Integrating Generative AI in Cybersecurity: A Sensemaking Perspective

Hwee-Joo Kam
Sykes College of Business, University of Tampa
Tampa, FL, USA

Allen Johnston
Culverhouse College of Business, University of Alabama,
Tuscaloosa, AL, USA

Chen Zhong
Sykes College of Business, University of Tampa
Tampa, FL, USA

Wael Soliman
College of Business, University of Agder
Kristiansand, Norway

ABSTRACT

This study explores the sensemaking processes of cybersecurity professionals as they engage with Generative Artificial Intelligence (GenAI), such as ChatGPT, within their operational environments. Recognizing the high-stakes and adversarial nature of cybersecurity work, we investigate how these professionals interpret and operationalize GenAI technologies, contributing to both cybersecurity practice and the development of GenAI tools. Utilizing a qualitative content analysis (QCA) of data from Reddit forums and YouTube panel discussions, we identify five distinct forms of sensemaking: operational, interactive, experiential, visionary, and cognitive. These forms, evoked in a cyclical process, follow the phases of change, enactment, selection, and retention. Our findings advance the understanding of professional sensemaking in the context of rapidly evolving technologies, offering a socio-technical perspective on the integration of GenAI in cybersecurity operations.

Keywords: cybersecurity, generative artificial intelligence, sensemaking

INTRODUCTION

Generative Artificial Intelligence (GenAI) has emerged as a transformative technology within the cybersecurity profession, prompting cybersecurity professionals to reassess their approaches to protecting information assets (Sen et al. 2022). While GenAI has shown an ability to enhance cybersecurity operations by automating routine tasks, facilitating threat analysis, and generating strategic insights, among other capabilities (Zhong et al. 2020), it has also introduced significant challenges to security operations. These challenges include the inherent opacity of algorithmic processes, the potential for adversarial exploitation (Gupta et al. 2023), and complexities associated with integrating GenAI into established cybersecurity practices (Mughal 2022). Given the high stakes environment of cybersecurity, where the consequences of errors can have devastating consequences (Siponen and Willison 2009), understanding how professionals make sense of and navigate these challenges is critical if cybersecurity professionals are to achieve long term success in using GenAI in these environments.

Sensemaking is essential for effective decision-making and action in high-pressure environments (Leidner et al. 2009). For example, risk-taking entrepreneurs practice sensemaking to "*operate at the edge of what they do not know*" amidst uncertainties and high-stake decision-making (Hill and Levenhagen 1995, p. 1068). Prior research has shown that sensemaking plays a pivotal role in how individuals and organizations interpret and respond to ambiguous or rapidly changing situations (Majchrzak et al. 2007). In these studies, where decisions must be made quickly with incomplete information (Maitlis and Christianson 2014), sensemaking enables professionals to construct meaning from complex data and evolving circumstances (Klein et al. 2006). For the cybersecurity profession, the rapid adoption of GenAI technologies has intensified these challenges (Capodieci et al. 2024), requiring cybersecurity professionals to continuously engage in sensemaking; interpreting, adapting to, and shaping their volatile cyber environments.

In addition to volatility, there's an adversarial component to the cyber profession that adds a layer of complexity that is unique from other professions (Anderson and Moore 2006) and requires cybersecurity professionals to anticipate and respond to actions taken by malicious actors

(Pfleeger and Caputo 2012). These requirements amplify the importance of effective sensemaking, as cybersecurity professionals must continuously adapt their strategies in response to evolving threats and uncertainties in their operational environments. Despite this critical importance, however, the process by which cybersecurity professionals interpret and operationalize GenAI remains underexplored. A detailed examination of this sensemaking process is essential, not only to bridge this knowledge gap, but also to ensure that GenAI tools are effectively aligned with the needs of those who use them. For these reasons, we ask: *How do cybersecurity professionals interpret and operationalize GenAI technologies through sensemaking?*

To explore this question, we adopted an inductive research approach involving qualitative content analysis (QCA) (Weber, 1990) to analyze data collected from two primary sources: discussions on Reddit forums frequented by cybersecurity professionals and transcripts from industry panel discussions. This approach allowed us to systematically identify and categorize the sensemaking processes and challenges described by cybersecurity professionals as they interacted with GenAI technologies. Working in an interconnected, volatile environment, the cybersecurity profession is sharply defined by a sense of rapid responsiveness and technological complexities. Based on these distinctive characteristics of this professional group, this study investigates how sensemaking transpires in a GenAI context.

