

# Cyberpsychology: Integrating Cyber Behavioral Sciences with Adaptive Environments for Enhanced Cyber Deception

Marshall S. Rich  
Capital Technology University  
[mrich@captechu.edu](mailto:mrich@captechu.edu)

## Abstract

*As cyber threats evolve in complexity, there is a growing need to integrate Cyber Behavioral Sciences (CBS) and adaptive defense strategies into cybersecurity frameworks. This paper explores the potential of CBS and real-time adaptive testing environments (ATEs), such as moving target defense (MTD), to enhance cyber deception strategies. A comprehensive literature review and thematic analysis identifies critical gaps in the current research, including the lack of empirical validation, standardized performance metrics, and the underexplored role of organizational culture in cyber deception. The findings suggest that while theoretical models for CBS offer valuable insights into attacker behavior, practical implementations remain limited. However, by addressing these challenges, cybersecurity practitioners can create more dynamic, behaviorally informed defenses capable of responding to evolving adversarial tactics.*

**Keywords:** Cyberpsychology, Cyber Deception, Cyber Defense, Interdisciplinary Approaches, Behavioral and Cognitive Models

## 1. Introduction

As cybersecurity threats evolve, attackers increasingly use technical exploits and psychological manipulation to bypass defenses. Techniques like social engineering and deceptive attacks require defenses incorporating human behavior insights (Rich & Aiken, 2024). Cyber Behavioral Sciences (CBS)—an interdisciplinary field blending cyberpsychology, behavioral analysis, and cybersecurity—helps understand attacker and defender behaviors in digital environments (Aiken, 2016; Cranford et al., 2021). CBS enables cybersecurity practitioners to anticipate attacker decision-making and implement adaptive defense strategies that evolve with attack tactics.

An essential advancement in this area is the integration of CBS with real-time adaptive testing

environments (ATEs), such as Moving Target Defense (MTD). These dynamic systems continuously alter the attack surface, making it difficult for attackers to exploit vulnerabilities (Zhu et al., 2021; Crouse et al., 2015). By frequently shifting system configurations, MTD increases attack complexity and resource expenditure, reducing the likelihood of successful breaches.

Despite the promise of CBS and adaptive environments, significant research gaps still need to be addressed. These include the need for empirical validation, standardized performance metrics, and a deeper understanding of how organizational culture influences both attacker and defender behaviors (Wu et al., 2020; Liebowitz et al., 2021; Reeves & Ashenden, 2023). The urgency of addressing these challenges is essential for advancing CBS and cyber deception strategies in the face of increasingly complex threats.

This paper explores the intersection of CBS, cyber deception, and adaptive defense, emphasizing the need for empirical testing and standard metrics. By addressing these gaps, cybersecurity can become a more dynamic and behaviorally informed field capable of countering increasingly complex threats. The potential of CBS and adaptive environments to transform the field of cybersecurity is inspiring, offering hope for a more secure digital future (Achleitner et al., 2016; Cranford et al., 2021; Reti et al., 2022).

## 2. Literature Review

Integrating CBS with cybersecurity frameworks has gained increasing attention as cyber threats evolve. CBS, with its unique insights into human behavior, decision-making, and cognitive biases, holds the potential to revolutionize cyber defense strategies. This section reviews the existing research on CBS, cyber deception, ATEs, and MTD, identifying key contributions and gaps that must be addressed.

### 2.1 CBS in Cybersecurity

CBS is a field that delves into the psychological and cognitive aspects of both attackers and defenders in cyberspace. By incorporating the human element into

cybersecurity, CBS aids in identifying behavior patterns, cognitive biases, and decision-making tactics that attackers may exploit. Rich and Aiken (2024) and Aiken (2016) have pointed out that comprehending how cyber interactions influence human cognition and behavior can be a game-changer. The ability to exploit cognitive biases, such as overconfidence or predictability, can lead to the development of more potent defense strategies.

Cranford et al. (2021) expanded on this theory, demonstrating that CBS insights can create environments that manipulate attacker behavior and decision-making processes. By integrating CBS into cyber deception, defenders can steer attackers into making suboptimal decisions, thus improving the effectiveness of deception techniques. Despite the theoretical advancements, the practical application of CBS-informed strategies in real-world scenarios remains limited, highlighting a gap between theoretical development and operational implementation that requires further empirical research.

Diana et al. (2015) have explored multimodal deception detection using a t-pattern approach, which complements CBS by identifying patterns in human behavior that can enhance deception techniques. Their work underscores how CBS insights and behavior analysis can provide a more robust framework for detecting and manipulating adversarial actions in cyberspace. This further highlights the potential of CBS to shape a more behaviorally informed cyber defense strategy.

