

# **Enhancing Cyber Threat Intelligence: Developing the InfoIntegrity Model Through Reflexive Ethnography**

**Early stage paper**

**Heba Taer**

University of Alabama, AL  
htaer@crimson.ua.edu

**Allen C. Johnston**

University of Alabama, AL  
acjohnston5@ua.edu

## **ABSTRACT**

The widespread proliferation of misinformation and disinformation, propelled by technological advancements, poses significant societal and economic threats. This threat not only challenges societal trust but also imposes significant economic damages, with the global economy suffering an estimated loss of \$78 billion annually due to these misleading practices. As these deceptive practices gain traction and evolve, there is an urgent need to develop strategies and tools that can effectively counteract their influence, safeguard cognitive functions, and promote information integrity across various online platforms. Traditional models, such as the social diffusion model introduced by (Karlova and Fisher 2013), effectively demonstrate the spread, influence, and evaluation of misinformation and disinformation in a social setting. While these models provide valuable contributions in the area by illustrating the spread and impact of misinformation and disinformation, limitations exist in addressing the multifaceted nature of misinformation and

disinformation in the context of current technological evolutions. Acknowledging these gaps, this research in progress introduces the InfoIntegrity Model, developed using reflexive ethnography to enhance the capabilities of CTI analysts in identifying and mitigating proliferation of misinformation and disinformation. By incorporating the unique background of researchers in CTI and employing a combination of ethnographic interviews and pilot testing observations, the model aims to improve information integrity across digital platforms. This paper outlines the model's development process, its initial assessment by cybersecurity-focused PhD students, and its potential implications for both theory and practice in the field of cyber threat intelligence.

## **Keywords**

Misinformation, disinformation, cognitive bias, reflexive ethnography.

## **INTRODUCTION**

Misinformation and disinformation present a growing threat to the reliability and integrity of factual information (Pérez Escolar et al. 2023). Misinformation refers to inaccurate information being disseminated without the purpose of misleading, yet it may still cause harm, as it may stem from exaggerated truths, mistakes, or a lack of knowledge about a particular topic. Misinformation is often disseminated unintentionally and can be revised with accurate and reliable information (Galvin 2021). In contrast, disinformation is purposely shaped and disseminated false information intended to mislead and manipulate individuals. It is often distributed with specific objectives, such as influencing public opinion, proliferating confusion, or undermining trust in societies (Hameleers et al. 2022; Praveenkumar 2024).

Disinformation is typically a practice of propaganda or purposeful campaigns to mislead the public (Shu et al. 2020).

Both misinformation and disinformation are attributed to various destabilizing societal and economic effects. The societal impacts of misinformation and disinformation are evident in various domains, specifically in public health, where they can significantly influence vaccination intentions (Loomba et al. 2021). Moreover, a 2019 survey conducted by the Pew Research Center revealed widespread concern among U.S. adults regarding the detrimental effects of misleading information, surpassing concerns about terrorism, illegal immigration, racism, and sexism (Mitchell et al. 2019). In terms of economic consequences, numerous examples exist, such as a 2013 disinformation tweet from the Associated Press falsely reporting an explosion injuring former President Barack Obama, which resulted in the U.S. stock market experienced a precipitous drop, temporarily erasing approximately \$130 billion in market value within minutes (Foster 2013; Shu et al. 2020). As another example, a recent disinformation campaign involving a deep fake voice impersonating the CEO of an undisclosed UK-based energy company resulted in the unauthorized transfer of USD \$243,000 USD to a Hungarian supplier (de Rancourt-Raymond and Smaili 2023). A comprehensive economic analysis conducted by Professor Roberto Cavazos from the University of Baltimore, commissioned by CHEQ, has revealed that the global financial implications of misinformation and disinformation campaigns are estimated to be at least USD \$78 billion annually, with predictions indicating that this figure will only escalate.

Additionally, with the inception of technological advancements, particularly in artificial intelligence (AI), the challenges posed by misinformation and disinformation campaigns become

increasingly complex, emphasizing the critical need to address this domineering issue (Cavazos 2019). AI can manipulate various forms of media rapidly and efficiently, amplifying the spread of false information (Bontridder and Pouillet 2021). For instance, a deepfake voice impersonated the director of an undisclosed company located in Hong Kong, leading to the authorization of multiple international transactions totaling \$35 million (de Rancourt-Raymond and Smaili 2023). Moreover, state-sponsored actors and other malicious entities invest significant resources in disinformation campaigns aiming to influence public opinion and exacerbate social divisions (De Witte 2022). For example, Andrus Ansip, former vice-president of the European Commission, claimed that Russia spends at least €1.1 billion (USD 1.2 billion) per year on pro-Kremlin media to create disinformation among their adversaries (Cavazos 2019).