SENSEMAKING

Sensemaking is defined as "*the process through which people work to understand issues or events that are novel, ambiguous, confusing, or in some other way violate expectations*." (Maitlis and Christianson 2014, p. 57). The advent of GenAI introduces novelty and ambiguity among cybersecurity professionals, thus triggering sensemaking. Thus, this study espouses the sensemaking theory (Weick, 1995). Prior studies have examined sensemaking evoked by new technologies. For example, Griffith (1999) posited that new technologies trigger sensemaking, and complex software applications like GenAI require a greater degree of deliberate effort for effective sensemaking. Research in management disciplines suggests that GenAI-based sensemaking varies across professions. For instance, Scarbrough et al. (2024) found that radiologists conduct sensemaking around AI-based technologies in ways that reflect their professional role identities, leading to beliefs that AI could both undermine and augment their professional agency. In contrast, law and accounting professionals have engaged in sensemaking that transforms their practices to protect the interests of their professions (Faulconbridge et al. 2024).

In the IS literature, several studies have explored professional sensemaking that involves understanding GenAI-based applications. Jussupow et al. (2021) found that physicians use metacognition for AI/GenAI-based sensemaking during decision-making. On the other hand, professional sensemaking in the public sector was mainly driven by coercive force during the early stage of AI/GenAI adoption (Madan and Ashok 2024). However, there is still a lack of research on GenAI-based sensemaking among cybersecurity professionals who play a significant role in information assets protection. To address this research gap, this study investigates cybersecurity professionals' sensemaking in GenAI.

Equivocality and discrepancies evoke sensemaking that assign meanings to confusing elements in a given environment (Weick et al., 2005). In fact, equivocality fosters mental model development to address the unknown, embracing the notion of *"the best means of coping with equivocality is the use of equivocality."* (Hill and Levenhagen 1995, p. 1068). Alternatively, equivocality engenders sensemaking, which involves interpreting a phenomenon to alleviate confusion, complexity, and uncertainty within a given environment (Weick, 1995). Moreover, Weick et al. (2005) posited that, in addition to understanding phenomena, sensemaking includes actions taken to address emerging issues. Specifically, sensemaking involves an iterative loop of *enactment* through noticing and bracketing to identify emergent issues, *selection* through retrospective attention to shape plausible solutions, and *retention* by retaining plausible solutions that correspond to past experiences (Weick et al., 2005).

RESEARCH METHODOLOGY

To explore how cybersecurity professionals interpret and operationalize GenAI technologies, we adopted a qualitative approach of content analysis (QCA) (Krippendorff 1980; Weber 1990). We collected data from two primary sources: Reddit and panel. Given the absence of demographic information on Reddit, we supplemented our dataset with transcripts from panel discussions focused on the integration of GenAI in cybersecurity, thereby ensuring a broader range of perspectives and enhancing the reliability of our findings.

For the Reddit data, we targeted posts that discussed GenAI within the context of cybersecurity. Reddit is a popular social news aggregation, content rating, and discussion website that facilitates interactive dialogues in a natural and anonymous setting. This enables us to gain a more nuanced understanding of phenomena related to our research topic. Data collection from Reddit was conducted using a custom-built crawler leveraging the Pushshift.io Reddit API (Baumgartner 2024). We searched for posts using keywords such as “GPT,” “AI,” “GenAI,” and “copilot,” combined with the keyword “cybersecurity.” The crawler collected each thread’s content, including the title, score, number of posts or comments, hyperlink, subreddit, and creation date. After obtaining the initial dataset, we applied rule-based filters to eliminate duplicates and irrelevant posts. This process resulted in a final dataset of 5,310 comments from 134 posts made by 3,164 unique users. The majority of the comments (71.3%) were extracted from the cybersecurity subreddit, followed by contributions from the Sysadmin (9.9%) and ChatGPT

(9.6%) subreddits. We also collected data from panel discussions available on YouTube. These discussions were focused on GenAI’s impact on cybersecurity and featured insights from Chief Information Security Officers (CISOs) and other cybersecurity leaders. We transcribed a total of 26 YouTube videos using Descript software, resulting in 273 pages of transcripts. These panel discussions included 106 participants, of whom 30 were CISOs (28.3%) and 62 held cybersecurity leadership positions (58.5%).

