Selected Papers of #AoIR2025:
The 26th Annual Conference of the
Association of Internet Researchers
Niterói, Brazil / 15 – 18 Oct 2025

THROWING SPAGHETTI, SEEING WHAT STICKS: ITERATIVE DECEPTION IN DIGITAL STRATEGIC INFORMATION OPERATIONS

Giada Marino
University of Urbino Carlo Bo, Italy

Fabio Giglietto
University of Urbino Carlo Bo, Italy

Anwesha Chakraborty
University of Urbino Carlo Bo, Italy

Massimo Terenzi
University of Urbino Carlo Bo, Italy

Samuel Olaniran
University of Witwatersrand, South Africa

Introduction and Theoretical Background

This study investigates the strategic exploitation of social media platforms, particularly Facebook, for information operations that extend beyond traditional disinformation campaigns, focusing on networks of potentially misleading accounts surfaced daily by the Vera AI Workflow. These operations employ a wide range of misleading content and tactics designed to maximize reach and influence and create assets to be repurposed at later times. Fundamentally deceptive, they manipulate platform algorithms and user engagement to amplify harmful content, compromising the integrity of digital spaces. Grounded in the theoretical framework of strategic information operations (Starbird et al., 2019), the study uses a mixed-methods approach to analyze the intersection of algorithmic affordances, deceptive tactics, and user-driven amplification dynamics. The intentions behind strategic information operations vary, including political influence (Vargo et al., 2018), issue-based campaigns (Huth et al., 2020), and financially motivated activities (Silverman & Alexander, 2016). However, determining intent remains methodologically challenging, as actors often disguise their identities and engage in strategic deception. Deception serves as a key analytical framework, emphasizing the intentional manipulation of beliefs and behaviors while focusing on the

Suggested Citation (APA): Marino, G.. Giglietto, F., Chakraborty, A., Terenzi, M., & Olaniran, S. (2025, October). *Throwing Spaghetti, Seeing What Sticks: Iterative Deception in Digital Strategic Information Operations*. Paper presented at AoIR2025: The 26th Annual Conference of the Association of Internet Researchers. Niterói, Brazil: AoIR. Retrieved from http://spir.aoir.org.

actions of deceivers (Chadwick & Stanyer, 2022). According to this framework, we pose the following research question: Are the strategic information operations identified by the Vera AI Workflow deceptive?

Strategic information operations leverage algorithm-driven flows and platform affordances to maximize reach and adaptability (Starbird et al., 2019; Bradshaw & Howard, 2018). Algorithmic curation prioritizes high-engagement content, often amplifying outrage, bias-confirming narratives, and misinformation regardless of accuracy (Al-Rawi, 2019; McLoughlin et al., 2024). The authors thus asked: How do malicious actors exploit Facebook's platform features to conduct strategic information operations?

Strategic information operations rely on collaborative coordination through social media affordances (Starbird et al., 2019; Bennett & Segerberg, 2013). By generating and amplifying misleading content, these efforts seek to manipulate public discourse and increase the perceived influence of deceptive narratives (Gleicher, 2018; Allen, 2022). Against this backdrop, the third research question is: How do users' participatory endeavors influence the creation and circulation of strategic information operations?

Data and Methods

The study focuses on three case studies—pro-Putin propaganda, online casino promotion, and adult content spread in poorly moderated groups—identified by the Vera AI Workflow (Giglietto et al, 2023). The workflow is designed to monitor, detect, and iteratively update lists of coordinated social media accounts by analyzing behavioral patterns and interaction metrics. Starting with a seed list of problematic accounts from academic research, verified fact-checking databases, and investigative findings, it systematically collects high-engagement and coordinated posts. Between October 2023 and August 2024, the workflow discovered 1,225 Facebook accounts, 10,681 coordinated links, and 2,126 new accounts. It was interrupted on August 14, 2024, due to CrowdTangle’s deprecation.

We analyzed actors, content, and behaviors, combining a qualitative grounded approach with a descriptive quantitative analysis of interactions.

Findings

The first case study examines a network of Facebook groups disseminating pro-Putin propaganda. This operation strategically coordinates content dissemination to promote political narratives, leveraging automated tools to synchronize distribution and exploit Facebook’s features to amplify pro-Kremlin messages. The study shows how a blend of overtly political and seemingly benign content is designed to fabricate an illusion of widespread grassroots support for Russia’s geopolitical goals, aligning with research on social media-based propaganda and coordinated amplification strategies (Giglietto et al, 2020).