Considering the profound impact of misinformation and disinformation campaigns on society and economies, it is crucial to equip our frontline defenses with effective tools for detecting and combating these threats. CTI analysts often serve in this frontline capacity (Shin and Lowry 2020), leveraging their expertise to monitor, analyze, and respond to cyber threats, thereby safeguarding organizations and individuals from the harmful effects of malicious misinformation and disinformation. The substantial gap between the current number of active CTI analysts in the U.S. and the professional demand in this field underscores a significant talent shortage (Eckert 2023). However, the primary challenge encountered by CTI researchers and analysts does not stem from their numbers or workload volume, but rather the lack of necessary resources to conduct their trade more effectively and efficiently (Team 2020). The absence of appropriate tools presents a challenge to their fundamental role, leading to escalated threats for the organization (Ariganello 2022; Team

2020). The propagation of misleading information on OSINT platforms has created significant concern in the field of CTI research (Ranade et al. 2021).

Furthermore, as more organizations increasingly incorporate government bulletins and media reports into their CTI analyses, there is an urgent need to address how CTI data collection is vulnerable to the influence of misinformation and disinformation, which can adversely impact the analysis of intelligence data, consequently implementing a pressing demand for tools that can enhance CTI analysts' ability to identify and mitigate such misleading information (Brown and Lee 2021). Addressing these challenges is critical, particularly regarding the sensitive nature of data analysis, highlighting the necessity need for tools that not only improve their training programs but also ensure the reliability and quality of intelligence outcomes.

Our objective is to help fill the resource void faced by CTI analysts by developing and testing an InfoIntegrity Model that can aid them in identifying misinformation and disinformation. Drawing from cognitive bias theories, including confirmation bias and cognitive dissonance theory, we developed this model using a reflexive ethnography approach.

While further development and testing is needed, for this research in progress, we present the findings of some initial interviews and pilot tests of the model using a sample of cybersecurity-focused Ph.D. students at a large university in the southeastern region of the U.S. The findings of these interviews and pilot tests indicate that the model may offer a systematic and comprehensive approach to identifying misinformation and disinformation, thereby enhancing the analyses

conducted by CTI analysts. This method supports analysts in their efforts to recognize misinformation and disinformation within their intelligence operations.

Once fully developed and tested, we anticipate that our InfoIntegrity model will provide a novel theoretical framework that enhances the dynamic identification of misinformation and disinformation. Additionally, this research has the potential to foster collaboration between academic researchers and cyber research analysts, narrowing the communication gap and facilitating the development of research tailored to the specific needs of academics and cybersecurity researchers. Our model is expected to improve the practice of misinformation and disinformation detection by providing CTI professionals with a valuable tool for their intelligence investigations. It aims to empower professionals to detect, prevent, and mitigate misinformation and disinformation proactively. Furthermore, our investigation will introduce additional enhancements and strategies for disrupting misinformation and disinformation, integrating them into the model. The research will also explore and identify the strengths of OSINT as a tool for identifying patterns and disputing misinformation and disinformation, highlighting its effectiveness and value for researchers and analysts.

It will reveal new strategies, patterns, and trends in analyzing misinformation and disinformation, contributing to ongoing research in the field. This model desires to empower CTI analysts with a toolset that enhances their ability to identify, analyze, and prevent amplification of misinformation and disinformation, thus mitigating their influence on economic and societal outcomes.

In the sections that follow, we first explore the existing literature within the field of Information Systems (IS) and other disciplines through a comprehensive literature review.

This review examines the phenomena of misinformation and disinformation, discussing their global impact on social trust and economic strength. It identifies existing gaps and highlights the limitations of current models, including our foundational model based on the Social Diffusion Model, which ineffectively addresses misinformation and disinformation. To bridge these gaps, the review introduces our study's implemented model, the "InfoIntegrity model," a comprehensive tool designed to identify misinformation and disinformation. We then outline our use of reflexive ethnography method to develop the InfoIntegrity Model. This section details the integration of the researcher's direct knowledge and experience, facilitated by continuous reflection across three phases: Before, During, and After. We then present our "After" phase data analysis and findings, followed by a discussion of these findings and their contributions to theory and practice, and the limitations of this study.

## **LITERATURE REVIEW**

Misinformation and disinformation have emerged as global concerns, marked by their rapid growth and substantial negative impacts on societal trust and economic stability (Wark 2024). For example, the U.S. Department of State identified the extensive reach of the Kremlin's disinformation campaign as Russia's most powerful strategy tool to manipulate global perceptions of its political intentions (Center 2024). Further, the widespread accessibility of social media platforms, such as Facebook and Instagram, significantly amplifies the reach and impact of misinformation and disinformation, allowing them to infiltrate vast audiences easily and become a prolific base for exploitation by malicious actors (Shu et al. 2020). This expansion only further intensifies global concerns over the circulation of false content and highlights the

need for novel strategies to identify and mitigate their dissemination. Research such as Petratos (2021) underscores the urgent need for effective strategies to mitigate these threats, which are expected to intensify with continued technological advancements. Agarwal and Alsaeedi (2020) point out the deficiency in existing models that address the proliferation of misinformation and disinformation, indicating a need for a comprehensive approach that can adapt to today's interconnected landscape. Misinformation, spread without malicious intent, contrasts with disinformation, which is deliberately crafted to deceive (French et al. 2023). This distinction is crucial for CTI professionals who utilize Open Source Intelligence (OSINT) but face increasing security concerns over identifying and mitigating misleading content across platforms. Ranade et al. (2021) explore how easily threat actors can distribute false CTI across OSINT platforms, leading analysts to validate inauthentic information inadvertently. This situation underscores the necessity for a structured framework that enhances analysts' capabilities to proficiently identify and mitigate significant threats posed by misinformation and disinformation.