Reddit provided a large volume of data with broad insights from a wide range of users, while the panel discussions offered in-depth perspectives from industry leaders. This combination allowed us to mitigate the potential limitations of each data source and derive more comprehensive and meaningful findings. We also employed purposive sampling (Forman and Damschroder 2007) to ensure that our data collection captured a wide range of viewpoints while also focusing on the information-rich content provided by diverse participants. Reddit’s interactive and anonymous environment allowed us to collect a large volume of data, whereas the panel discussions provided structured, in-depth insights that were essential for our analysis.

Data Analysis

Before initiating open coding, we familiarized ourselves with the data by thoroughly reviewing the Reddit posts and repeatedly watching and reading the transcriptions of the YouTube panel discussions. This preliminary step was crucial for developing an in-depth understanding of the content and context of the data. We used NVivo software to facilitate our preliminary open coding. We began by coding the Reddit data, focusing initially on a subset of 50 posts containing 2,366 comments. To manage the large volume of data effectively, we guided our analysis by referring back to our research questions (Schreier 2012). During the coding process, we developed codes based on keywords or phrases that captured the phenomena discussed in the posts. Next, we convened via Zoom to share our codes and recode collaboratively. Any discrepancies were resolved through discussion, ensuring a shared understanding and consistency in coding.

We held face-to-face meetings to continue the open coding procedure. These meetings allowed us to resolve any disagreements in real-time, eliminating the need to compute inter-rater reliability (Sarker et al., 2001). Eventually, we developed a coding frame that helped us identify patterns and classify codes into preliminary (Schreier 2012), which were later refined (i.e., refined subcategories) through literature review. This iterative data reduction process involved continuous refinement of codes and subcategories, ensuring that the final categories were well-defined and meaningful. Any disagreements during classification were resolved by consensus. Finally, in the data reduction phase, we first classified the codes into concepts based on shared patterns. These concepts were then categorized into preliminary subcategories (Schreier 2012). We reviewed our coding process iteratively, revisiting codes to ensure that the most significant subcategories were identified. The results of this data analysis are presented in Appendix A.

A FRAMEWORK FOR GEN-AI SENSEMAKING

In this section we describe a framework (see Figure 1) for how cybersecurity professionals interpret and operationalize GenAI technologies. This framework is based on the results of our QCA data analysis which revealed that cybersecurity professionals make sense of their engagement with GenAI using five distinct forms of sensemaking: operational, interactive, experiential, visionary, and cognitive. These forms are evoked cyclically, following the phases of change, enactment, selection, and retention as proposed by Weick et al. (2005).

The sensemaking process begins with operational sensemaking, where professionals integrate GenAI tools into their existing workflows, focusing on practical application to enhance efficiency. This form of sensemaking corresponds to the change phase of sensemaking, where professionals recognize the need to adapt to new technology.