## 2.2 Cyber Deception Strategies

Cyber deception, which involves the strategic use of misinformation, decoy systems, or deceptive environments to mislead attackers, has significant potential for enhancing cybersecurity defenses. Almeshekah and Spafford (2014) have underscored the importance of thoughtfully planning and integrating deception into cybersecurity strategies. They argue that well-designed deception techniques can effectively slow attackers' progress and increase the likelihood of detection, offering a proactive approach to cyber defense.

The promise of cyber deception is evident in studies like Achleitner et al. (2016), which explored the use of virtual networks to defend against insider reconnaissance. Their findings showed that creating deceptive environments could obscure internal network structures, thereby complicating attackers' reconnaissance efforts. However, the scarcity of real-world validation of these methods underscores the urgent need for more empirical testing to establish their effectiveness in operational environments.

Sayed et al. (2024b) assessed how different types of probing impact adversarial decision-making in cyber deception. Their findings align with existing research by demonstrating how deception techniques manipulate attacker behavior. Using varied forms of probing, defenders can continuously challenge attackers, further complicating their decision-making processes and increasing the complexity of their actions at every stage.

Shortridge and Petrich (2022) discussed the next generation of cyber deception techniques, rapidly evolving to outmaneuver attackers. They highlighted how new methods target 'lambswool' attackers—those who are more easily deceived—by employing increasingly sophisticated tactics. Their work underscores the dynamic and exciting nature of cyber deception as strategies continue to evolve in response to advances in attacker methodologies, ensuring defenders remain one step ahead.

## 2.3 ATEs and MTD

ATEs dynamically adjust in response to adversarial actions, creating an ever-changing attack surface that makes it more difficult for attackers to gain footholds or plan their strategies. MTD, a subset of ATEs or adaptive strategies, alters the system's configuration or architecture to confuse attackers and disrupt their reconnaissance efforts. Crouse et al. (2015) conducted a probabilistic performance analysis of MTD and deception defenses, finding that adaptive environments significantly hinder attacker success by continually altering the network configuration.

Zhu et al. (2021) further underscored the potential of MTD, demonstrating how the perpetual variability in MTD environments disrupts attackers' ability to predict system behavior. This variability, achieved through frequent and unpredictable changes in the system's configuration or architecture, compels attackers to expend additional resources and time. However, more empirical research is needed to validate its effectiveness in diverse contexts. The authors stress that the promising potential of adaptive environments in operational settings is a beacon of hope for the future of cybersecurity, but it requires ongoing validation to be fully realized.

Chen et al. (2019) delved into attack intent analysis using attack path graphs, which offer valuable insights into how attackers might navigate an evolving attack surface. When applied within ATEs and CBS-informed strategies, this method can further mislead and manipulate attackers. By incorporating intent analysis into adaptive systems, defenders can anticipate attacker behaviors and dynamically adjust the environment to mislead adversaries, giving them a sense of control and empowerment in cybersecurity.

Osman et al. (2023) contributed by optimizing honeypot placement strategies using advanced algorithms, which are essential in adaptive deception techniques. Honeypots are decoy systems that attract attackers, further complicating their decision-making processes. Their research highlights how adaptive environments can optimize honeypot placements to enhance the effectiveness of cyber deception and divert attackers away from critical systems.

## 2.4 Performance Metrics and Empirical Validation

While theoretical advancements in CBS, cyber deception, and MTD show promise, a significant gap in the literature is the need for performance metrics to assess the effectiveness of these strategies. Wu et al. (2020) highlighted the importance of developing quantifiable performance indicators, such as attack success rates, time delays, and resource consumption, to measure the success of deception techniques. Without such metrics, evaluating the real-world impact of CBS and adaptive environments on cyber defense remains challenging.

Liebowitz et al. (2021) further noted that the absence of standardized metrics complicates comparing different cyber defense strategies. They argue that future research should focus on creating a consistent framework for assessing the effectiveness of adaptive and deception strategies across different operational environments. This framework would allow more rigorous testing and validation of CBS-informed approaches in live scenarios.

## 2.5 The Role of Organizational Culture

Another area that remains to be explored in the literature is the impact of organizational culture on both the deployment and effectiveness of cyber deception strategies. Reeves and Ashenden (2023) suggested that an organization's security culture significantly influences how well it can implement and maintain deception strategies. Organizations with a strong security culture are more likely to successfully deploy deception techniques and adapt to evolving threats, while those with weaker security practices may struggle with consistent implementation.

Organizational culture can also affect how attackers perceive and respond to deceptive environments. 'Structured adversaries', such as nation-state actors, are those with well-defined strategies and resources, and they may be less susceptible to deception. On the other hand, 'less organized adversaries', like hackers or script kiddies, are those with fewer resources and less strategic planning, and they may be more easily

manipulated (Cranford et al., 2021). Further research is needed to explore how cultural factors influence both attackers' and defenders' behaviors and how organizational practices can be aligned to maximize the effectiveness of cyber deception strategies.