The literature includes models such as (Karlova and Fisher 2013) social diffusion model, which provides insights into how misinformation spreads, is implemented, and evaluated within social settings. The model delineates the diffusion process into three primary stages: initiation, where misinformation is created and introduced into the network; dissemination, which describes the spread of this information through social connections; and integration, where misinformation becomes embedded in community beliefs and behaviors. This model highlights the role of social media as a catalyst in the rapid spread of misinformation due to its inherent network structures and the influence of key individuals or gatekeepers who can either amplify or mitigate the spread



of false information. By focusing on these dynamics, the social diffusion model provides insights into the mechanisms behind the viral nature of misinformation and suggests points of intervention to curb its impact on society.

Despite its insights into the dissemination of misinformation, the social diffusion model exhibits limitations that fail to address the influence of foreign actors in the proliferation of disinformation or consider engagement metrics like likes, shares, and comments that significantly impact the spread of misleading content (Jakstaite and Ricardo ; Théro and Vincent 2022). Additionally, it lacks a discussion on fact-checking, an essential component for validating information accuracy (Li and Chang 2023). Addressing cognitive biases is also vital, as they significantly affect how individuals perceive and decide upon encountering online information.

Soon and Goh (2018) and Figl et al. (2019) further argue that online platforms often present information contradicting individuals' cognitive beliefs, encouraging users to resolve this dissonance by altering or reevaluating their views on the reliability of misleading information or the credibility of its source. From this, the strategy of "consider the opposite," has proven effective in assisting individuals to overcome their confirmation bias, as it becomes apparent that individuals naturally pursue consistency in their beliefs (Soon and Goh 2018, p. 25). These studies highlight the role of confirmation bias and cognitive dissonance in influencing individuals' acceptance of information that aligns with their beliefs and the discomfort they experience when faced with conflicting information.

In response to these gaps, our InfoIntegrity Model integrates cognitive biases and cognitive dissonance theory, offering a novel approach to combat misinformation and disinformation. This model represents an evolution of the social diffusion model, emphasizing the cognitive factors influencing analysts' judgments and providing a comprehensive framework for CTI analysts. This development is critical for addressing the societal and economic consequences of misinformation and disinformation campaigns and enhancing the digital landscape's resilience against these threats. By integrating cognitive theories and leveraging the latest technological innovations, our model caters to the specific and evolving needs of CTI analysts.

## **REFLEXIVE ETHNOGRAPHY METHOD**

In our efforts to develop and test the InfoIntegrity Model, which aims to assist CTI analysts in identifying misinformation and disinformation, we employ the reflexive ethnography method. This method focuses on social processes and integrates the observations and experiences of the lead researcher into the implemented model, promoting a holistic understanding of the misinformation and disinformation phenomena by encouraging continuous reflection on personal biases and perspectives.

Building on the practical applications of reflexive ethnography, its significance in ethnographic research is notably underscored by Roberts and Sanders in their work "Before, During and After: Realism, Reflexivity and Ethnography" (Roberts and Sanders 2005). They argue that reflexive ethnography involves much more than simple reflection; it encompasses continuous, deep reflection throughout the entire research process. The authors identify three critical phases—

before, during, and after—which necessitate the researcher’s reflective engagement at each stage, particularly emphasizing the integration of cognitive theories like confirmation bias and cognitive dissonance to enhance the validity and depth of the research investigation (Gayibor 2015). In the "Before" phase, researchers prepare by deeply reflecting on their biases and how their backgrounds may influence their approach to the research. During the "During" phase, this reflexivity extends into the field, where researchers continuously assess and adapt their approach based on their interactions and findings, ensuring that the research evolves with a comprehensive understanding of the social dynamics at play. Finally, the "After" phase involves analyzing and integrating these insights to refine the findings, reflecting on the entire process to understand how the interactions and biases influenced the outcomes and how these outcomes can inform future research and practice.

