International Journal of
Advanced Science Computing and Engineering

Journal Homepage www.ijasce.org/index.php/ijasce

The Architecture of Digital Deception: Mapping Fake News Typologies, Bot Behaviors, and Platform Vulnerabilities

Muhammad Fikri Afansyah [a,*], Haslinda Sutan Ahmad Nawi [a]

[a] School of Graduate Studies, Management and Science University, Shah Alam, Malaysia
[b] Faculty of Information Sciences and Engineering, Management and Science University, Shah Alam, Malaysia
Corresponding author: [*]mfikriafansyah.msu@gmail.com

***Abstract*—The emergence of social media has radically changed the nature of information production, dissemination, and consumption. Alongside its advantages, the diffusion of misinformation has become a major threat to debate, democratic processes, and social cohesion. The following paper presents an extensive review of typologies of fake news, drawing on existing scholarship that categorizes fake news as satire, propaganda, disinformation, misinformation, manipulation, rumor, crowdturfing, hate speech, spam, trolls, and cyberbullying. The two categories are discussed with respect to their purpose, precision, and influence on users. The role of bots and computational propaganda, which automate and amplify the spread of misleading content on the internet, particularly during sensitive periods when politics is salient, is also examined. The paper identifies several shortcomings of existing platform moderation systems, which largely fail to block the real-time dissemination of dangerous content. In a reaction, the paper highlights the important work of information professionals, i.e., journalists, teachers, educators, librarians, and specialists in digital media, being able to reduce the dissemination of false information. They are tasked with fact-checking, source validation, media literacy, and citizen empowerment in the assessment of online information. In addition, the paper promotes the development of more resilient AI-based detection mechanisms that can respond quickly to the proliferation of harmful content. Finally, the research is expected to foster a more aware and less vulnerable world, prepared to meet the challenges of the digital information era through technological devices and human knowledge.**

***Keywords*—Digital deception; fake news; misinformation; bots; computational propaganda; platform vulnerabilities.**

Manuscript received 8 Aug. 2025; revised 17 Oct. 2025; accepted 28 Nov. 2025. Date of publication 30 Dec. 2025.

I. INTRODUCTION

On occasion, fake news manifests as news fabrication: the publication of unverified and inaccurate material in the form of conventional news stories. Since fake news is often created solely to mislead readers, readers face a more difficult task in assessing the veracity and credibility of such stories, as the misinformation is often highly similar to legitimate news and is often published by non-news outlets. Social media is the most preferred platform when it comes to the spread of false news, and fake news is often mixed up with genuine news because of the nature of the platforms it engages in, using the ecosystem of real-time propaganda on social media, as well as the style of composition found in its articles. In such a virtual ecosystem, bots provide an information network based on fake news and use algorithms to identify readers most vulnerable to false information, subjecting them to increasing doses of it [1].

As readers seek to corroborate the news, they may turn to another website that reports the same fake news, thereby reinforcing their belief in its content. This trend of pushing creates the impression among readers that a significant number of individuals are simultaneously reading fake news. The type of fake news is manipulation, i.e., the transformation of images or videos, which is primarily the case. This type of fake news is usually produced through the manipulation, splicing, compositing, and alteration of films and images in order to spread misleading information.

Most social media platforms strike a balance between free speech and content moderation when fake news goes live, allowing the content to be released while restricting its distribution and access [2]. Social media platforms such as Facebook and Twitter have implemented reporting tools to screen and limit the reach of such inappropriate content. When a user encounters harmful comments in a piece of fake news while using the software, they can report the article to the platform's censors. The censors will review the article to determine whether it is accurate and act accordingly.

Nevertheless, even consumers who currently report this erroneous information may be influenced by the censoring-review process. This is because other individuals can still read the content even when it is not considered dangerous, and the reporting system is time-consuming. In this case, social media platforms require a more robust automated blocking system to ensure compliance with tweets. Thus, offensive comments will be reduced, and the content push can be lower initially [3].

The study examines how information and media professionals can address the issues of false news and misinformation that have become prevalent on social media. With the rise of misinformation and fake news in the digital era, the role of information professionals is increasingly important. In this paper, the point is that practitioners should be equipped with the skills to critically evaluate information and to distinguish reliable from unreliable sources. The purpose of this study is to contribute to the ongoing fight against misinformation and to foster a more knowledgeable and digitally competent citizenry.