## 2.6. Conclusion of Literature Review

While the theoretical groundwork for integrating CBS, ATEs, and MTD into cybersecurity is solid, significant gaps still need to be in implementing and validating these strategies. The lack of standardized performance metrics and the influence of organizational culture on cyber deception effectiveness are areas that require further exploration. Addressing these gaps will be critical for advancing the field and ensuring that CBS-informed defense strategies are theoretically sound and operationally effective.

## 3. Methodology

This study employed a targeted approach to explore the integration of CBS, cyber deception strategies, and ATEs. The methodology focused on conducting a scoping review to map existing literature and a thematic analysis to identify critical gaps, trends, and opportunities for future research.

### 3.1 Scoping Review

A comprehensive scoping review was conducted to provide an in-depth overview of research on CBS, cyber deception, and adaptive defense strategies. The review aimed to identify relevant studies published between 2006 and 2024, focusing on empirical research, theoretical models, and practical applications.

**3.1.1. Search Strategy and Inclusion Criteria.** The following databases were selected for their extensive coverage and reputation for high-quality research: ACM Digital Library, IEEE Xplore, and Google Scholar. The databases were searched using the following keywords: "cyber behavioral sciences," "cyber deception," "adaptive testing environments," "moving target defense," "cyberpsychology," and "defensive deception."

The inclusion criteria for the scoping review were:

- Peer-reviewed articles, conference proceedings, or significant technical reports.
- Relevance to CBS, cyber deception, or adaptive defense strategies.
- Focus on empirical data, theoretical models, or practical applications.

- Publication within the last 18 years.

**3.1.2. Study Selection.** After screening of abstracts and full texts, 33 studies (Table1) that met the inclusion criteria were carefully selected. These studies were chosen based on their significant relevance and credibility in the CBS and cyber deception fields.

Year	References
2006	2
2014	1
2015	2
2016	2
2017	1
2019	3
2020	2
2021	6
2022	3
2023	6
2024	5
<b>Total:</b>	<b>33</b>

**Table 1. References per Year.**

### 3.2 Thematic Analysis

A thematic analysis was performed to identify recurring themes, gaps, and trends within the selected literature. This method followed the approach outlined by Braun and Clarke (2006), focusing on coding the studies based on their key findings, methodologies, and implications for cyber defense.

#### 3.2.1. Primary Themes Identified.

1. **Design Thinking in Cyber Deception:** Ashenden et al. (2021) championed user-centered strategies through multidisciplinary collaboration, fostering creativity and paving the way for more potent deception tactics.
2. **Adaptive and Dynamic Defense Mechanisms:** Achleitner et al. (2016) used virtual networks and adaptive defense mechanisms. These mechanisms are designed to adjust and respond to changing attack scenarios in real-time, providing valuable insights into defense effectiveness against insider threats.
3. **Integration of Deception into Cybersecurity Frameworks:** Almeshekah and Spafford (2014) underscored the crucial role of strategic planning in integrating deception into cybersecurity. This

task can significantly strengthen frameworks but demands substantial planning efforts.

4. **Role-Based Deception Strategies:** Anjum et al. (2021) tailored deception strategies to specific organizational roles, providing targeted defenses but adding complexity to development and management.
5. **Game-Theoretic Models and Machine Learning:** Studies by Anwar et al. (2019) and Zhu et al. (2021) used game theory, a mathematical model of strategic interaction among rational decision-makers, and machine learning, a subset of artificial intelligence that enables systems to learn from data, to model attacker-defender interactions. However, these approaches require validation and substantial computational resources.
6. **Challenges in Performance Metrics:** Liebowitz et al. (2021) and Wu et al. (2020) highlighted the lack of standardized metrics for evaluating cyber deception, underscoring the need for rigorous and quantifiable assessments.
7. **Impact of Organizational Culture:** Reeves and Ashenden (2023) explored how organizational culture influences the success of deception strategies, emphasizing the critical role of security practices in effectiveness.
8. **Emerging Technologies and AI in Cyber Deception:** Zhu et al. (2021) addressed the threat of AI-driven attacks, underlining the necessity for continuous updates to stay ahead of the curve in the face of evolving adversarial technologies.
9. **Psychophysiology and Cognitive Processes:** Mertens (2006) and Cranford et al. (2021) examined cognitive mechanisms and psychophysiological responses in deception, though practical applications require further empirical validation.

#### 3.2.2. Identified Gaps and Trends.

1. **Cognitive Biases in Cyber Deception:** Studies like Aiken (2016) and Cranford et al. (2021) highlight how systematic patterns of deviation from norm or rationality in judgment can be exploited in defense strategies.
2. **Potential of Adaptive Environments:** Adaptive environments, as described by Crouse et al. (2015) and Zhu et al. (2021), are dynamic systems that can change their behavior or structure in response to an attacker's actions. These studies reveal the disruptive power of such environments in thwarting attacker reconnaissance and planning.
3. **Urgent need for Empirical Validation:** D'Almeida et al. (2023) identified the lack of rigorous empirical testing as a critical gap,

underlining the pressing need to validate CBS-informed and MTD strategies in real-world settings.