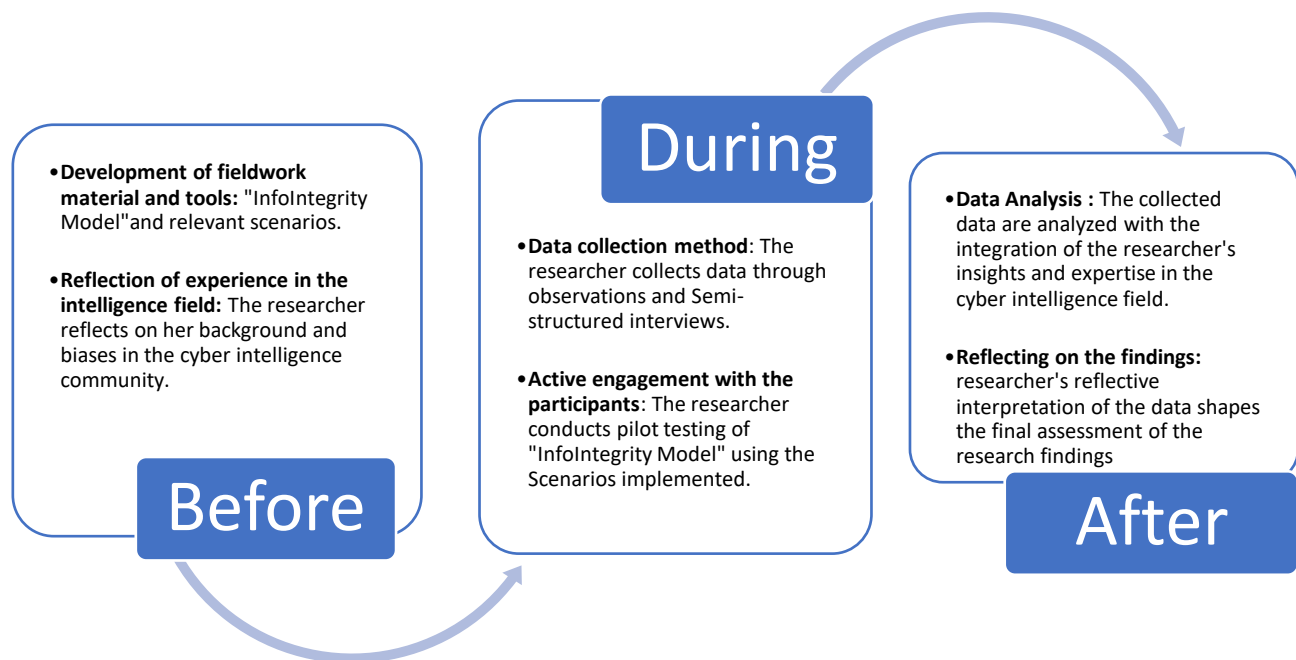
Our application of these three phases of the reflexive ethnography method is illustrated in Figure 1 and described in detail below. In applying Roberts and Sanders (2005) three-phased approach to reflexive ethnography, the development of the InfoIntegrity Model began in the "Before" phase, where we deeply reflected on the lead researcher's background as a CTI supervisor and analyst. This phase requires us to be acutely reflexive of the lead researcher’s “local culture” and her inherent cognitive biases (Roberts & Sanders, 2005. p.301). This reflection included acknowledging and anticipating inherent cognitive biases through the cognitive theories of confirmation bias and cognitive dissonance. Confirmation bias signifies the tendency to interpret information in a manner that confirms the pre-existing beliefs of an individual (Schweiger 2021), while cognitive dissonance is the discomfort experienced when encountering conflicting

information (Jeong et al. 2019). Both theories helped explain the complexities inherent in misinformation and disinformation. The outcomes of this “Before” phase was an initial InfoIntegrity Model that leveraged the researcher’s extensive experience in directing information operations teams and uncovering threats within misinformation and disinformation realms, as well as a set of initial testing scenarios that simulate real-world cyber threat environments.

Our application of the "During" phase of Roberts and Sanders (2005) three-phased approach to reflexive ethnography involved facilitating collaborative tests and assessments of the InfoIntegrity Model. To date, these tests and assessments include a set of semi-structured interviews and pilot tests of the model with four cyber-security-focused Ph.D. students from the primary researcher’s home institution in the Southeastern U.S.

The semi-structured interviews were conducted after participants applied the InfoIntegrity Model to the scenarios involving misinformation and disinformation across various contexts, such as Cultural & Social, Health & Medical, and Political. Participants provided feedback on the model’s usability and functionality, which the researcher recorded. The pilot testing comprised three distinct sessions, each adopting a different approach and each highlighting key issues related to the model’s flow and content validity. The first pilot test was focused on individual testing, while the second and third tests involved participants working in teams and as duos with the lead researcher, respectively.

Our application of the "After" phase focused on analyzing how the cognitive biases and dissonances observed during the semi-structured interviews and pilot tests influenced the outcomes from applying the InfoIntegrity model to the set of scenarios developed in the "Before" phase of this method. In doing so we thoroughly examined the data collected from the semi-structured interviews and pilot tests, focusing on identifying and understanding instances where cognitive biases and dissonance may have skewed the analysis; the details of this analysis and its findings are presented next.



**Figure 1. Illustration of the study's Reflexive Ethnographic phases "Before, During, and After," adapted from the works of Roberts and Sanders (2005)**

## **“After” Phase Data Analysis and Findings**

To analyze the data derived from the “During” phase interviews and pilot tests, we continued to rely on the lead researcher’s experiences, reflections, and insights. We employed an in vivo code approach for our qualitative analysis. This method ensured the preservation of the accuracy of participant feedback by incorporating their exact phrases as transcribed in Microsoft Word.

The transcription process involved more than mere documentation; it included engaging with the content through reflexive ethnography. This approach enabled the lead researcher to actively interact with the data, applying an in vivo coding strategy to themes such as “Usability Confusion,” “Model Usability,” and “Participant Model Insight.” These themes directly inform the continuous refinement of the model. Additionally, we addressed the complexities introduced by user biases, which were evident during the transcription and coding process. Themes such as “Unbiased Model” and “Cognitive Biases” were specifically coded to understand how cognitive biases may have influenced users' interaction with the model and whether the model could mitigate such biases. This iterative process refinement was crucial, as it empowered real-time adjustments after each session based on the participant's responses. Such an active method of analysis was instrumental in the further development of the model’s functionality, ensuring it was adequately prepared for subsequent testing and eventual implementation in the field.

