Weaponization of Social Media: Beyond Clicks and Shares

Colonel (Dr.) Inderjeet Singh
Cyber Sleuths, C-303, Plot 9, Sector 12, Dwarka, New Delhi 110078 India
inderjit.singh@cybersleuths.io

Abstract -- **Weaponization of social media is a disturbing phenomenon with far-reaching implications. Social media platforms have been exploited to spread misinformation, disinformation, fake news, deep-fakes, manipulate public opinion, and incite violence. State and non-state actors, including foreign governments and extremist groups, utilize social media as a tool for achieving their strategic objectives and exerting influence. Weaponized social media has detrimental psychological and societal impacts, such as the erosion of trust, polarization, and proliferation of conspiracy theories. Policy makers, social media companies, and individuals and now the nation states are facing challenges in countering and mitigating the negative effects of weaponization of social media beyond just clicks and shares which these social media platforms were thought to be.**

Ethical and legal considerations arise, including privacy, freedom of speech, and the role of social media platforms in moderating content. Collaboration between governments, technology companies, and civil society is crucial to develop effective strategies and regulations that protect the integrity of the social media space.

Keywords: Social media, Astroturfing, Bots, GenAI, Cyber attacks, Fake news

I. INTRODUCTION

WEAPONIZATION of social media refers to the use of social media platforms such as Facebook, Twitter, Instagram, WhatsApp, Telegram, YouTube etc to spread propaganda, misinformation, disinformation, fake news, deep fakes, manipulate public opinion, and influence political outcomes. Weaponization of social media platforms is a growing concern because of its potential to undermine democratic processes, erode trust in institutions, promote extremist ideologies and exacerbate social and political polarization.

Social media has become a powerful tool for individuals, non-nation state and governments to spread propaganda, manipulate public opinion, and influence elections because of its ability to reach a large audience quickly and easily. It is important to be aware of these tactics and to take steps to combat their use through critical thinking, fact-checking, and responsible use of social media platforms.

Reasons why we should be worried about the weaponization of social media are:

- *Disinformation and Propaganda*: Social media platforms can be used to spread false information and propaganda, which can influence public opinion and political decisions.
- *Manipulation and Psychological Warfare:* Social media can be used to manipulate individuals and groups, creating psychological warfare and social unrest.
- *Amplification of Hate Speech and Extremism*: Social media can amplify hate speech and extremist ideologies, leading to violence and social unrest.
- *Erosion of Privacy*: Social media platforms can collect and exploit personal data, compromising individual privacy and security.
- *Interference in Elections and Political Processes:* Social media can be used to interfere in elections and political processes, undermining democracy and political stability.
- *Cyber Attacks and Cyber Warfare:* Social media can be used to launch cyber attacks and engage in cyber warfare, compromising critical infrastructure and national security.
- *Polarization and Social Division:* Social media can exacerbate social divisions and political polarization, leading to social unrest and conflict.
- *Loss of Trust in Institutions:* Social media can be used to undermine trust in institutions, such as the media, government, and political systems.
- *Psychological Impact on Individuals:* Social media can have a significant psychological impact on individuals, including anxiety, depression and loneliness.

II. HISTORICAL CONTEXT

Social media platforms such as Facebook, Twitter, WhatsApp, YouTube etc. have been weaponized over the years in various ways, with several notable examples of its use for propaganda and manipulation of public opinion. Social media has been used

in various instances to sow discord and influence outcomes, often with the intent of achieving political or ideological goals. Historical events that illustrate the weaponization of social media are:

- *2016 and 2020 US Presidential Election*: The US Presidential election in 2016 and 2020 was a turning point in the weaponization of social media platforms with false information and propaganda being spread on social media platforms such as Facebook, Twitter and YouTube etc. Russian operatives were found to have used social media platforms to spread false information and sow discord among American voters.

- *Brexit Referendum*: The 2016 Brexit referendum in the UK was also influenced by social media manipulation. False information and propaganda were spread on social media platforms such as Facebook, which allowed political advertising to be targeted to specific demographics.

- *Indian Elections:* In recent years, social media has played a significant role in Indian elections, with political parties using social media platforms to target specific demographics with tailored messaging. False information and propaganda have also been spread on social media platforms in an attempt to influence public opinion.

III. DIFFERENT METHODS

Weaponization of social media such as Facebook, Twitter, Instagram, WhatsApp, Telegram, YouTube etc. involves the use of various tactics to manipulate public opinion, promote a particular agenda, and sow discord. These tactics can have serious consequences for democracy, human rights, and social cohesion, highlighting the need for responsible use of social media platforms and measures to combat disinformation and propaganda.