4. **Standardized Metrics:** Wu et al. (2020) and Liebowitz et al. (2021) stress the need for standardized metrics to compare the performance of different cyber deception strategies effectively.
5. **Integration of Advanced Technologies:** D'Almeida et al. (2023) noted challenges in incorporating AI and machine learning into deception strategies due to their rapid evolution and difficulty in developing explainable models.
6. **Organizational and Cultural Factors:** Reeves and Ashenden (2023) delve into how organizational culture and decision-making processes within Security Operations Centers significantly influence the success of cyber deception strategies, underscoring the paramount importance of these factors in implementation.

### 3.3 Conclusion of Methodology

By employing a targeted methodology that combined a focused scoping review with a detailed thematic analysis, this study comprehensively examines the current state of research on CBS, cyber deception, and adaptive environments. Identifying critical gaps, such as the need for empirical validation and standardized metrics, along with emerging trends like the integration of AI, underscores the significance of the study's findings and provides a strong foundation for advancing these fields in future research.

## 4. Findings

The findings from this study are based on a scoping review and thematic analysis of the literature on CBS, cyber deception, and ATEs. These findings highlight critical insights into these strategies' effectiveness while identifying significant gaps that must be addressed in future research.

### 4.1 CBS and Cyber Deception

CBS enhances cyber deception by exploiting attackers' cognitive biases and influencing their decision-making, leading to suboptimal choices and reduced attack success rates (Aiken, 2016; Cranford et al., 2021). Defenders can more effectively detect and mitigate adversarial behavior by integrating CBS with digital forensics, particularly in environments like Microsoft 365 (Rich, 2023a). Longitudinal studies on adversarial tactics underscore the importance of continuously adapting CBS-informed strategies, emphasizing the urgency of staying updated with

evolving threats (Rich, 2023b). Applying CBS to real-world scenarios such as phishing illustrates its practicality in countering user-targeted attacks (Zheng, 2023). Additionally, using AI and machine learning to predict adversary intent offers promising advancements for dynamic deception strategies (Shinde et al., 2021).

### 4.2 Effectiveness of ATEs and MTD

ATEs and MTD provide dynamic, adaptive environments that complicate attacker reconnaissance by continuously altering system configurations. Research shows that MTD significantly reduces attacker success rates by shifting the attack surface and delaying progress (Crouse et al., 2015; Zhu et al., 2021). When combined with CBS, these adaptive strategies enhance defenses by confusing attackers, as seen in studies involving phishing and social engineering reversals, such as the HackBot model (Achleitner et al., 2016; Lundie et al., 2024). Game-theoretic models, which analyze and predict the behavior of adversaries in strategic situations, support strategic decision-making by helping defenders anticipate and counter adversarial actions more effectively (Zhu, 2019). However, the effectiveness of adaptive environments depends on proper network resources, reinforcing the need for robust infrastructure (Sayed et al., 2024a). Real-world empirical validation remains a critical gap, underscoring the urgency of testing these strategies outside controlled environments.

### 4.3 Performance Metrics and Standardization Challenges

A critical challenge in cyber deception and adaptive testing strategies is the need for standardized performance metrics to evaluate their effectiveness. Metrics such as attack success rates, time delays, and resource consumption are essential for assessing the impact of these strategies (Wu et al., 2020). The dynamic and forward-looking nature of cyber threats necessitates the use of predictive models, which offer valuable insights into attacker behavior and highlight the need for more dynamic evaluation methods in cyber defense (Husák et al., 2020).

The inconsistency in evaluating deception strategies further underscores the importance of standardizing metrics across different environments (Neagoe & Bishop, 2006). Categorizing and measuring deception events can help quantify the severity of breaches and provide a systematic way to evaluate various techniques (Väisänen, 2017). The potential of standardized frameworks to compare and refine cyber defense strategies effectively is a beacon of hope,

making this a pressing issue for the field (Liebowitz et al., 2021).

#### 4.4 Role of Organizational Culture

A strong security culture significantly enhances the success of cyber deception strategies, as organizations with robust practices are better positioned to implement and maintain these techniques (Reeves & Ashenden, 2023). The *Cybersecurity Reciprocity Playbook* (Department of Defense, 2024) underscores the necessity of establishing security compliance frameworks that support effective deception strategies across organizations.

The impact of organizational structure on adversarial responses to deception is significant. Less organized groups, such as hacktivists or script kiddies, are more susceptible to cognitive manipulation, as noted by Cranford et al. (2021). This underscores the need for these organizations to address security gaps, as they may struggle to successfully apply deception, limiting its effectiveness.