The initial pilot test, individual testing, involving a single participant, highlighted significant issues related to the model’s flow and usability. The participant characterized their experience as “confusing” and indicated that the model “should be more clear,” expressing difficulty in using it

to accurately identify misinformation and disinformation. These concerns were coded under “Usability Confusion.” Additionally, the participant recommended enhancements to the logical flow and emphasized the importance of the model accommodating both false and true information. Specifically, the participant suggested that “it should be added to the model for the answer, for there to be a chance that this is true” and “an option where someone evaluates a piece of information,” underscoring the need for a more comprehensive approach that includes verifying the truthfulness of the information.

This feedback was coded under “Participant Model Insight,” which highlights the importance of broadening the model's focus beyond identifying false information. Reflecting on this feedback and drawing on established CTI practices for identifying misinformation and disinformation, the researcher reorganized the model's flow.

A Yes/No navigation option was introduced to enhance the model's usability. This adjustment, along with a strategic reconfiguration of the model's flow, improved the model's ability to engage users initially and support more in-depth investigation processes, facilitating a transition from surface-level to a more comprehensive analysis. These changes significantly enhanced the model's accessibility for newcomers and aligned it more closely with the operational needs of the expanding field of cyber operations.

The second pilot test, which was a team testing session including the researcher and a group of participants, the session fostered interactive engagement and provided insightful feedback on the model's usability, which had been improved based on prior refinements after the individual pilot testing session. They underscored how “The model provides a very good, systematic way to verify

such information” and “it helps me to go through a step-by-step procedure.” These endorsements highlight the accomplishment of our iterative refinements and the participants’ direct experience with the model. Consequently, these responses have been coded under “Model Usability”.

Additionally, one participant pointed out the necessity for further refinement of the model by expanding the definitions within the categories of misinformation and disinformation to better address specific scenarios. They emphasized the importance of being “more accurate and specific about certain scenarios,” highlighting the need to have more key initiators.

This feedback was coded under “Participant Model Insight.” In response, the researcher enhanced the model by categorizing “unintentional” as a form of identification for misinformation and “intentional” for disinformation. These feedback-driven adjustments were aimed at making the model more relevant and closely aligned with CTI operations. Reflecting on this session, the researcher acknowledged that understanding the intention behind the information would help best define its nature. This insight led to a clearer distinction between misinformation and disinformation. In the final pilot test, which included a duo session with a single participant and the lead researcher, intuitive feedback was provided on the model’s usability. The participant stated, “It gives me very clear clues to identify.” This feedback was helpful statement was coded under “Model Usability,” indicating that the refinement made to the model in the previous sessions had effectively enhanced its functionality.

Moreover, the participant noted that information specifically designed to stimulate emotional responses is more effective within groups predisposed to such influence. Therefore, it is crucial to integrate "cognitive and emotional factors" in the analysis. This feedback emerged from



observations during the pilot testing, where scenarios involving emotionally charged false information significantly could impact those positioned adversarial to the presented misleading content. Reflecting on this suggestion, the researcher expanded the “Emotional Decision Making” category within the model to more accurately address the emotional decision-making processes of targeted groups influenced by misleading information.

This adjustment reflects the understanding that disinformation is intentionally created to manipulate emotional responses and influence decision-making, distinguishing it from misinformation, which does not typically aim to manipulate emotions so directly.

After compiling and analyzing all interview and pilot testing data, the researcher further reflected on all recorded responses, identifying patterns, and aligning the findings with CTI operations, drawing on extensive field knowledge and insights.

In addition to practical model adjustments, this research examines the influence of users’ inherent biases on their online search behaviors while identifying misinformation and disinformation. Observations and semi-structured interviews confirmed that individuals tend to favor information that aligns with their pre-existing beliefs. Participants recognized that their biases affected their information gathering processes and valued the model’s approach to mitigating these biases.

During individual pilot testing, the solo participant displayed a strong bias toward the expected outcome of the provided scenario. They maintained their belief even when presented with conflicting information, despite the scenario being proven false and aligned with the participant’s

preconceived biases. They stated, “But because I did have previous knowledge, the video was not

*Proceedings of 2024 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*  
*Kennesaw, Georgia, USA*

going to change my mind,” which may indicate a bias based on perceived credible sources. This observation was coded under “Cognitive biases.” Such a situation mirrors what might happen when a cyber professional, convinced of the reliability of misleading information, continues to adhere to their initial beliefs despite encountering conflicting evidence. This behavior underscores the cognitive dissonance theory, which posits that individuals often prefer information that aligns comfortably and consistently with their established beliefs, even when faced with contradictory evidence.

Further “After” phase reflection was aimed at the objectivity of the InfoIntegrity Model. Pilot testing participants noted that without the model, they would likely yield to their cognitive dissonance and confirmation biases, especially when tasked with identifying misinformation and disinformation for personal use. In duo pilot testing, the model effectively challenged initial biases.