II. Materials and Methods

Tandoc et al. [9] identified six categories of fake news: news parody, news satire, fabrication, manipulation, propaganda, and advertising. All of them can be characterized by the factors of facticity and intention: some exhibit high facticity and deceptive intentions, whereas others exhibit low facticity and deceptive intentions [4]. Communication scholars identify three typologies that are alike. There are seven types of fake news: satire or parody, inaccurate information, imposter, fabricated information, false connection, false context, and pixel-edited information [5].

According to Haque [6], the four types of fake news include disinformation, misinformation, hoaxes, and rumors. Ouedraogo classified fake news on social media into six categories: malicious false news, neutral false news, satirical news, disinformation, misinformation, and rumor [7]. These two studies, like the four other studies, are less concerned with the thematic issues of fake news. According to Khan et al. [8], fake news comprises five different types of content: clickbait, satire and parody, propaganda or sloppy news, and biased or partisan news

The counterfeit reflects in this typology. It employs the news typology proposed by Tandoc et al. [9] and provides a more journalistic definition of fake news. According to Nielsen and Graves, they examined five categories of fake news (i.e., satire, poor journalism, propaganda, advertising, and false news). Two major weaknesses of these typologies are that they are highly proximate and share similar types (e.g., satire and false news) to identify fake news, and, furthermore, they are more preoccupied with claims than with specifics. The topics of fake news. Two additional studies suggested typologies of fake news, establishing links between fake news and rumor, misinformation, and disinformation [10]. To gain a clearer understanding of fake News on social media, it is recommended to classify the types of Fake news as follows, although the division is not exhaustive.

1) Inadvertently Disseminated Disinformation: Not all misinformation is conveyed with the intention of tagging on to the recipients. Benign and regular users may also contribute to its spread simply because they trust sources of information, such as friends, family, colleagues, or even influential users within the social network. They never want to lie, but they do so to inform their friends in society or on social networks about a particular issue or situation. This is evidenced by the widespread misinformation about Ebola [11].

2) Intentionally Spread Misinformation: Certain misinformation is even purposefully disseminated so as to mislead its recipients, and that was the reason that induced the heated debate regarding misinformation and fake news that occurred recently. The popularization is typically followed by writers and groups of coordinated spreaders, who are likely to have a clear goal and agenda in compiling and promoting the misinformation. The most common cases of intentionally spread misinformation are conspiracy theories, rumors, and fake news that were widely discussed in 2016, around the time of the Presidential Elections. Such fake-news creators as Paul Horner have taken responsibility for multiple pieces of fake news that went viral in 2017 [12].

3) Urban Legend: Urban legend is something like fake information that is willingly propagated and connected to fictional tales concerning local phenomena. It may sometimes serve as entertainment.

4) Fake News: Fake news is misinformation in the form of news that is deliberately distributed. Current events indicate that misinformation, when disseminated through news and social media, may be treated as propaganda and can go viral [13], [14].

5) Unverified Information: Our definition also entails unverified information, which at times may be valid and accurate. Information that has not yet been confirmed is unconfirmed, and information confirmed as false or inaccurate constitutes misinformation. It can produce effects similar to those of other forms of misinformation, including fear, hatred, and astonishment.

6) Rumor: Rumor refers to unconfirmed information that may be real (true rumor). The deaths of numerous ducks in Guangxi, China, from avian influenza is an instance of the real rumor [15]. It was once a persistent rumor until the government confirmed it [16]. Another similar case of avian influenza, which was found to be untrue, was that some individuals had been infected after consuming well-cooked chicken meat [17].

7) Crowdturfing: The concept of crowdturfing derives from astroturfing, which implies that the campaign conceals those behind it. Sponsors, in order to make it appear as if they were brought in by grassroots participants. Crowdturfing, also known as crowd-sourced astroturfing, is the practice of acquiring online support. As with unverified information or rumors, the information advertised through crowd-turfing may be true; however, the popularity it receives from crowdsourcing workers is false and unjustified. There are instances of misinformation with undesirable consequences, and such cases are often attributable to crowdturfing. It is straightforward to find crowdsourcing workers online through platforms such as Zhubajie, Sandaha, and Fiverr. It has been alleged that crowd-turfing has been used to target specific politicians [18].

8) Spam: Spam refers to unsolicited data, which unduly concentrates on its users. It has been observed across various platforms, including instant messaging, email, and social media.

