Article Review #2: Review of Online Open-Source Investigation and Its Relation to Principles of the Social Sciences

Student Name: Eric Zhao

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/13/2025

Introduction/BLUF

The article introduces the concept of open-source investigation, defined as "intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (Pitman & Walsh, 2025, p. 48). The article abbreviates open-source intelligence as OSINT, and as such, this review will do the same. The purpose of the study was to address some concerns about OSINT collection; particularly regarding the necessity of public and online use of OSINT, what the information is used for, and who this may negatively impact (Pitman & Walsh, 2025, p. 47). This study also focused on Bellingcat's online investigation patterns from 2014 to 2024. The results of this study show that OSINT collection can produce diverse consequences for people of all levels, ranging from leaking civilian data to military operations. In their analysis, Pitman & Walsh state that Bellingcat's researchers use pictures and/or videos to increase credibility of their findings (Pitman & Walsh, 2025, p. 55). As a result, it can reveal valuable, personal information of individuals not wanted by law enforcement (Pitman & Walsh, 2025, p. 55). Although the authors make it known that Bellingcat's researchers emphasize that a person in a photo is not a part of a crime, it can still expose them to negative reactions from people online and face to face. An example provided was Sunil Tripathi, who was misidentified suspect in the Boston Marathon bombings (Pitman & Walsh, 2025, p. 55). The case ends with Sunil taking his own life and with harassment by social media users and journalists to him and his family (Pitman & Walsh, 2025, p. 55). An example of OSINT that affected both users and even national security was the Strava app released in 2017. The app was designed to help users "socialize when benefiting from physical activity", collecting and releasing 13 million GPS locations (Pitman & Walsh, 2025, p. 49). In turn, this leaked unveiled military bases and other

installations because some soldiers also used the application. OSINT investigation can also cover a wide range of topics. The authors found that Bellingcat had a focus on armed conflicts, missing/abused children, extremism/information operations, and organized crime groups (Pitman & Walsh, 2025, p. 55). Following the analysis, they state that special attention needs to be paid to the necessity of an investigation and the implications of said investigation (Pitman & Walsh, 2025, p. 57). The article is concluded with the claim that “open-source investigations can be a significant asset... but only if it is handled with the necessary care for accurate information, attention to privacy, diversity of sources, topics, and focus-areas"
(Pitman & Walsh, 2025, p. 57).

Relation/Connection to Social Science Principles

The article demonstrates many core social science principles such as objectivity, empiricism, and ethical neutrality. Objectivity is a core part of the study that Pitman and Walsh conducted. Given that OSINT can have both positive and negative effects, the authors did not involve their own values. They presented potential benefits like increasing transparency, but they do not fail to include risks like privacy concerns and the possibility of unintended harm. Another principle that the authors have exercised is empiricism. Their analysis of the Bellingcat investigations was based on patterns in the empirical data they collected, and the observed events that occurred where the investigations took place, rather than speculation. The third principle that the authors have demonstrated is ethical neutrality. The authors’ treatment of sensitive information was careful, and their analysis avoided contributing to privacy violations. However, their discussion shows the complexity behind the ethics of OSINT and how potential harm can come to those with little awareness of how public information can be used.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Question: what are the characteristics of the open-source investigations conducted by Bellingcat – one of the most often cited open-source investigative platform in the world? (Pitman & Walsh, 2025, p. 50)
- Hypothesis: Although not explicitly stated in the article, it is implied that the authors wanted to test the relationship between the patterns in data collected by Bellingcat's OSINT investigations and the individuals or groups that it would affect.
- Independent Variable: The independent variables included the year of the investigation, the countries that investigations were focused on, topic of the investigation, source of the data, and the presence or lack of pictures or videos tied to the investigations. (Pitman & Walsh, 2025, p. 50)
- Dependent Variable: The dependent variable(s) varied among each investigation, but there was not a clear operationalization of the dependent variable(s) and how they were measured.

Types of Research Methods used

This study employed quantitative research methods like gathering data about the number of Bellingcat's OSINT investigations by countries, topics, and sources of Bellingcat's data. They systematically categorized each investigation into the groups and drew conclusions based on the data and events surrounding it. For example, they explain that the years with the most investigations could be explained by major events such as COVID-19 and major military conflicts in Europe and the Middle East (Pitman and Walsh, 2025, p. 50).

Types of Data Analysis used

The authors analyzed the data mainly using the frequency in which an investigation occured for each of their categories. For example, the authors noted that the main emphasis of most cases is on great power rivalries, with Russia and the US having carried out a large portion of Bellingcat's analyses (Pitman and Walsh, 2025, p. 54). This is supported by their data tables on pages 51 through 52, as well as their analysis on the following pages.

Connections to other Course Concepts

This study contains certain cybersecurity concepts that were discussed in lectures, including ideas like the human factor, Maslow's hierarchy of needs, perceptions and safety, and motives. The human factor plays a big role in article as it is the primary interpretation of the data and how it would be phrased to best represent the ideas. While Bellingcat states that certain people in the photos are not involved, it is only human to be skeptical and not immediately trust the information given. This leads to motives. The researchers' motives shape how they went about the study and the different things that they did. Since the researchers wanted to address some of the concerns around OSINT, they took caution in how they addressed the issue and did not include their own ethical compass in the study. Their analysis of the OSINT investigations relate to the perceptions and safety that surround publicly available information. Finally, it loops back to Mazlow's hierarchy of needs. Specifically, self-fulfillment needs. This article could serve as a form of self-fulfillment and a way for the authors to make their own path in their career.

Connections to the Concerns or contributions of Marginalized Groups

Some marginalized groups that this investigation may concern could include older individuals and people in less developed countries without as much knowledge of the details behind OSINT. Furthermore, OSINT has directly influenced the daily lives of civilians who can have no involvement with a conflict. This can involve people living close to a conflict zone or even individuals on the internet that happened to come across an investigation. This can be seen in the aforementioned case of Sunil Tripathi and other cases like "John Doe 29" (Pitman and Walsh, 2025, p. 55). The article suggests that the simple act of exposure, not to mention other forms of publicization, can lead to harsh consequences for certain marginalized groups.

Overall societal contributions of the study/Conclusion

The study makes a societal contribution by increasing the general understanding of OSINT data collection and how that might affect certain individuals. Through the analysis of Bellingcat's investigations, the authors highlight the importance of ethical, careful use of public data. The implications of this study can be applied to both cybersecurity and social sciences. For cybersecurity, it serves as an example of how digital information can be used or misused by researchers and cyber criminals. For the social sciences, it can help us further understand how information can affect the perceptions of a global conflict. In conclusion, the common message shared between these two fields is the emphasis on how public digital data is used, and that special attention needs to be given to understanding the impact that OSINT has on the world.

Reference

Pitman, L. & Walsh, L. (2025). Policy Considerations of Open-Source Intelligence: A Study of Bellingcat's Online Investigation Patterns (2014-2024) . International Journal of Cybersecurity Intelligence & Cybercrime, 8(2), - . DOI: https://doi.org/10.52306/2578-3289.1202

Article Link: https://vc.bridgew.edu/ijcic/vol8/iss2/4