Initially, a participant labeled information based on biases but adjusted their views after engaging with the model. This adjustment demonstrates the model’s effectiveness in promoting unbiased information assessment. The participant remarked, “I believe that this model is really good for me to identify the of the fake news and including the misinformation and the disinformation.” In other sessions, participants observed that using the model helped reduce their biases. They commented, “If someone gave me this kind of flow chart, it helps me to reduce biases even if it's the things that are against my thoughts,” and another added, “I think the model would be less biases involving” These insights suggest that the model mitigated biases. Responses such as these have been coded under the “unbiased model.” This highlights the importance of a structured model in the CTI field,

where analysts frequently encounter misinformation and disinformation. Without a structured tool, individuals may persist with inaccurate beliefs even when confronted with conflicting evidence. However, a structured model like the InfoIntegrity Model can counteract these biases, thereby enhancing the accuracy of information processing in cyber operations.

The InfoIntegrity Model, as it stands today in this research in progress is presented in Figure 2. The insights from the initial examinations presented in this study were crucial for the refinement of the model from its initial formulation in the “Before” phase, ensuring it effectively identifies misinformation and disinformation and supports analysts in overcoming cognitive biases to make more informed decisions.

In the coming months, the three phases of Roberts and Sanders (2005) approach to reflexive ethnography will be repeated to prepare for and elicit the expertise of CTI analysts as they utilize the InfoIntegrity Model in their work with actual threat intelligence cases. The insights derived from these future tests of the model will only further enhance its efficacy and value to CTI analysts.

## **DISCUSSION**

The development of the InfoIntegrity Model was significantly influenced by the researcher’s experience as a CTI analyst and supervisor managing a team engaged in daily cyber operations. The initial model leveraged various methods for identifying misinformation and disinformation, informed by the researcher’s direct observations and experiences.

Feedback from semi-structured interviews and pilot testing highlighted the need for improved navigation and flow, leading to significant adjustments that enhanced the model’s user-friendly and efficacy in the identification process. Specifically, the inclusion of a targeted group within

the “Emotional Decision Making” category during the final pilot session reflected a sophisticated understanding that disinformation often aims to manipulate specific groups’ decision-making processes.

This enhancement was a direct result of reflecting on participants’ feedback, emphasizing the critical need to address cognitive biases within the model’s framework.

Further, the integration of structured flow into the model not only addresses cognitive biases, but also supports CTI professionals in effectively navigating complex information environments. Such an approach aligns with theoretical insights into cognitive biases, suggesting that a structured flowchart model would assist in counteracting the natural tendencies towards biased information processing.

Initial adjustments demonstrated the model’s effectiveness in promoting unbiased information assessment and illustrated its value in a field where analysts frequently confront misinformation and disinformation. The model’s capacity to mitigate biases underscores the necessity of a structured approach in the CTI field.

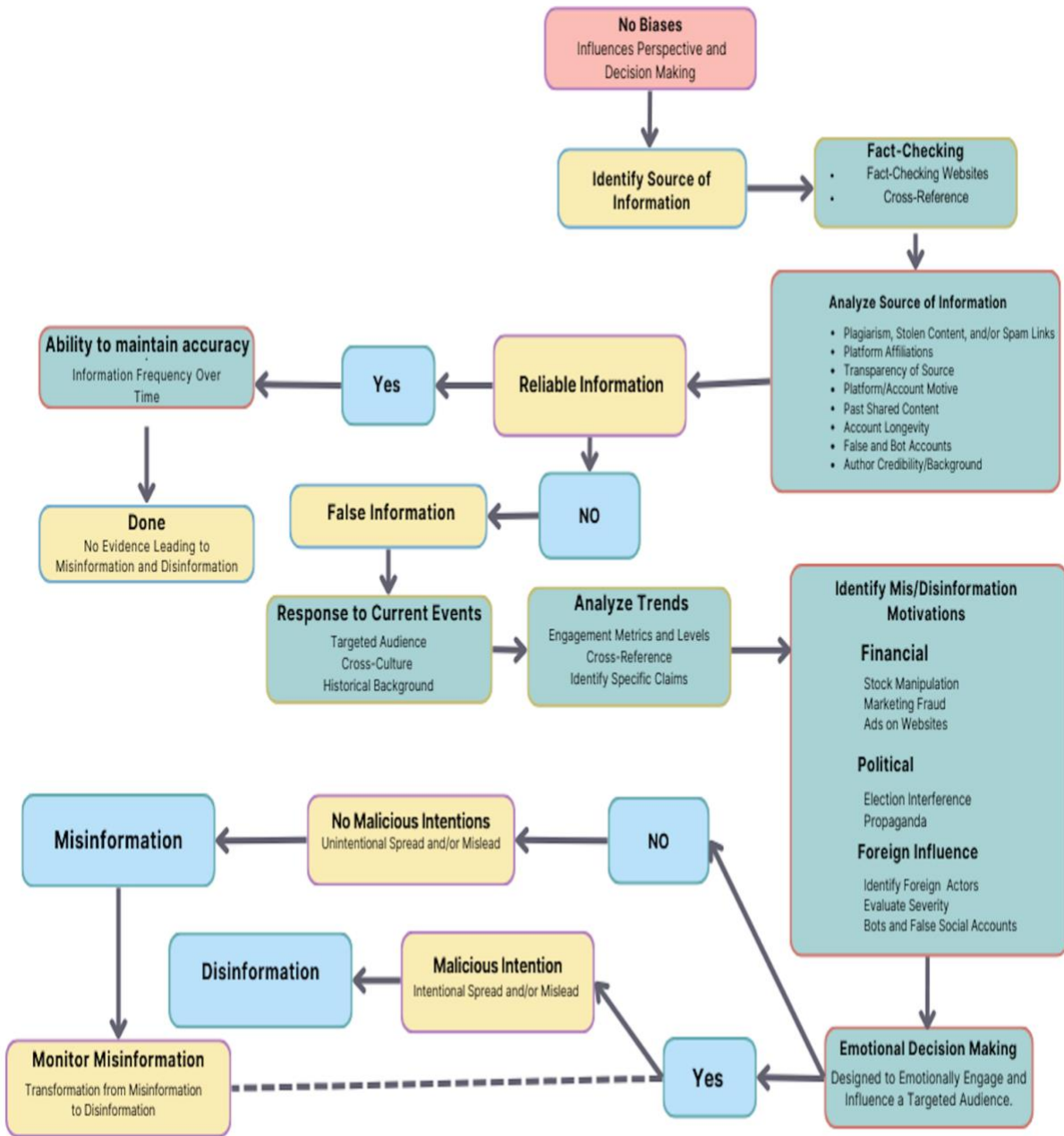
The continuous refinement process throughout the study has significantly enhanced the usability and effectiveness of the InfoIntegrity model. The final version, now integrating comprehensive feedback from participants and the reflective insights from the researcher, has evolved into a practical tool ready for further testing with CTI analysts. The study faced limitations, primarily due to its relatively small sample size and restricted timing of pilot tests, which limited the diversity