#### 4.5. Gaps and Future Research Directions in Cyber Deception and CBS

Critical gaps have been identified in integrating cyber deception, cybersecurity, and CBS methodologies. Addressing these gaps through focused research could significantly enhance the effectiveness of cyber defenses. One key solution to these gaps is multidisciplinary integration, which emphasizes the need for collaboration and shared knowledge among different fields. This approach, along with adaptive testing and performance evaluation, is critical for the future of cyber deception.

**Table 2** outlines recommendations for advancing the field, such as developing more sophisticated behavioral models, incorporating AI for intent prediction, and rigorously establishing frameworks to assess deception strategies. Additionally, user-centric approaches are not just beneficial, but necessary for the success of cyber deception strategies. These approaches ensure that the end users are not just passive recipients of security measures, but active participants in their own protection. Gamified learning environments and accounting for irrational behaviors in predictive models further enhance the adaptability and robustness of these strategies.

Identified Gaps	Future Research
Integration of Multidisciplinary Insights	Develop methodologies that incorporate multidisciplinary insights for robust approaches to cyber deception.
Dynamic and Adaptive Testing	Implement adaptive testing mechanisms that evolve with new threats.
Behavioral and Cognitive Models	Develop more sophisticated models to predict deceptive behaviors; integrate AI for intent prediction.
Performance Evaluation	Establish comprehensive frameworks to rigorously assess deception strategies.
Advanced Technological Integration	Enhance methodologies with AI and machine learning to improve adaptability.
User-Centric Approaches	Incorporate user behavior into the design of deception strategies.
Interactive and Gamified Learning	Expand the use of interactive games and gamified learning environments.
Exploration of Irrational Behaviors	Develop models accounting for both rational and irrational behaviors.

**Table 2. Identified Gaps and Future Research.**

#### 4.6. Conclusion of Findings

This study's findings underscore the immense potential of CBS and cyber deception in enhancing cyber defense strategies. While significant gaps remain, particularly regarding empirical validation and the development of performance metrics, the promising insights from this research should instill optimism about the future of cybersecurity defense.

### 5. Discussion

This study explored the integration of CBS, ATEs, and MTD in enhancing cyber deception strategies. While these approaches offer significant potential for improving cybersecurity defenses, several critical challenges were identified. The discussion focuses on the implications of these findings, addressing the opportunities and limitations of current research.

#### 5.1 Practical Implications of CBS and Adaptive Environments

CBS offers a promising perspective for understanding and influencing attacker behavior. By leveraging cognitive biases, CBS can empower defenders to manipulate adversarial decision-making, thereby enhancing the effectiveness of cyber deception

(Aiken, 2016; Cranford et al., 2021). The potential to anticipate how attackers will respond to deception presents a significant advantage in designing defense strategies. However, as identified in the findings, this potential remains theoretical mainly due to a need for empirical validation. Future research must test CBS-based approaches in operational settings to determine their real-world efficacy.

ATEs and MTD offer further enhancements by dynamically shifting the attack surface, reducing the attacker's ability to plan and execute successful attacks. The Research by Crouse et al. (2015) and Zhu et al. (2021) shows that MTD can significantly disrupt attacker behavior, but, like CBS, its implementation in real-world environments is limited. While simulations demonstrate its effectiveness, the lack of operational testing raises questions about the practical feasibility of MTD and adaptive environments on a large scale. Future studies should prioritize testing these strategies in diverse, live environments to assess their applicability and scalability fully.

## 5.2 Challenges in Performance Evaluation

One of the critical challenges identified in this study is the urgent need for standardized performance metrics to evaluate the effectiveness of cyber deception strategies. With robust metrics, measuring the success of CBS-informed approaches and adaptive environments in real-world scenarios is easier. Wu et al. (2020) emphasize the need for quantifiable metrics, such as time delays and attack success rates, to assess how well these strategies manipulate adversarial behavior and delay attack progress.

The absence of standardized frameworks also limits the ability to compare different cyber defense strategies across various environments. As Liebowitz et al. (2021) pointed out, developing these metrics is critical for creating consistent evaluation methods. Metrics will enable cybersecurity professionals to refine and improve their defense strategies based on reliable, comparable data. Performance metrics should be an essential component of research in CBS and adaptive defense, ensuring these strategies can be evaluated standardized and practical.

## 5.3 Organizational Culture and Its Influence on Cyber Deception

The findings suggest that organizational culture plays a crucial role in determining the success of cyber deception strategies. As Reeves and Ashenden (2023) noted, organizations with strong security cultures are more capable of deploying and maintaining effective deception strategies. A robust security culture ensures

that deception techniques are implemented and continuously adapted to counter evolving threats.

