainted political campaigns, misinformation, and hybrid military operations. The medium is now being used both by state and non-state actors as a tool of intelligence which is often responsible for undermining the territorial sovereignty and integrity of states. Several countries, as discussed in this paper, are actively involved in exploiting social media, therefore, it is becoming a national security concern.

Since there is no unanimous regulatory and security model at the international level to control the flow and distribution of information on social networking sites, states should take precautionary measures and strengthen their digital security to ensure their own national security. With the state, the responsibility to halt the flow of fake news, misinformation and disinformation also falls on individual citizens. To prevent the militarisation of social media, the paper recommends measures at the individual level as well as for the Government of Pakistan to ensure the security of Pakistan's digital space. The paper concludes that it is a state's responsibility to secure and monitor its social media environment by formulating a dynamic and evolving Social Media Policy for Pakistan.

RESEARCH TEAM & DIRECTORS

Amna Tauhidi is a researcher at the Centre for Aerospace & Security Studies (CASS), Islamabad, Pakistan. She holds an MPhil in Government and Public Policy from National Defence University, Pakistan. Her areas of interest include national, economic and governance challenges.

Maheen Shafeeq is a researcher at the Centre for Aerospace & Security Studies (CASS), Islamabad, Pakistan. She holds a Master's degree in International Relations from The University of Sheffield, UK. Her research interests include emerging technologies and international security.

Air Vice Marshal Faheem Ullah Malik (Retd) is a Director at the Centre of Aerospace & Security Studies (CASS), Islamabad, Pakistan dealing with Warfare & Aerospace. He joined CASS in 2020 after serving more than 32 years as an active duty PAF fighter pilot, retiring as an Air Vice Marshal. His last appointments before joining CASS included Deputy President and Advisor to President National Defence University, Pakistan.

Air Vice Marshal Sohail Malik (Retd) is former Director (Tech and Industry) at the Centre for Aerospace & Security Studies (CASS), Islamabad, Pakistan. He was part of Pakistan Air Force's flagship JF-17 Production Project from its initiation to the completion of aircraft production at the Aircraft Manufacturing Factory of Pakistan Aeronautical Complex.

ABOUT CASS

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

VISION

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

MISSION

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

PROGRAMMES

Foreign Policy

National Security

Emerging Technologies

Aviation Industry & Technology Studies

Economic Affairs & National Development

Warfare & Aerospace

Strategic Defence, Security & Policy

Peace & Conflict Studies

CENTRE FOR AEROSPACE & SECURITY STUDIES, ISLAMABAD
Independence. Analytical Rigour. Foresight

Old Airport Road, Islamabad, Pakistan
+92 051 5405011
www.casstt.com
cass.editor@gmail.com/ cass.thinkers@gmail.com

Centre for Aerospace & Security Studies
cassthinkers
@CassThinkers
cass.thinkers