9) Troll: The other type of misinformation that we are concentrating on is the troll. A troll is intended to disturb and dispute one group of people. Unlike other forms of misinformation that attempt to persuade their audiences, trolling aims to heighten friction among ideas and, ultimately, to foster hatred and widen the rift. Being trolled is one example of how the likelihood that a median voter would cast their vote is brought to life. In 2016, the troll army that had purportedly been placed under orders by the Russian government was found to be engaged in trolling at crucial election times [19].

10) Hate speech: Hate speech is an abusive script that presides over social media that is both prejudiced and threatening to some groups of people. The interactions between the 2016 presidential elections and hate speech against certain groups that are legally protected became very dynamic, and the day of the elections proved to be the day when hate speech was at its climax [20].

11) Cyberbullying: Cyberbullying is the type of bullying occurring online, most often in social media, which can include any kind of misinformation, including rumors and hate speech. Social network use, in itself, can be a sign of societal problems. Investigating whether global social media usage correlates with a country-by-country assessment of political stability found a strong negative correlation, with correlations in developing countries stronger [21]. Online social networks (OSNs) have become a primary source of news, and while they enable instant communication, the spread of misinformation remains a complex issue [22]. Trust in social networks as an information source is increasing [23], [24].

The mass-scale spread of political messages, misinformation, and malware links requires little to no effort, involves no major figures, and entails no expensive traditional advertising campaigns. Studies show that bots on social media platforms have played a crucial role in shaping recent political events. Computational propaganda has become a primary weapon among political warriors, and bots are now the go-to technology. In contrast to traditional propaganda, computational propaganda relies on the decentralized dissemination of content and anonymity, making it more difficult to perceive and control [25]. It also affects public health, and bots have already been found spreading health-related misinformation and advertisements [26]. The most widely researched type of malicious bots is continuously evolving [27]. A botmaster typically operates these bots and controls their activities.

Mendoza et al. [28] also discussed the problem of differentiating between trustworthy and unreliable sources of information in the new social media. When discussing the increasing access to information, authors also note that people's knowledge of important issues has not evolved as quickly, largely due to the widespread circulation of rumors, conspiracy theories, and other forms of misinformation across social platforms. The fractured and fragmented news media have also given rise to the presence of "competing and often chaotic voices," and social media have thus been used to spread political agendas and fake news, and social media activity has been used to amplify such misinformation and propaganda, resulting in incivility and polarization.

A fact is a very assertive statement by a person of prominence who is also powerful enough to make it in as far as social media is concerned, and because it is a fact, it is therefore right. This, however, also allows the journalist to avoid fact-checking the statement by presenting it as something that cannot be verified. Thus, the importance of information verification in the work process can be overlooked in favor of prioritizing newsworthiness. Very similar responses were given by respondents regarding official institutions (e.g., state offices, the government). In the third developed episode, the respondents' information was presented in the form of a tweet and a blog post by the Estonian Veterinary and Food Board. This Twitter account had a single follower, although the tweet received seventy-eight retweets, indicating the extent of information sharing on social media. The respondents who detected the discrepancy would have continued to search for the original tweet and to confirm the information with the Board. The manipulated content would have been recognized [29].

Specifically, the inadequacy of social media competencies manifested as a lack of awareness that official accounts may be hacked or contain fake or impostor information. It means that journalists have the skills about social media as consumers, but they might lack the expertise to use them during fact-checking [30].

III. Results and Discussion

Studying the various types of fake news and their spread across social media demonstrates an intricate issue that concerns both technological and human-related factors. Despite enabling user-generated content, social media has also been a breeding ground for disinformation, whether knowingly or unknowingly. Different typologies, such as satire and manipulated content, hate speech, and crowdturfing, demonstrate that misinformation is not one-dimensional but exists in various forms and for different purposes. This complexity tends to make detection and mitigation difficult, especially in real time.

Another important conclusion is that automated systems and bots play a central role in the spread of misinformation. These bots also tend to behave like humans, can easily integrate into online communities, and can spread misleading information effectively. These bots also cause polarization, incivility, and confusion, especially during elections and public health crises.

Facebook and Twitter have established platforms and frameworks for moderation and reporting that are largely reactive and manual. Existing technologies with the potential to intervene in real time include automated detection systems that use artificial intelligence, which are still under development. Information professionals (such as librarians, journalists, and educators) are essential to resolving this crisis. They have the potential to evaluate sources, fact-check claims, and teach media literacy, thereby completing the technological solution to the problem and being more user-friendly.