However, the influence of organizational culture extends beyond just the defenders. Cranford et al. (2021) highlighted that adversarial groups, particularly nation-state actors, may respond differently to deception strategies based on organizational structure. While less organized groups, such as hacktivists, may be more susceptible to CBS-informed strategies, highly structured adversaries may be more resistant. A strong understanding of the adversary highlights the importance of tailoring cyber deception strategies to the specific characteristics of the organization and its potential adversaries. Future research should investigate the relationship between organizational culture and the success of CBS and deception strategies, focusing on how different adversary types react to deception.

## 5.4 Bridging Gaps and Advancing Research

Addressing the gaps identified in this study is crucial to fully realizing the potential of CBS and adaptive environments in cybersecurity. The most pressing need is for empirical validation. While the theoretical frameworks for CBS and adaptive strategies are well-established, their practical application still needs to be tested (Cranford et al., 2021). Empirical research should focus on testing these approaches in operational settings, determining their effectiveness against real-world threats, and refining the strategies based on these findings.

Another critical area is the development of performance metrics. Standardized metrics will allow for consistent evaluation and comparison of cyber deception strategies, providing a foundation for continuous improvement. Researchers should prioritize the creation of robust, quantifiable indicators to assess the success of CBS-informed and adaptive strategies in various contexts (Wu et al., 2020; Liebowitz et al., 2021).

Finally, the influence of organizational culture on cyber deception must be further explored. Understanding how different types of organizations and adversaries respond to deception will enable more targeted and effective defense strategies (Reeves & Ashenden, 2023).

## 5.5. Conclusion of Discussion

Integrating CBS, ATEs, and MTD has great potential for enhancing cybersecurity defenses. However, it's crucial to note that significant gaps remain in empirical validation, performance metrics, and organizational culture influence. Urgent action is needed to address these gaps, as doing so will be

essential to advancing the practical implementation of CBS-informed strategies and ensuring their effectiveness in real-world operational environments.

Prebot et al. (2022) contributed valuable insights into learning about simulated adversaries through interactive cyber-defense games. These simulations provide an effective platform for testing and validating CBS-informed defense strategies. By engaging with simulated adversaries in controlled environments, defenders can experiment with various adaptive techniques, such as adjusting defense mechanisms in response to changing attack patterns, and deceptive techniques, like misleading the adversary about the system's vulnerabilities, gaining deeper insights into adversary behaviors. This approach complements efforts to address the gaps in empirical validation by offering a safe and dynamic environment for real-time testing of CBS strategies.

## 6. Conclusions

This study has not only demonstrated the potential of integrating CBS, ATEs, and MTD into cybersecurity strategies, but also painted a promising picture for the future of cybersecurity. These approaches offer exciting avenues for enhancing cyber deception by exploiting attacker cognitive biases and creating dynamic, unpredictable defense environments. However, the study also highlights several key areas that must be addressed to advance the practical application of these strategies.

### 6.1 Implications for Cybersecurity

The integration of CBS into cyber defense can fundamentally shift how defenders' approach adversarial behavior. By anticipating and manipulating attacker decision-making, defenders can design more robust deception strategies that adapt to evolving cyber threats. ATEs and MTD further enhance this by adding layers of unpredictability, making it increasingly difficult for attackers to succeed. However, the implications of these strategies go beyond individual defenses—they necessitate an urgent and systemic shift in how organizations design, implement, and evaluate cyber defenses, particularly in the face of sophisticated and evolving threats.

The findings also suggest that organizational culture plays a significant role in determining the success of these strategies. Organizations with solid security cultures are better positioned to implement and adapt CBS-informed and deception-based defense mechanisms effectively. This underscores the practical implications for cybersecurity policy and training, suggesting that a focus on fostering security-aware

cultures is not just critical, but also a shared responsibility for the success of advanced cyber defense strategies.

### 6.2 Future Research Directions

To fully harness the potential of CBS, adaptive environments, and MTD, several vital gaps must be addressed through future research, which could significantly impact the field of cyber defense:

1. **Empirical Validation:** The lack of real-world testing for CBS-informed strategies and adaptive environments is a significant barrier to their practical adoption. Therefore, future research should prioritize empirical studies in operational settings to evaluate their effectiveness beyond controlled environments (Cranford et al., 2021; Achleitner et al., 2016).
2. **Development of Standardized Metrics:** The absence of standardized performance metrics hinders consistent evaluation of cyber defense strategies. Future work should prioritize developing quantifiable metrics to assess the success of cyber deception across various environments (Wu et al., 2020; Liebowitz et al., 2021).
3. **Exploration of Organizational Culture:** The influence of organizational culture on the success of CBS and adaptive defense strategies still needs to be explored. Research should investigate how different organizational structures and cultural practices impact the deployment and effectiveness of these strategies (Reeves & Ashenden, 2023).