There are several methods that can be used to weaponize social media, including:

- *Creation and Dissemination of False Information:* False information is often used to spread conspiracy theories, misinformation, and propaganda on social media platforms.

- *Propaganda***:** Propaganda is a systematic effort to influence or manipulate public opinion through information, often with a political or ideological agenda. On social media, propaganda can be spread through targeted messaging, the use of persuasive language, images, and videos.

- *Social Media Bots:* Social media bots are automated accounts that can be used to amplify certain messages or spread false information. Bots can be programmed to create the impression of widespread support for a particular cause, or to flood social media platforms with false information to create confusion and sow discord.

- *Trolling:* Trolling involves the deliberate provocation of others on social media, often with the intent of causing chaos or promoting a particular agenda. Trolling can be used to disrupt civil discourse, promote division, and spread hate speech.

- *Cyber attacks:* Cyberattacks can also be used to weaponize social media. This can involve hacking into social media accounts to spread false information or cause chaos, or using malware to spread propaganda or steal information.

- *Astroturfing:* Astroturfing involves the creation of fake grassroots campaigns to promote a particular agenda. Astroturfing can be used to influence public opinion, promote a particular product or brand, or to discredit opposing views.

- *Bots:* Bots are automated accounts that can be used to amplify certain messages or spread false information. Bots can be used to create the illusion of widespread support for a particular ideology or viewpoint.

- *Deep-fake Videos***:** Deep-fake videos can manipulate audio and visual content to create a convincing and false representation of events. Deep-fake videos can be used to spread false information or discredit individuals or groups.

- *Fake-news***:** Fake-news is spread of false or misleading information through traditional media or social media platforms. Fake-news can be used to promote a particular agenda or ideology, discredit opposing views, or manipulate public opinion.

- *Memes:* Memes are humorous images, videos, or text that are shared widely on social media platforms. Memes can be used to spread propaganda or disinformation, often with the intent of influencing public opinion or promoting extremist ideologies.

- *Hashtags:* Hashtags are used to categorize content on social media platforms. Hashtags can be used to promote a particular agenda or ideology, and can be used to create the impression of widespread support for a particular cause.

- *Influence Campaigns***:** Influence campaigns involve the use of paid influencers, or other tactics to promote a particular agenda or ideology. Influence campaigns can be used to influence public opinion, promote a particular product or brand, or to discredit opposing views.

IV. USE OF GENAI

Weaponization of social media has reached a new level of sophistication with the advent of Generative AI (GenAI). This powerful technology has enabled the rapid creation and dissemination of highly convincing and manipulative content, including deep-fakes, AI-generated bots, and personalized disinformation. As a result, the integrity of global political discourse, social cohesion, and democracy are under threat like never before. The spread of disinformation and propaganda has become increasingly difficult to detect and counter, with far-reaching implications for political decision-making, public opinion, and the very fabric of our societies.

- *Deep-fakes*: GenAI-generated deep-fakes can create convincing videos, audio, or images that manipulate public opinion, damage reputations, or spread disinformation. For instance, a deep-fake video could make a political leader appear to say something they never said, leading to widespread confusion and mistrust.

- *AI-generated Bots:* GenAI-created bots can amplify disinformation and propaganda on social media, making it seem like a majority of people hold a particular viewpoint when, in reality, it's just a coordinated bot attack.

- *Personalized Disinformation*: GenAI can use personal data and psychological profiling to create targeted, persuasive content that exploits individual vulnerabilities and biases.

- *AI-written Propaganda*: GenAI can generate convincing, well-researched propaganda articles, blog posts, and social media posts that spread disinformation and manipulate public opinion.

- *Synthetic Media:* GenAI-created synthetic media, such as fake news articles, videos, and podcasts, can blur the lines between reality and fiction, further eroding trust in media and institutions.

- *Influence Operations*: GenAI can amplify influence operations by generating content that resonates with specific audiences, manipulating public opinion, and shaping political discourse.

- *Psychological Operations:* GenAI can use psychological profiling and personalized content to manipulate individuals' emotions, beliefs, and behaviours, potentially even influencing political decisions.

- *Disinformation Campaigns:* GenAI enables the rapid creation and dissemination of disinformation campaigns, making it challenging for fact-checkers and social media platforms to keep pace.