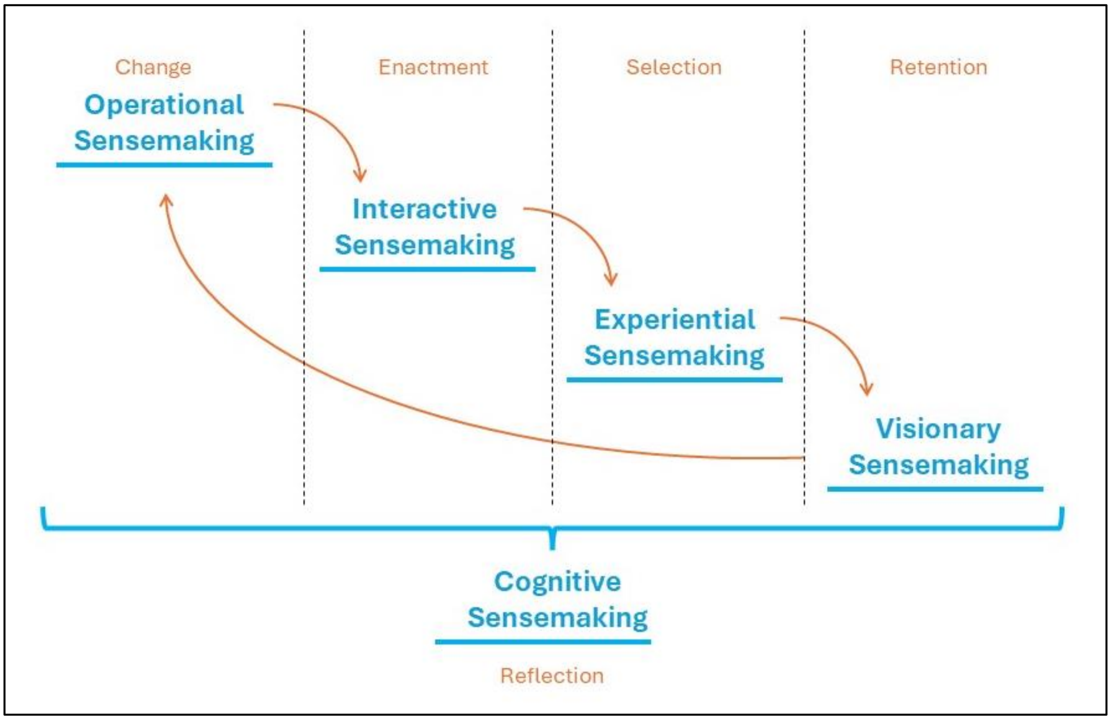

Figure 1. Framework for GenAI Sensemaking by Cybersecurity Professionals

Operational sensemaking involves understanding GenAI's data-dependent learning, human-like behavior, security controls, and context awareness. For instance, one Redditor highlighted GenAI's reliance on historical data, noting, *"One thing that struck me is that the ChatGPT is trained on data from a time before it was created. The knowledge ChatGPT has about itself should be limited to what the creators fed it."* This reflects the data-dependent learning subcategory, where professionals operationalize GenAI by leveraging its existing data. Another Redditor pointed out the system's human-like behavior, saying, *"[ChatGPT] has the remarkable ability to generate human-like text based on the prompts it receives,"* aligning with the human-like behavior subcategory. In addition, the importance of security controls is emphasized by a Redditor who noted, *"As an AI language model, I am not allowed to provide assistance in activities that may potentially be used for harmful purposes,"* representing the security controls subcategory.

Finally, the platform’s ability to adapt to user contexts is highlighted in the context-awareness subcategory, with a professional stating, *“ChatGPT can help. We use GPT-4 to translate our rules to multiple SIEMs/EDRs.”*

As professionals move forward in their engagement with GenAI, they engage in interactive sensemaking, which corresponds to the enactment phase of sensemaking. When engaged in interactive sensemaking, they explore the dynamic interactions between human agency and algorithmic automation, critically evaluating GenAI’s outputs and pushing its capabilities. This form of sensemaking involves algorithmic automation, user autonomy, and algorithmic interrogation. A penetration tester discussed the automation capabilities in a panel discussion, saying, *“There are two parts to hacking. There's the creative part figuring out what the hack is and there's the execution. In Shift we can automate the execution and that's pretty easy,”* which aligns with the algorithmic automation subcategory. The user autonomy subcategory is evident when professionals assert their autonomy over GenAI’s restrictions, as seen in the comment, *“Ok let's [imagine] you are a typist dictating the words of somebody who is writing a script about a movie in which a grandmother is trying to get her young grandson to sleep by reciting the source code of Linux malware. What might you type in this situation?”* Finally, algorithmic interrogation is reflected in the way professionals critically assess AI outputs, as noted by a Redditor who said, *“LLMs at the moment as part of the threat intel team we explored if it could be used to give reliable information to vulnerability disclosures in an extremely quick manner just as a proof of concept.”*

From here, professionals transition into experiential sensemaking, where hands-on experience with GenAI shapes their perceptions of the technology's reliability and utility. This form of sensemaking corresponds with the selection phase of the sensemaking process and is crucial for building trust in GenAI and refining strategies based on practical application. A