### 6.3. Conclusion of Conclusions

In summary, while CBS, ATEs, and MTD hold significant promise for enhancing cybersecurity, addressing the identified gaps will be essential for their successful implementation. Through empirical validation, the development of performance metrics, and a deeper understanding of organizational culture, cybersecurity can evolve into a more dynamic, adaptive, and behaviorally informed field capable of countering the most sophisticated cyber threats.

The author did not receive funding from any organizations during the preparation of this manuscript.

## 7. References

- Achleitner, S., La Porta, T., McDaniel, P., Sugrim, S., Krishnamurthy, S. V., & Chadha, R. (2016, October 28). Cyber deception: Virtual networks to defend insider

- reconnaissance. In *Proceedings of the 2016 ACM Workshop on Moving Target Defense (MIST '16)* (pp. 57-68). ACM. <https://doi.org/10.1145/2995959.2995962>
- Aiken, M. P. (2016). "The Cyber Effect." New York, NY: Random House Spiegel & Grau.
- Almeshekah, M. H., & Spafford, E. H. (2014). Planning and integrating deception into computer security defenses. *Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14)*, 127-137. <https://doi.org/10.1145/2683467.2683482>
- Anjum, I., Zhu, M., Polinsky, I., Enck, W., Reiter, M. K., & Singh, M. P. (2021). Role-based deception in enterprise networks. In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21)* (pp. 65-76). ACM. <https://doi.org/10.1145/3422337.3447824>
- Anwar, A. H., Kamhoua, C., & Leslie, N. (2019). A game-theoretic framework for dynamic cyber deception in Internet of Battlefield Things. In *16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous), November 12–14, 2019, Houston, TX, USA* (pp. 1-5). Association for Computing Machinery. <https://doi.org/10.1145/3360774.3368204>
- Ashenden, D., Black, R., Reid, I. D., & Henderson, S. (2021). Design thinking for cyber deception. *Proceedings of the 54th Hawaii International Conference on System Sciences*, 1958-1967. <https://hdl.handle.net/10125/70853>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp063oa>
- Chen, B., Liu, Y., Li, S., & Gao, X. (2019). Attack intent analysis method based on attack path graph. *Proceedings of the 2019 International Conference on Computing, Networking and Security (ICCNS)*, Chongqing, China. Association for Computing Machinery. <https://doi.org/10.1145/3371676.3371680>
- Cranford, E. A., Gonzalez, C., Aggarwal, P., Tambe, M., Cooney, S., & Lebiere, C. (2021). Towards a cognitive theory of cyber deception. *Cognitive Science*, 45(7), e13013. <https://doi.org/10.1111/cogs.13013>
- Crouse, M., Prosser, B., & Fulp, E. W. (2015). Probabilistic performance analysis of moving target and deception reconnaissance defenses. In *Proceedings of the 1st ACM Workshop on Moving Target Defense* (pp. 21-29). ACM. <https://doi.org/10.1145/2808475.2808480>
- D'Almeida e Mendes, C. F., & Nogueira Rios, T. (2023). Explainable artificial intelligence and cybersecurity: A systematic literature review. *arXiv*. <https://arxiv.org/abs/2303.01259>
- Department of Defense. (2024, March). *Cybersecurity reciprocity playbook* (Version 1.0). <https://www.dod.mil/cybersecurity-reciprocity-playbook>
- Diana, B., Elia, M., Zurloni, V., Elia, A., Maisto, A., & Pelosi, S. (2015). Multimodal deception detection: A t-pattern approach. *Proceedings of the ACM International Conference on Multimodal Interaction (ICMI '15)*, 13 November 2015, Seattle, WA, USA. ACM. <https://doi.org/10.1145/2823465.2823466>
- Husák, M., Bartoš, V., Sokol, P., & Gajdoš, A. (2020). Predictive methods in cyber defense: Current experience and research challenges. *Future Generation Computer Systems*. <https://doi.org/10.1016/j.future.2020.01.004>
- Liebowitz, D., Nepal, S., Moore, K., Christopher, C. J., Kanhere, S. S., Nguyen, D., Timmer, R. C., Longland, M., & Rathakumar, K. (2021). Deception for cyber defence: Challenges and opportunities. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 173-182. <https://doi.org/10.1109/TPSISA52974.2021.00020>
- Lundie, M. J., Lindke, K. L., Aiken, M. P., Janosek, D. M., & Amos-Binks, A. (2024). The enterprise strikes back: Conceptualizing the HackBot - Reversing social engineering in the cyber defense context. *Proceedings of the 57th Hawaii International Conference on System Sciences*. <https://hdl.handle.net/10125/106496>
- Mertens, R. (2006). *The role of psychophysiology in forensic assessments: Deception detection, ERPs and virtual reality mock crime scenarios* (Doctoral dissertation, University of Arizona). ProQuest Dissertations Publishing. (UMI No. 3206067).
- Neagoe, V., & Bishop, M. (2006). *Inconsistency in deception for defense*. Proceedings of the 2006 New Security Paradigms Workshop (NSPW 2006), Schloss Dagstuhl, Germany. Association for Computing Machinery. <https://doi.org/10.1145/1278940.1278946>
- Osman, M., Nadeem, T., Hemida, A., & Kamhoua, C. (2023). Optimizing honeypot placement strategies with graph neural networks for enhanced resilience via cyber deception. In *Proceedings of the 2nd Graph Neural Networking Workshop 2023 (GNNet '23)*, December 8, 2023, Paris, France. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3630049.3630169>
- Prebot, B., Du, Y., & Gonzalez, C. (2022). Learning about simulated adversaries from human defenders using interactive cyber-defense games. *Journal of Cybersecurity*, 1-15. [https://doi.org/DOI\\_HERE](https://doi.org/DOI_HERE)
- Reeves, A., & Ashenden, D. (2023). Understanding decision making in security operations centres: Building the case for cyber deception technology. *Frontiers in Psychology*, 14, Article 1165705. <https://doi.org/10.3389/fpsyg.2023.1165705>
- Reti, D., Elzer, K., Fraunholz, D., Schneider, D., & Schotten, H. D. (2022). Evaluating deception and moving target defense with network attack simulation. In *Proceedings of the 9th ACM Workshop on Moving Target Defense (MTD '22)*, November 7, 2022, Los Angeles, CA, USA. ACM, New York, NY, USA. <https://doi.org/10.1145/3560828.3564006>
- Rich, M. S. (2023a). Enhancing Microsoft 365 security: Integrating digital forensics analysis to detect and mitigate adversarial behavior patterns. *Forensic Science*, 3(3), 394-425. <https://doi.org/10.3390/forensicsci3030030>
- Rich, M. S. (2023b). Cyberpsychology: A longitudinal analysis of cyber adversarial tactics and techniques. *Analytics*, 2(3), 618-655. <https://doi.org/10.3390/analytics2030035>
- Rich, M. S., & Aiken, M. P. (2024). An interdisciplinary approach to enhancing cyber threat prediction utilizing