The second case study investigates a campaign promoting online casinos through automated and AI-generated content. This operation maintains high visibility and reach by mass-producing promotional materials and using engagement bait tactics to manipulate content indexing in users' feeds. We detected a prevalence of content removed by the platform, showing signs of policy violation.

The third case study delves into the misuse of large, poorly moderated Facebook groups to disseminate adult content. These groups, often built around fandoms or memes, are repurposed for illicit activities, including pornographic scams and

engagement manipulation. Weak moderation policies create an environment where misleading content thrives, often with users contributing to its spread.

Discussion and Conclusions

The study underscores significant governance and policy implications, advocating for robust strategies to mitigate these operations. However, Meta's recent rollback of fact-checking initiatives raises concerns about its commitment to mitigating these threats (Kaplan, 2025), particularly given the already limited enforcement of its policy and terms of service. The findings emphasize the vital role of external researchers in detecting deceptive practices and the need for scalable, platform-agnostic solutions to monitor and combat these threats effectively.

The research also addresses the growing challenges posed by restricted access to social media data, which hinder efforts to counter these threats. The discontinuation of tools like CrowdTangle and the limited functionality of Meta's Content Library API create barriers to replicating this research across multiple social media platforms. Despite these challenges, the study calls for greater investment in accessible monitoring tools and transparent data-sharing mechanisms between platforms, regulators, and researchers.

The presentation will describe the three case studies in light of the current scenario, highlighting the critical need for enhanced social media governance and monitoring tools to combat deceptive information operations.

References

Allen, J. (2022). Misinformation amplification analysis and tracking dashboard. Integrity Institute. https://integrityinstitute.org/blog/misinformation-amplification-tracking-dashboard

Al-Rawi, A. (2019). Viral news on social media. Digital Journalism, 7(1), 63–79. https://doi.org/10.1080/21670811.2017.1387062

Bennett, L. W., & Segerberg, A. (2013). The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics. Cambridge University Press.

Bradshaw, S., & Howard, P. N. (2018a). Challenging truth and trust: A global inventory of organized social media manipulation. Oxford Internet Institute. https://demtech.oii.ox.ac.uk/research/posts/challenging-truth-and-trust-a-global-inventory-of-organized-social-media-manipulation/

Chadwick, A., & Stanyer, J. (2022). Deception as a bridging concept in the study of disinformation, misinformation, and misperceptions: Toward a holistic framework. Communication Theory: CT: A Journal of the International Communication Association, 32(1), 1–24. https://doi.org/10.1093/ct/qtab019

Giglietto, F., Righetti, N., Rossi, L., & Marino, G. (2020). It takes a village to manipulate the media: coordinated link sharing behavior during 2018 and 2019 Italian elections. Information, Communication & Society, 23(6), 867–891. https://doi.org/10.1080/1369118X.2020.1739732

Giglietto, F., Marino, G., Mincigrucci, R., & Stanziano, A. (2023). A Workflow to Detect,

Monitor, and Update Lists of Coordinated Social Media Accounts Across Time: The Case of the 2022 Italian Election. Social Media + Society, 9(3). https://doi.org/10.1177/20563051231196866

Gleicher, N. (2018). Coordinated inauthentic behavior explained. Meta. https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/

Huth, K., Peters, J., & Seufert, J. (2020, February 11). The heartland lobby. Correctiv.org; CORRECTIV. https://correctiv.org/en/top-stories/2020/02/11/the-heartland-lobby/

Kaplan, J. (2025, January 7). More speech and fewer mistakes. Meta. https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/

McLoughlin, K. L., Brady, W. J., Goolsbee, A., Kaiser, B., Klonick, K., & Crockett, M. J. (2024). Misinformation exploits outrage to spread online. Science (New York, N.Y.), 386(6725), 991–996. https://doi.org/10.1126/science.adl2829

Silverman, C., & Alexander, L. (2016, November 3). How Teens In The Balkans Are Duping Trump Supporters With Fake News. BuzzFeed News. https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo

Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations. Proc. ACM Hum.-Comput. Interact., 3(CSCW), 1–26. https://doi.org/10.1145/3359229

Vargo, C. J., Guo, L., & Amazeen, M. A. (2018). The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. New Media & Society, 20(5), 2028–2049. https://doi.org/10.1177/1461444817712086