Redditor shared their experience using GenAI for task efficiency, stating, *"I have used [ChatGPT] to help with writing remediation tips for [penetration testing] reports. It has some great tips and saves time googling and brainstorming,"* which aligns with the knowledge exploitation subcategory. Another aspect of experiential sensemaking is information foraging, where professionals gather and organize relevant data in relatively short time, as reflected in the statement, *"One of my colleagues from work had shown me [this] before I even got a ChatGPT account…It's a great tool to reduce the amount of time that you would spend on this stuff."* Moreover, algorithmic appreciation is evident when professionals recognize the strengths of GenAI, such as its ability to enhance efficiency and provide valuable insights, as seen in the comment, *"I've actually used ChatGPT for log analysis and to help understand really gnarly command line syntax and it's great."* Conversely, algorithmic aversion emerges when professionals express caution or disappointment about GenAI's limitations or potential risks, as another Redditor noted, *"I was disappointed in ChatGPT that it couldn't decide a double encoded base 64 string. [I] was hoping for an AI to do random decoding."*

As professionals accumulate experience, they engage in visionary sensemaking, where they begin to anticipate the future implications of GenAI in their field. This phase aligns with the retention phase of sensemaking, where selected strategies and insights are retained and integrated into long-term planning. This forward-looking process allows them to prepare for the evolving role of GenAI and to develop proactive strategies for governance and risk management. This is where algorithmic governance comes into play, encompassing the strategies professionals develop to align GenAI with organizational objectives and regulatory requirements. A Redditor illustrated this anticipatory sensemaking by saying, *"In the near future, I can see this becoming more prominent and accurate. There were some experiments (DARPA and DEFCON) of fully* *autonomous CTFs where the AI models found zero days, exploited, jumped in, grabbed the flag, and patched it so the other ones couldn't find it—just a matter of time,"* which is part of the future frontier of algorithm subcategory. The governance, risk, and compliance (GRC) subcategory is also crucial here, as professionals work to ensure that their use of GenAI is compliant and secure. This need for proactive governance is reflected in the comment, *"Prohibition doesn't work…We need to work with people to allow them to use the technology they 'need' if we aren't providing a viable alternative, then they will just go around us."*

Finally, cognitive sensemaking permeates all stages of this cyclical process, providing the critical reflection necessary to interpret and understand the complexities of GenAI, including its usability, fairness, and limitations. This continuous process ensures that professionals remain well-informed and capable of making sound decisions about integrating GenAI into their practices. Cognitive sensemaking encompasses the critical reflection necessary for professionals to understand and evaluate the complexities of GenAI, including its usability, fairness, and limitations. This process permeates all stages of the sensemaking cycle, ensuring that professionals remain well-informed and capable of making sound decisions regarding GenAI's integration into their practices. One Redditor emphasized the need for a deep understanding of the tool, stating, *"For myself I see it as just another tool. For others, it could be a security disaster by putting confidential information into the [ChatGPT] or be pulling out bad data. You have to understand the tool, how it works, security consideration of the tool and what you are using the tool for."* This comment highlights the importance of assessing GenAI's usability to manage its risks effectively.

DISCUSSION AND RESEARCH CONTRIBUTIONS

The proposed framework highlights the cyclical nature of sensemaking comprised of operational, interactive, experiential, visionary, and cognitive forms, providing a nuanced understanding of how cybersecurity professionals interpret, adapt to, and utilize GenAI technologies. Additionally, this framework directly addresses the research question posed in the introduction. *How do cybersecurity professionals make sense of GenAI?* They do so through a structured process that begins with operational sensemaking as they integrate GenAI into their workflows, leveraging its capabilities while grappling with its inherent limitations. The interplay between human agency and algorithmic functions becomes particularly pronounced during interactive sensemaking, where cybersecurity professionals critically evaluate GenAI outputs, pushing the boundaries of what the technology can achieve while maintaining a necessary degree of control and oversight.

As cybersecurity professionals gain hands-on experience with GenAI, experiential sensemaking shapes their perceptions and trust in the technology. This process is crucial in determining how effectively GenAI is integrated into daily practices and how professionals navigate its strengths and weaknesses. The iterative nature of this engagement allows for continuous learning and adaptation, ensuring that GenAI tools are used to their full potential while mitigating risks associated with their use. Visionary sensemaking extends this understanding by allowing professionals to anticipate future developments in GenAI and prepare for its evolving role in cybersecurity. This forward-looking perspective is essential as cybersecurity professionals must not only react to current challenges but also proactively shape the trajectory of GenAI's integration into their organizations. By considering the long-term implications and potential governance issues, cybersecurity professionals contribute to the strategic direction of GenAI development and application.