of teams and scenarios. This constraint may have narrowed the range of feedback and potentially influenced the comprehensiveness of the findings in the pilot testing.

To overcome these limitations, future research will include teams and scenarios across a wider range of contexts to provide more diverse and thorough insights. Future research should focus on evaluating the model in a more varied range of operational settings among CTI analysts.

We expect to continue this research and assess the model's impact in real-world environments. In doing so we hope to contribute to the field of cyber intelligence by deepening the understanding of the model's utility across different cyber intelligence contexts.

Moreover, with misinformation and disinformation increasingly threatening intelligence operations, there is an urgent need for practical tools like the InfoIntegrity Model, designed to enhance misinformation and disinformation identification, supporting cyber professionals in the field.



**Figure 2. The InfoIntegrity Model: Misinformation and Disinformation**

## CONCLUSION

The development and refinement of the InfoIntegrity Model through reflexive ethnography offers a significant advancement in the field of CTI. By integrating the experiential insights and reflecting on the personal biases of researchers, this model stands as a robust tool designed to enhance the detection and mitigation of misinformation and disinformation.

Our research underscores the critical role of structured analytical processes in countering the complex challenges posed by the digital dissemination of false information. As the model undergoes further testing and refinement, its potential to improve the operational efficiency of CTI analysts becomes clearer.

Looking forward, the continued evolution of the InfoIntegrity Model will be crucial in equipping professionals with the means to safeguard information integrity against the evolving threats of misinformation and disinformation, ultimately strengthening the resilience of digital societies against these daunting challenges.

## REFERENCES

- Agarwal, N. K., and Alsaeedi, F. 2020. "Understanding and Fighting Disinformation and Fake News: Towards an Information Behavior Framework," *Proceedings of the Association for Information Science and Technology* (57:1), p. e327.
- Ariganello, J. 2022. "Why Are Organizations Suffering from a Lack of Threat Intelligence Information?", from <https://www.anomali.com/blog/why-are-organizations-suffering-from-lack-of-threat-intelligence-information>
- Bontridder, N., and Pouillet, Y. 2021. "The Role of Artificial Intelligence in Disinformation," *Data & Policy* (3), p. e32.
- Brown, R., and Lee, R. M. 2021. "2021 Sans Cyber Threat Intelligence (Cti) Survey."
- Cavazos, R. 2019. "The Economic Cost of Bad Actors on the Internet: Fake News."
- Center, G. E. 2024. "Disarming Disinformation: Our Shared Responsibility." from <https://www.state.gov/disarming-disinformation/>

