Caitlene Baer **9/28/2025**

Article Review #1: Policy Considerations of Open-Source Intelligence

Introduction

The article "Policy Considerations of Open-Source Intelligence: A Study of Bellingcat's Online Investigation Patterns," written by Pitman and Walsh, is reviewed. Bellingcat is a leading open-source investigative group utilizing open-source intelligence over the past ten years, and ethical and policy issues emanating from Bellingcat's practices are explored. The review evaluates the study in terms of social scientific principles, research design and data analysis, classroom concepts, marginalized populations, and impacts on society.

Relation to Social Science Principles

Key principles of social science are pulled from the study as it examines human engagement with digital systems, flows of information dealing with power, and individuals acting alone or collectively. Their analysis of Bellingcat's investigations underscores the interrelation of social structures, individual behavior, and institutional practices in digital space or online environments. These are all principles in sociological and criminological frameworks that examine how societies produce knowledge and/or knowledge production, regulate behavior, and deal with ethical dilemmas in the realm of governance and security. (Pitman & Walsh, 2024).

Research Question, Variables, and Hypotheses

The research question is: What patterns emerge from Bellingcat's online investigations published in 2014-2024, and what are the policy implications of these practices?

- Independent Variables: Year of the investigation, type of issue investigated, presence of photos or video, type of primary sources used.

- Dependent Variables: Number of investigations, number of cases that utilized various types of media, distribution of primary sources.

While the authors do not explicitly state hypotheses, they suggest that OSINT practices have changed over time, including increasing use of visual media and changing the issues they investigate. (Pitman & Walsh, 2024).

Research Methods

The researchers took a longitudinal content analysis approach to Bellingcat investigations published over the last decade. Each investigation was treated as a case and then coded according to the topic, the use of visual media, and the type of sources used in their investigations. Since coding occurred systematically, researchers were able to track trends over a decade of the study's analytical outputs. Overall, the design is descriptive and exploratory, as the purpose was to document and state patterns but not test hypotheses.

Data and Analysis

The dataset is comprised of coded categorical data from the Bellingcat investigations, and the researchers analyzed the data using descriptive statistics, including percentages and frequency distribution, to demonstrate how investigative practices evolved in this time-period. Time-based comparison is a useful means for revealing trends or changes in the use of media and reliance on sources during investigations. For example, the authors indicate a growing reliance on pictures and videos in the last few years and shifts in the types of issues investigated. These

findings demonstrate how OSINT has evolved in practice and relevance to policy. (Pitman & Walsh, 2024).

Connection to Course Concepts

The ethical issues raised have relations to class discussions about privacy, accountability, and the need for rules against digital investigatory practices. Related to the course, social scientists have examined the role of victims in cyber incidents, which ties into the article's discussion of larger implications. Research demonstrates that for many victims, they were completely unaware of their victimization; psychological variables also moderate susceptibility. For example, lower levels of self-control conferred greater risk for victimization. The Big Five Personality Traits can also be relevant. Openness to experience might increase the likelihood an individual would be willing to try risky online behaviors; Agreeableness would amplify susceptibility by increasing the risk of oversharing; and Extraversion meant an individual would have a larger social network (and thereby a larger number of possible attackers). Conscientiousness would mean reduced vulnerability, and neuroticism would correlate to being a victim, although it is uncertain if it is cause or effect. These ideas further support the ideas of the article by demonstrating in general how human behavior, cognition, and personality influence risks to cybersecurity.

Relevance to Marginalized Groups

Although the article is not based on marginalized populations, there are implications to the findings. People living in conflict zones—frequently from vulnerable or marginalized groups—may feature disproportionately in OSINT investigations. Images of humans, their personal videos, and social media posts can all be used, often without consent. This raises ethical concerns associated with surveillance and their exploitation. The authors also highlight how

policy considerations must address protection for these populations, who are unlikely to have the resources to be aware of or control the way their data is being used by OSINT investigators.

Contributions to Society

This article makes an important contribution to society in three main ways. First, it provides the first empirical evidence suggesting the evolution of OSINT practices, which, in turn, contributes to transparency in such investigations. Second, it initiates discussions around policy and ethics as essential considerations for lawmakers, platforms, and the public. Finally, the article highlights an area in which there is a tension between theories generated in academia and the realities of investigative practice, which will lead to additional discourse regarding accountability, regulation, and equity in digital investigations.

Conclusion

Pitman and Walsh's study is a timely and significant contribution to the field related to open-source intelligence practices, specifically how Bellingcat has documented investigative practices around the world. It raises important questions about both the benefits and potential risks of OSINT, especially on privacy and ethics. The authors encourage policymakers to consider how to better create boundaries or frameworks to allow various investigations to be conducted safely while publicly ensuring the protection of populations at risk and the transparency and accountability of investigators.

References

Pitman, L., & Walsh, L. (2024). Policy considerations of open-source intelligence: A study of Bellingcat's online investigation patterns. International Journal of Cybersecurity Intelligence & Cybercrime. https://vc.bridgew.edu/ijcic/vol8/iss2/4