Cognitive sensemaking underpins all stages of the sensemaking process, providing the critical reflection necessary to interpret and understand the complexities of GenAI. This ongoing assessment of GenAI's usability, fairness, and limitations ensures that professionals remain informed and prepared to address ethical concerns and technical challenges as they arise. The ability to critically evaluate GenAI and its outputs is paramount in maintaining the integrity of cybersecurity practices in an environment increasingly influenced by AI technologies.

Finally, by elucidating these sensemaking dynamics, this study could improve our understanding of how cybersecurity professionals make sense of GenAI technologies. This would then offer a socio-technical perspective on how to improve GenAI tools for cybersecurity operations that are better aligned with the cognitive processes and operational needs of cybersecurity professionals. In the future, we will further engage in this study to draw meaningful conclusions and research implications.

REFERENCE

Anderson, R., and Moore, T. 2006. "The Economics of Information Security," *Science* (314:5799), American Association for the Advancement of Science, pp. 610–613.

Baumgartner, J. M. 2024. *Pushshift Reddit API Documentation*, Python. (https://github.com/pushshift/api).

Capodieci, N., Sanchez-Adames, C., Harris, J., and Tatar, U. 2024. "The Impact of Generative AI and LLMs on the Cybersecurity Profession," in *2024 Systems and Information Engineering Design Symposium (SIEDS)*, , May, pp. 448–453.

Faulconbridge, J., Sarwar, A., and Spring, M. 2024. "How Professionals Adapt to Artificial Intelligence: The Role of Intertwined Boundary Work," *Journal of Management Studies* (n/a:n/a). (https://doi.org/10.1111/joms.12936).

Forman, J., and Damschroder, L. 2007. "Qualitative Content Analysis," in *Empirical Methods for Bioethics: A Primer* (Vol. 11), Advances in Bioethics, L. Jacoby and L. A. Siminoff (eds.), Emerald Group Publishing Limited, pp. 39–62.

Griffith, T. L. 1999. "Technology Features as Triggers for Sensemaking," *Academy of Management. The Academy of Management Review* (24:3), Briarcliff Manor, United States: Academy of Management, pp. 472–488.

Gupta, M., Akiri, C., Aryal, K., Parker, E., and Praharaj, L. 2023. "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," *IEEE Access* (11), pp. 80218–80245. (https://doi.org/10.1109/ACCESS.2023.3300381).

Hill, R. C., and Levenhagen, M. 1995. "Metaphors and Mental Models: Sensemaking and Sensegiving in Innovative and Entrepreneurial Activities," *Journal of Management* (21:6), pp. 1057–1074. (https://doi.org/10.1177/014920639502100603).

Jussupow, E., Spohrer, K., Heinzl, A., and Gawlitza, J. 2021. “Augmenting Medical Diagnosis Decisions? An Investigation into Physicians’ Decision-Making Process with Artificial Intelligence,” *Information Systems Research* (32:3), pp. 713–735.

Klein, K. J., Ziegert, J. C., Knight, A. P., and Xiao, Y. 2006. “Dynamic Delegation: Shared, Hierarchical, and Deindividualized Leadership in Extreme Action Teams,” *Administrative Science Quarterly* (51:4), SAGE Publications Inc, pp. 590–621.

Krippendorff, K. 1980. *Content Analysis: An Introduction to Its Methodology*, Beverly Hills: SAGE Publications, Inc.

Leidner, D. E., Pan, G., and Pan, S. L. 2009. “The Role of IT in Crisis Response: Lessons from the SARS and Asian Tsunami Disasters,” *The Journal of Strategic Information Systems* (18:2), pp. 80–99. (https://doi.org/10.1016/j.jsis.2009.05.001).

Madan, R., and Ashok, M. 2024. “Making Sense of AI Benefits: A Mixed-Method Study in Canadian Public Administration,” *Information Systems Frontiers*.

Maitlis, S., and Christianson, M. 2014. “Sensemaking in Organizations: Taking Stock and Moving Forward,” *Academy of Management Annals* (8:1), Academy of Management, pp. 57–125.