- de Rancourt-Raymond, A., and Smaili, N. 2023. "The Unethical Use of Deepfakes," *Journal of Financial Crime* (30:4), pp. 1066-1077.
- De Witte, M. 2022. "What Stanford Research Reveals About Disinformation and How to Address It." from <https://news.stanford.edu/report/2022/04/13/what-stanford-research-reveals-about-disinformation/>
- Eckert, C. 2023. "Ust In: U.S. Desperately Needs Cyber Talent, Congress Says." from <https://www.nationaldefensemagazine.org/articles/2023/6/26/us-desperately-needs-cyber-talent-congress-says>
- Figl, K., Kießling, S., Rank, C., and Vakulenko, S. 2019. "Fake News Flags, Cognitive Dissonance, and the Believability of Social Media Posts," in: *Fortieth International Conference on Information Systems, Munich 2019*
- Foster, P. 2013. "'Bogus' Ap Tweet About Explosion at the White House Wipes Billions Off Us Markets," in: *The Telegraph*.
- French, A. M., Storey, V. C., and Wallace, L. 2023. "The Impact of Cognitive Biases on the Believability of Fake News," *European Journal of Information Systems*, pp. 1-22.
- Galvin, M. 2021. "As Surgeon General Urges 'Whole-of-Society' effort to Fight Health Misinformation, the Work of the National Academies Helps Foster an Evidence-Based Information Environment." *National Academies of Science, Engineering, and Medicine*, from <https://www.nationalacademies.org/news/2021/07/as-surgeon-general-urges-whole-of-society-effort-to-fight-health-misinformation-the-work-of-the-national-academies-helps-foster-an-evidence-based-information-environment>
- Gayibor, A. 2015. "Integration of Immigrants into the Swedish Labor Market: An Intersectional Perspectiv." Linköping University, The Tema Institute, The Department of Gender Studies. Linköping University, Faculty of Arts and Sciences, p. 74.
- Hameleers, M., Brosius, A., Marquart, F., Goldberg, A. C., Van Elsas, E., and De Vreese, C. H. 2022. "Mistake or Manipulation? Conceptualizing Perceived Mis- and Disinformation among News Consumers in 10 European Countries," *Communication Research* (49:7), pp. 919-941.
- Jakstaite, D., and Ricardo, M. "Extracting Cyber Threat Intelligence from Social Media with Case Studies in Twitter and Reddit," *social networks* (25:24), p. 17.
- Jeong, M., Zo, H., Lee, C. H., and Ceran, Y. 2019. "Feeling Displeasure from Online Social Media Postings: A Study Using Cognitive Dissonance Theory," *Computers in Human Behavior* (97), pp. 231-240.
- Karlova, N. A., and Fisher, K. E. 2013. "A Social Diffusion Model of Misinformation and Disinformation for Understanding Human Information Behaviour," *Information Research* (18:1), p. 573.
- Li, J., and Chang, X. 2023. "Combating Misinformation by Sharing the Truth: A Study on the Spread of Fact-Checks on Social Media," *Information systems frontiers* (25:4), pp. 1479-1493.
- Loomba, S., De Figueiredo, A., Piatek, S. J., De Graaf, K., and Larson, H. J. 2021. "Measuring the Impact of Covid-19 Vaccine Misinformation on Vaccination Intent in the Uk and USA," *Nature human behaviour* (5:3), pp. 337-348.



- Mitchell, A., Gottfried, J., Stocking, G., Walker, M., and Fedeli, S. 2019. "Many Americans Say Made-up News Is a Critical Problem That Needs to Be Fixed," *Pew Research Center* (5), p. 2019.
- Pérez Escolar, M., Lilleker, D., and Tapia Frade, A. J. 2023. "A Systematic Literature Review of the Phenomenon of Disinformation and Misinformation," *Media and Communication* (11:2), pp. 76-87.
- Petratos, P. N. 2021. "Misinformation, Disinformation, and Fake News: Cyber Risks to Business," *Business Horizons* (64:6), pp. 763-774.
- Praveenkumar, B. 2024. "Misinformation and Disinformation: Unravelling the Web of Deceptive Information," *Journal of Law and Legal Research Development*), pp. 29-33.
- Ranade, P., Piplai, A., Mittal, S., Joshi, A., and Finin, T. 2021. "Generating Fake Cyber Threat Intelligence Using Transformer-Based Models," *2021 International Joint Conference on Neural Networks (IJCNN)*, Shenzhen, China: IEEE, pp. 1-9.
- Roberts, J. M., and Sanders, T. 2005. "Before, During and After: Realism, Reflexivity and Ethnography," *The Sociological Review* (53:2), pp. 294-313.
- Schweiger, S. 2021. "Confirmation Bias in Information Search with Social Tags," in: *Psychologie*. Universität Tübingen.
- Shin, B., and Lowry, P. B. 2020. "A Review and Theoretical Explanation of the 'Cyberthreat-Intelligence (Cti) Capability' that Needs to Be Fostered in Information Security Practitioners and How This Can Be Accomplished," *Computers & Security* (92), p. 101761.
- Shu, K., Wang, S., Lee, D., and Liu, H. 2020. *Disinformation, Misinformation, and Fake News in Social Media*. Springer.
- Soon, C., and Goh, S. 2018. "Fake News, False Information and More: Countering Human Biases," *Institute of Policy Studies (IPS) Working Papers* (31).
- Team, A. 2020. "Cyber Threat Intelligence: Lack of Training, Tools, Oversight.", from <https://www.authentic8.com/blog/cti-osint-lack-of-training-tools-oversight>
- Théro, H., and Vincent, E. M. 2022. "Investigating Facebook's Interventions against Accounts That Repeatedly Share Misinformation," *Information Processing & Management* (59:2), p. 102804.
- Wark, W. 2024. *Foreign Interference Online: Where Disinformation Infringes on Freedom of Thought*. Centre for International Governance Innovation.