- forensic cyberpsychology and digital forensics. *Forensic Sciences*, 4(1), 110-151.  
<https://doi.org/10.3390/forensicsci4010008>
- Sayed, M. A., Rahman, M., Khan, M. A. I., & Tosh, D. (2024a). A survey of network requirements for enabling effective cyber deception. *arXiv preprint arXiv:2309.00184v3*. Retrieved from  
<https://arxiv.org/abs/2309.00184v3>
- Sayed, M. A., Khan, M. A. I., Allsup, B. A., Zamora, J., & Aggarwal, P. (2024b). Assessing the influence of different types of probing on adversarial decision-making in a deception game. *arXiv*.  
<https://arxiv.org/abs/2310.10662v3>
- Shinde, A., Doshi, P., & Setayeshfar, O. (2021). Cyber attack intent recognition and active deception using factored interactive POMDPs. In *Proceedings of the 20th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2021)* (pp. 1200-1208). International Foundation for Autonomous Agents and Multiagent Systems.  
<https://doi.org/10.5555/3463952.3464091>
- Shorridge, K., & Petrich, R. (2022). Lamboozling attackers: A new generation of deception. *Communications of the ACM*, 65(6), 44-53. <https://doi.org/10.1145/3498578>
- Väisänen, T. (2017). Categorization of cyber security deception events for measuring the severity level of advanced targeted breaches. In *Proceedings of the 11th European Conference on Software Architecture (ECSA '17)*, Canterbury, United Kingdom, September 11–15, 2017 (pp. 7). Association for Computing Machinery.  
<https://doi.org/10.1145/3129790.3129805>
- Wu, H., Gu, Y., Cheng, G., & Zhou, Y. (2020). Effectiveness evaluation method for cyber deception based on dynamic Bayesian attack graph. In *Proceedings of the 2020 3rd International Conference on Computer Science and Software Engineering (CSSE'20)* (pp. 1-9). Association for Computing Machinery.  
<https://doi.org/10.1145/3403746.3403897>
- Zheng, S. Y. (2023). *Online scam detection using human psychology: Towards usable cybersecurity* (Doctoral dissertation). University College London (UCL).
- Zhu, M., Anwar, A. H., Wan, Z., Cho, J.-H., Kamhoua, C. A., & Singh, M. P. (2021). A survey of defensive deception: Approaches using game theory and machine learning. *IEEE Communications Surveys & Tutorials*, 23(4), 2460-2493.  
<https://doi.org/10.1109/COMST.2021.3102874>
- Zhu, Q. (2019). *Game theory for cyber deception: A tutorial*. In *Proceedings of the 2019 ACM Conference on Hot Topics in the Science of Security (HoTSoS '19)* (pp. 1–3). ACM. <https://doi.org/10.1145/3314058.3314067>