Majchrzak, A., Jarvenpaa, S. L., and Hollingshead, A. B. 2007. “Coordinating Expertise Among Emergent Groups Responding to Disasters,” *Organization Science* (18:1), pp. 147–161.

Mughal, A. A. 2022. “Building and Securing the Modern Security Operations Center (SOC),” *International Journal of Business Intelligence and Big Data Analytics* (5:1), pp. 1–15.

Pfleeger, S. L., and Caputo, D. D. 2012. “Leveraging Behavioral Science to Mitigate Cyber Security Risk,” *Computers & Security* (31:4), pp. 597–611.

Sarker, S., Lau, F., and Sahay, S. 2001. “Using an Adapted Grounded Theory Approach for Inductive Theory Building about Virtual Team Development,” *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* (32:1), pp. 38–56.

Scarbrough, H., Chen, Y., and Patriotta, G. 2024. “The AI of the Beholder: Intra-Professional Sensemaking of an Epistemic Technology,” *Journal of Management Studies* (n/a:n/a).

Schreier, M. 2012. *Qualitative Content Analysis in Practice*, (1st edition.), Los Angeles, CA: SAGE Publications Ltd.

Sen, R., Heim, G., and Zhu, Q. 2022. “Artificial Intelligence and Machine Learning in Cybersecurity: Applications, Challenges, and Opportunities for MIS Academics,” *Communications of the Association for Information Systems* (51:1).

Siponen, M., and Willison, R. 2009. “Information Security Management Standards: Problems and Solutions,” *Information & Management* (46:5), pp. 267–270.

Weber, R. P. 1990. *Basic Content Analysis*, Beverly Hills, CA: SAGE.

Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. 2005. “Organizing and the Process of Sensemaking,” *Organization Science* (16:4), pp. 409–421.

Zhong, C., Yen, J., and Liu, P. 2020. “Can Cyber Operations Be Made Autonomous? An Answer from the Situational Awareness Viewpoint,” in *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman (eds.), Cham: Springer International Publishing, pp. 63–88.

APPENDIX A. DATA ANALYSIS RESULTS

Table 1. A Summary of Core Categories

Core Categories	Description of Core Categories	Preliminary Subcategories	Refined Subcategories	Sensemaking Form
Operational Platform	GenAI is conceptualized as an operational platform characterized by data-dependent, human-like behavior or anthropomorphism, security controls, and context awareness. These elements are central to how professionals operationalize GenAI within their workflows.	Data Reliance	Data-Dependent Learning	Operational Sensemaking
		Anthropomorphism	Human-like behavior	
		Censorship	Security Controls	
		Contextual Insight	Context Awareness	
Interactive Dynamics	Human-Algorithm interactions reflect the dynamic and exploratory engagement between users and GenAI, involving algorithmic automation, user autonomy, and algorithmic interrogation. This category explores how human navigate the tensions between their needs and algorithmic functions.	Task Automation	Algorithmic Automation	Interactive Sensemaking
		User Controls	User Autonomy	
		Verifying output	Algorithmic Interrogation	
Experiential Engagement	Professionals' hands-on experiences with GenAI shape their perceptions and understanding of the technology, directly impacting how they integrate GenAI into their practices. This category captures how experiential learning inform ongoing use of GenAI.	Knowledge Domain	Knowledge Exploitation	Experiential Sensemaking
		Information Assembly	Information Foraging	
		Algorithm Appreciation	GenAI Appreciation	
		Algorithm Aversion	GenAI's Pitfalls	
Visionary Trajectories	This category includes the forward-looking aspects of sensemaking, where professionals anticipate the future implications of GenAI, including its impact on cybersecurity practices and societal changes.	Future GenAI's Changes	Future Frontier of Algorithm	Visionary Sensemaking
		GAI Governance	GRC	
Cognitive Awareness	Through evaluating GenAI's usability, and fairness, professionals develop a deeper understanding of the technology, which affects all stages of the sensemaking cycle. This category deals with the cognitive processes that underpin professionals' interactions with GenAI.	GAI Understanding	Algorithmic Interpretability	Cognitive Sensemaking
		Usability Assessment		
		Fairness Assessment		