Article Review #2: Policy Considerations of Open-Source Intelligence: A Study of Bellingcat's Online Investigation Patterns

Student Name: Aaron Fields

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

This article looks at how Bellingcat, an open-source intelligence group, investigates events using publicly available digital content. The authors review Bellingcat's work from 2014 to 2024 and focus on the policy and ethical issues that come with using OSINT. The main point is that while these methods can support truth and transparency, they also raise concerns about privacy and misuse. There is a need for clearer guidelines.

The study ties into social science ideas like behavior, institutions, and culture. It shows how people use digital tools to investigate and share information, and how governments and media respond, sometimes in ways that protect their own interests. It also highlights how culture shapes what gets investigated and how digital evidence is interpreted. Overall, it shows how tech is changing how people act and how society adjusts to new ways of gathering and sharing information.

The authors explore how Bellingcat's OSINT practices raise policy questions. They argue that while these tools help uncover facts, they also bring up ethical concerns that need more attention. The independent variable is Bellingcat's use of OSINT methods like video and social media analysis. The dependent variable is how those methods affect privacy and influence policy decisions.

They used qualitative methods, analyzing a dataset of Bellingcat investigations to find patterns in how visual media was used and what topics were covered. They also pulled from existing research on OSINT and policy to support their conclusions.

Content analysis was used to break down Bellingcat's investigations. The authors looked at what kinds of sources were used, like videos and social media posts, and how often certain techniques showed up. They also tracked the ethical concerns raised in each case.

This connects to ideas from class, especially around digital surveillance and the role of non-state actors in cybersecurity. It also ties into discussions about transparency, accountability, and the risks of exposing personal data. The study reinforces that cybersecurity isn’t just technical. It’s also social and ethical.

One important point is how OSINT can affect marginalized groups. When personal data is used without consent, it can put people at risk. The article shows how these groups can be both victims and sources of information in digital investigations.

Overall, the study helps explain the growing role of OSINT in cybersecurity and public investigations. It shows that while these tools can support truth and accountability, they also come with risks that need to be managed. The authors call for better policies to guide ethical use and protect individuals. The article adds to the field by showing the need to balance transparency with privacy.

Reference

Pitman, L., & Walsh, L. (2024). Policy Considerations of Open-Source Intelligence: A Study of Bellingcat's Online Investigation Patterns (2014–2024). *International Journal of Cybersecurity Intelligence & Cybercrime*, 8(2). https://vc.bridgew.edu/ijcic/vol8/iss2/4/