IV. Conclusion

In sum, fake news and misinformation that continue to spread on social media pose a dynamic and multifaceted problem that affects political stability, public perception, and social trust. A comprehensive review of typologies (including disinformation, satire, manipulated content, rumor, and crowdturfing) is employed, as this research paper examines false information across these typologies. Additional complications arising from fake content are exacerbated by the involvement of bots and algorithmic amplification, which further disseminate misleading information, and by the fact that human moderation teams would address similar content on social media platforms less frequently.

A set of steps must be taken to address this issue, rather than relying solely on technology. Although artificial intelligence and automation will be helpful in detecting and filtering misinformation, the role played by the human agent, especially information professionals, cannot be replaced. Librarians, journalists, educators, and those involved in the digital media landscape need to be equipped with critical media literacy and empowered to train the public in the verification and assessment of online media.

Ultimately, the battle against misinformation requires an inclusive strategy that combines public awareness, robust policymaking, and the effective use of digital technologies. By combining human and intelligent-system expertise, societies can create a better, smarter, more robust, and more morally accountable digital world. Such efforts are needed to maintain high standards of information integrity in the digital era and to protect the discourse of democracy against the menace of fake news.

References

[1] J. Albright, "The #Election2016 micro-propaganda machine," *Medium*, 2020. [Online]. Available: https://medium.com/@d1gi/the-election2016micro-propaganda-machine-383449cc1fba

[2] G. Di Domenico, D. Nunan, J. Sit, and V. Pitardi, "Free but fake speech: When giving primacy to the source decreases misinformation sharing on social media," *Psychol. Mark.*, vol. 38, no. 10, pp. 1700–1711, 2021, doi: 10.1002/mar.21479.

[3] S. Ullmann and M. Tomalin, "Quarantining online hate speech: Technical and ethical perspectives," *Ethics Inf. Technol.*, vol. 22, no. 1, pp. 69–80, 2020, doi: 10.1007/s10676-019-09516-z.

[4] E. C. Tandoc Jr., Z. W. Lim, and R. Ling, "Defining 'fake news': A typology of scholarly definitions," Digit. Journal., vol. 6, no. 2, pp. 137–153, 2018, doi: 10.1080/21670811.2017.1360143.

[5] C. Wardle, "Fake news. It's complicated," *First Draft*, Feb. 16, 2017. [Online]. Available: https://firstdraftnews.org/articles/fake-news-complicated/.

[6] M. Haque, "'Fake news' in social media: Conceptualizing, detection and finding ways of prevention," *Nirikkha*, vol. 223, pp. 9–18, Jun. 2019.

[7] N. Ouedraogo, "Social media literacy in crisis context: Fake news consumption during COVID-19 lockdown," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3641230.

[8] S. A. Khan, M. H. Alkawaz, and H. M. Zangana, "The use and abuse of social media for spreading fake news," in Proc. IEEE Int. Conf. Autom. Control Intell. Syst. (I2CACIS), Shah Alam, Malaysia, Jun. 2019, pp. 324–329, doi: 10.1109/I2CACIS.2019.8825081.

[9] E. C. Tandoc Jr., D. Lim, and R. Ling, "Diffusion of disinformation: How social media users respond to fake news and why," *Journalism*, vol. 21, no. 3, pp. 381–398, 2020, doi: 10.1177/1464884919868325.

[10] R. K. Nielsen and L. Graves, "Audience perspectives on fake news," Reuters Inst. Study Journal., Oxford, U.K., Factsheet, Oct. 2017. [Online]. Available: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Nielsen%26Graves_factsheet_1710v3_FINAL_download.pdf.

[11] J. Bollen, H. Mao, and A. Pepe, "Determining the public mood state by analysis of microblogging posts," in *Proc. 12th Int. Conf. Artif. Life (ALIFE)*, Odense, Denmark, Aug. 2010, pp. 667–668.

[12] C. Castillo, M. Mendoza, and B. Poblete, "Information credibility on Twitter," in Proc. 20th Int. Conf. World Wide Web (WWW), Hyderabad, India, Mar. 2011, pp. 675–684, doi:10.1145/1963405.1963500.

[13] K. Sharma, F. Qian, H. Jiang, N. Ruchansky, M. Zhang, and Y. Liu, "Combating fake news: A survey on identification and mitigation techniques," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 3, pp. 1–42, May 2019, doi: 10.1145/3305260.