- *AI-generated Hashtags*: GenAI-generated trending hashtags and coordinated social media campaigns can amplify disinformation and propaganda, making it appear more popular and widespread than it actually is.

- *Evasion of Detection*: GenAI can help malicious actors evade detection by generating content that circumvents existing AI-powered moderation tools and fact-checking algorithms.

V. DAMAGES CAUSED

Weaponization of social media can have serious consequences for democratic processes, social cohesion, and human rights. Social media can be used to manipulate public opinion and to promote extremist ideologies, and to take steps to combat the spread of disinformation and hate speech. This includes efforts to improve media literacy, strengthen democratic institutions, and promote civil discourse.

The weaponization of social media poses a significant threat to individuals, society, politics, economics, national security, and global stability.

Individual level

- Manipulation of personal opinions and beliefs, leading to
  - Emotional distress
  - Financial losses (*e.g.,* investing in fraudulent schemes)
  - Reputational damage (*e.g.,* online harassment)
- Invasion of privacy and identity theft
- Psychological manipulation and influence operations

Social level

- Erosion of trust in
  - Institutions (government, media, education)
  - Social cohesion and community bonds
  - Democratic processes and political legitimacy
- Social unrest and polarization
- Hate speech and violence against marginalized groups
- Disinformation and propaganda leading to social chaos

Political level

- Interference in
  - Elections (*e.g.*, voter suppression, disinformation campaigns)
  - Political decisions and policy-making
  - Political advertising and campaign finance
- Undemocratic outcomes and political instability
- Geopolitical tensions and conflicts

Economic level

- Disruption of
  - Markets (*e.g.* flash crashes, market manipulation)

  - Financial systems (*e.g.*, fraud, cyber attacks)
  - Businesses and organizations (*e.g.*, reputational damage, IP theft)
- Financial losses and economic instability
- Global financial crises and trade wars

National security level
- Threats to
  - Critical infrastructure (*e.g.*, energy, transportation)
  - Intelligence operations and national security
  - Military communications and operations
- Compromised national security and geopolitical instability
- Cyber warfare and digital espionage

Global level
- Undermining of
  - International relations and diplomacy
  - Global governance and multilateral institutions
  - International law and norms
- Collapse of the global order and increased conflict
- Global economic and political instability.

VI. GOVERNMENT RESPONSES

Weaponization of social media is a problem that poses significant challenges to the functioning of democracies and the well-being of societies around the world. Governments are responding to the weaponization of social media through a range of measures aimed at promoting transparency, accountability, and responsible social media use. These measures reflect a growing recognition of the significant risks associated with the weaponization of social media and the need for collective action to address these risks.

Some of the strategies that governments are using to combat disinformation and the manipulation of public opinion on social media platforms are:

- *Legislations and Regulations of Social Media Platforms***:** Many governments are looking to regulate social media platforms to combat disinformation and hate speech.

- *Increased Funding for Research***:** Governments are also investing in research on the impact of social media on society.

- *Collaboration with Social Media Companies:* Some governments are working with social media companies to combat disinformation and hate speech.

- *Diplomacy and International Cooperation:* Governments are also working together at the international level to combat the weaponization of social media.

- *Support for Independent Media*: Governments may support independent media outlets to counter disinformation and propaganda.

- *Cyber-security Measures*: Governments are investing in cyber-security measures to prevent hacking, data breaches, and other forms of cyber attacks that can be used to manipulate public opinion on social media.

- *Education and Awareness Initiatives*: Governments are also investing in education and awareness initiatives to help individuals better understand the risks associated with social media and to promote responsible social media use.

- *Legal Action:* Some governments are taking legal action against individuals and organizations that engage in the weaponization of social media.

VII. SOCIAL MEDIA COMPANIES RESPONSE TO WEAPONISATION OF PLATFORMS

Social media companies are responding to the problem of weaponization by implementing various measures, such as fact-checking, labelling false information, and increasing transparency around political advertising. However, there is still much more that needs to be done. Social media companies can further invest in content moderation, detection of bots and fake accounts, and cooperation with governments and civil society organizations.

Social media companies are responding in following manner:

- *Fact-checking*: Social media companies have implemented fact-checking mechanisms to identify false or misleading information.

- *Labelling False Information*: In addition to fact-checking, social media companies are also labelling false information to inform users about the veracity of the content.

- *Increased Transparency Around Political Advertising*: Social media companies are also increasing transparency around political advertising on their platforms.

- *Removal of Fake Accounts and Bot Networks:* Social media companies are removing fake accounts and bot networks that are used to spread false information or manipulate public opinion.

- *Partnerships with Third-Party Organizations:* Social media companies are partnering with third-party organizations, such as fact-checkers, academics, and civil society groups, to address disinformation on their platforms.

- *Improvements to Algorithms:* Social media companies are also making changes to their algorithms to reduce the spread of false information and propaganda.

- *Promoting Media Literacy:* Social media companies are promoting media literacy to help users better identify false information and propaganda.

VIII. CONCLUSION

Weaponization of social media is a growing problem that poses a significant threat to democratic processes and the social fabric of our society. To address this issue, a multi-faceted approach is necessary that involves cooperation between governments, social media companies, civil society and individual users.

Firstly, social media platforms need to take more responsibility for the content that is shared on their platforms. Secondly, governments should enact laws and regulations that hold social media platforms accountable for the content they host. Thirdly, Individual users of social media have a responsibility to be more aware of the content they consume and share.

REFERENCES

[1] J. M. Berger, "Weaponizing Social Media. The ISIS Case", Brookings Institution, 2015.

[2] S. Bradshaw and P.N. Howard, *The Weaponization of Social Media. Towards a Conceptual Framework for State and Non-State Actors,* Cambridge University Press, 2018.

[3] Z. Tufekci, "Weaponizing Social Media. The Rise of Personalized Political Communication in the 2016 US Presidential Election", *University of North Carolina at Chapel Hill*, 2018.

[4] S.K. Sharma and S. Gupta, "The Weaponization of Social Media. Platforms as Target, Amplifier, and Beacon of Global Conflict", *Int. J. Communication*, 2020.

[5] G. Weimann, "The Weaponization of Social Media. Exploring the Linkages between Information Operations and Social Media Manipulation", *J. Terrorism Research*, 2019.

[6] A. Smith, "The Dark Side of Social Media. The Weaponization of Social Media Spaces by Authoritarian Regimes", *J. Int. Affairs*, 2017.

[7] E. Gonzalez and H. Lee, "Weaponizing Social Media. A Comparative Analysis of Russian and Chinese Strategies", *Strategic Studies Quarterly*, 2019.

[8] T. Rid and B. Buchanan, "Weaponization of Social Media. Cyber Influence Operations during the 2018 US Mid-term Elections", *J. Cybersecurity*, 2020.

[9] M. Clarke and A. Bennett, "Countering the Weaponization of Social Media. Strategies and Challenges", *J. Strategic Security*, 2018.

[10] P. Johnson and R. Smith, "The Weaponization of Social Media. Implications for National Security", *National Defense University Press*, 2016.

[11] M. Rahman and S. Ali, "The Role of Social Media in the Weaponization of Disinformation. A Case Study of the Rohingya Crisis", *Conflict Studies Quarterly*, 2020.

[12] L. Davis and K. Wilson, "The Weaponization of Social Media. Challenges for Democratic Societies", *Georgetown J. Int. Affairs*, 2019.

[13] H. Chen and C. Chang, "The Weaponization of Social Media. Cyber Warfare in the Information Age", *J. Information Warfare*, 2017.

[14] T. Nguyen and H. Tran, "Social Media as a Battlefield. The Weaponization of Information in Hybrid Warfare", *Defence Studies*, 2018.

[15] J. Smith and K. Jones, "The Weaponization of Social Media. Combating Misinformation in the Digital Age", *Int. J. Communication Ethics*, 2021.

Colonel (Dr.) Inderjeet Singh is Founder & Chief Cyber Officer, CyberSleuths. With over 30+ years of experience as an Information Systems professional, he has served in the Indian Army, is an alumnus of Indian Institute of Technology, Kharagpur and Symbiosis Institute of Management, Pune, and holds a Doctorate of Science in Cyber Security. He is working on Security Operation Centre, Threat Intelligence, Attack Surface Management, Dark-net Forensics, Crypto-currency forensics, Operation Technology (OT) Security, Asset Management Solutions and many more. He has spoken at TEDx events twice. He has provided instruction and guidance on Cybercrime Prevention, Cyber-terrorism, Dark-net forensics, and Crypto-currency forensics to Law Enforcement Agencies, Colleges, and the general public. Additionally, he emphasizes the value of "Cyber Citizenship" among the populace.

He is a permanent representative to United Nations Office at Geneva as part of International Organization for Educational Development, UN ECOSOC. He authored books and research papers and was consistently awarded for his work.