[14] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, "Fake news detection on social media: A data mining perspective," *ACM SIGKDD Explor. Newslett.*, vol. 19, no. 1, pp. 22–36, Jun. 2017, doi:10.1145/3137597.3137600.

[15] C. Castillo, M. Mendoza, and B. Poblete, "Predicting information credibility in time-sensitive social media," *Internet Res.*, vol. 23, no. 5, pp. 560–588, 2013, doi: 10.1108/IntR-05-2012-0095.

[16] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Who is tweeting on Twitter: Human, bot, or cyborg?," in Proc. 26th Annu. Comput. Secur. Appl. Conf. (ACSAC), Austin, TX, USA, Dec. 2010, pp. 21–30, doi:10.1145/1920261.1920265.

[17] A. Friggeri, L. A. Adamic, D. Eckles, and J. Cheng, "Rumor cascades," in *Proc. 8th Int. AAAI Conf. Web Social Media (ICWSM)*, Ann Arbor, MI, USA, Jun. 2014, pp. 101–110, doi: 10.1609/icwsm.v8i1.14559.

[18] J. Gao *et al.*, "On community outliers and their efficient detection in information networks," in *Proc. 16th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining (KDD)*, Washington, DC, USA, Jul. 2010, pp. 813–822, doi: 10.1145/1835804.1835907.

[19] G. B. Guacho, S. Abdali, N. Shah, and E. E. Papalexakis, "Semi-supervised content-based detection of misinformation via tensor embeddings," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, Barcelona, Spain, Aug. 2018, pp. 322–325, doi:10.1109/ASONAM.2018.8508241.

[20] A. Gupta and P. Kumaraguru, "Credibility ranking of tweets during high impact events," in *Proc. 1st Workshop Privacy Secur. Online Social Media*, Lyon, France, Apr. 2012, p. 2, doi:10.1145/2185354.2185356.

[21] T. A. Nguyen, T. C. Bui, M. Dudareva, and V. Bubnov, "Correlation between the world's social media usage and political stability in a country," *Public Organ. Rev.*, vol. 24, no. 1, pp. 217–233, 2024, doi:10.1007/s11115-023-00744-y.

[22] E. Aïmeur, S. Amri, and G. Brassard, "Fake news, disinformation and misinformation in social media: A review," *Social Netw. Anal. Mining*, vol. 13, no. 1, p. 30, 2023, doi: 10.1007/s13278-023-01028-5.

[23] M. Kolomeets, A. Chechulin, and I. Kotenko, "Bot detection by friends graph in social networks," J. Wireless Mobile Netw. Ubiquitous Comput. Dependable Appl., vol. 12, no. 2, pp. 141–159, 2021, doi:10.22667/JOWUA.2021.06.30.141.

[24] M. Aljabri *et al.*, "Machine learning-based social media bot detection: A comprehensive literature review," *Social Netw. Anal. Mining*, vol. 13, no. 1, p. 72, 2023, doi: 10.1007/s13278-022-01020-5.

[25] M. Pote, "Computational propaganda theory and bot detection system: Critical literature review," *arXiv:2404.05240*, 2024. [Online]. Available: https://arxiv.org/abs/2404.05240.

[26] M. Orabi, D. Mouheb, Z. Al Aghbari, and I. Kamel, "Detection of bots in social media: A systematic review," *Inf. Process. Manag.*, vol. 57, no. 4, p. 102250, 2020, doi: 10.1016/j.ipm.2020.102250.

[27] S. Cresci, M. Petrocchi, A. Spognardi, and S. Tognazzi, "On the capability of evolved spambots to evade detection via genetic engineering," *Online Social Netw. Media*, vol. 9, pp. 1–16, 2019, doi:10.1016/j.osnem.2018.10.005.

[28] M. Mendoza, E. Providel, M. Santos, and S. Valenzuela, "Detection and impact estimation of social bots in the Chilean Twitter network," Sci. Rep., vol. 14, no. 1, p. 6525, 2024, doi: 10.1038/s41598-024-57227-3.

[29] J. Wihbey, "Journalists' use of knowledge in an online world," *Journalism Pract.*, vol. 11, no. 10, pp. 1267–1282, 2017, doi:10.1080/17512786.2016.1255149.

[30] X. Zhang and W. Li, "From social media with news: Journalists' social media use for sourcing and verification," *Journalism Pract.*, vol. 14, no. 10, pp. 1193–1210, 2020, doi: 10.1080/17512786.2019.1665523.