

Evaluating Cognitive Security in an Operationally Relevant Field Environment

Sarh R. Bostrom^{1,*}, Victoria Leppert¹, Ana Flynn¹, Talmadge Hollowell¹, Gianna Martyna¹, Michael Couri¹,
Kaylee I. Stouder¹, Melissa McLain^{1,2}, Ewart J. de Visser¹, Leanne Hirshfield², and Richard E. Niemeyer¹

* Corresponding Author: Sarah.Bostrom.CTR@afacademy.af.edu

¹ United States Air Force Academy
Air Force Academy, USA

² University of Colorado Boulder
Boulder, USA

Abstract— Cognitive security highlights the protection of human cognition and information processing systems from undue influence from surrounding information environments. While most research exists in a tightly controlled lab setting, additional research is needed to examine the effects in real-world and field-based environments. Within a military Joint Operations Center context, it is crucial for all team members to make accurate and timely decisions in potentially chaotic high information density (HID) environments. In a simulated field environment at the United States Air Force Academy, we are engaged in an ongoing effort to collect audio and survey data to assess the cognitive security of individuals and teams engaged in a realistic war game simulation. Daily information updates are delivered to each component team (air, land, marine, space, cyber, and special operations) at the beginning of all four simulation days. Three of the total 24 information updates contain false information that contradicts the correct information available from reliable sources in the simulation. Using surveys collected during debriefs, we assess outcomes related to cognitive security including veracity discernment and confidence in accuracy judgements. We present these exploratory findings both in aggregate and by component team to assess individual and group dynamics. These exploratory findings are some of the first assessing cognitive security in operationally relevant field-based environments during task completion.

Keywords— cognitive security, information processing, veracity discernment, teams

I. INTRODUCTION

In the modern era, the nature of conflict has undergone a profound transformation. Moving beyond the traditional physical domains of land, air, and sea and transitioning to include the cognitive space, the realm of human information processing and decision-making [1] [2]. This is particularly evident in the systematic political warfare campaigns waged by foreign powers that seek to exploit cognitive weaknesses and subvert democratic processes through information technology (see e.g., [3] [4]). This fundamental shift means that effective cognitive security is needed for military advantage [3] [5]. Cognitive security represents the protection of human cognition and information processing systems from undue influence of surrounding information environments and is the necessary

defense of the human mind against strategic manipulation [1] [3] [6].

While most research exists in controlled laboratory settings (see e.g., [7] [8]), additional work is needed to examine the effects of cognitive security in real-world and field-based environments. Within a military Joint Operations Center context, it is crucial for all team members to make accurate and timely decisions in chaotic and high information density environments [9]. Despite its importance, cognitive security research with these environments is lacking.

This study examines the cognitive security of individuals and teams in a simulated Joint Operations Center field environment. Specifically, we unpack cognitive security by examining veracity discernment and judgement confidence outcomes by team.

II. BACKGROUND

A. Cognitive Security

The cognitive security research space examines efforts to protect humans from information threats to cognitive processes, such as reasoning and decision making [10] [11]. This concept sits at the intersection of military information operations and academic information processing, leading to divergent approaches. Within the military literature, cognitive security typically emphasizes the manipulation of information environments and defines it in terms of adversarial shaping of perceptions and judgements in cognitive warfare, political warfare, and psychological operations [1] [5]. West Point's Cognitive Security Research Lab defines cognitive security as protecting rational decision-making during adversarial attacks [6]. Similarly, NATO situates the importance of improving human cognition both for normal tasks and maintaining resilience during cognitive attacks [3] highlighting the adversarial nature of cognitive security within the military perspective. In this framing, cognition is a battlespace and the objective is to influence or disrupt opponent decision-making.

Academic work, by contrast, studies internal cognitive processing, vulnerability to disruption of information processing, and belief formation [12] [13]. It focuses on how

individuals evaluate, update, and integrate information. These perspectives rely on models of susceptibility, misinformation spread, and belief updating to explain why information influence succeeds and perpetuates [14] [15] [16]. Despite emphasizing different mechanisms, both communities agree that cognition can be influenced through the information environment and that protective measures are increasingly necessary in the modern technological world.

References [10], [17], and [18] note that research has relied heavily on veracity discernment—the ability to identify true versus false information—despite this only being a partial indicator. Without considering the importance of accurate identification of accurate information, cognitive security interventions may backfire and produce more critical information consumers that tend to accurately identify false information as a result of reduced belief and increased skepticism in all information (see e.g., [19] [20] [21]) which may not be protective during a cognitive attack. Further, without considering confidence in veracity discernment judgements, cognitive security may be capturing accuracy guesses as well as accurate discernment.

Assessing individual level cognitive security requires comprehensive measurable outcomes [22]. Specifically, [10] and [17] argue that meaningful outcomes of cognitive security are threefold: 1) veracity discernment, 2) decision-making, and 3) propagation following exposure. Additional vulnerabilities include susceptibility to cognitive biases, effective metacognition regulation, and avoidance of behaviors that amplify misinformation such as uncritical sharing [23] [24]. Together, these outcomes frame cognitive security as the capacity to judge information correctly and maintain sound cognition with adaptive behavior when confronted with information threats.

B. The Need for Ecologically Valid Research

According to [18], only one percent of studies in misinformation research measure the impact on real, observable behavior, highlighting a substantial gap between laboratory findings and natural occurrences. Reference [7] argues that exposure to misinformation occurs within individuals’ private and occupational contexts with impacts shaped by psychological and neurophysiological susceptibilities. Consequently, research designs that integrate psychological and neural mechanisms with real world tasks and interaction are needed. Similarly, [8] distinguishes between lab based efficacy and real world effectiveness of interventions. Specifically, they state that most misinformation research relies on item-level accuracy judgements, self-reported intentions, and short-term post-intervention measures rather than behavioral outcomes and argue this approach overlooks real-world behavior, durability of effects, uptake across populations, and broader system level dynamics that shape information environments. Together, these critiques indicate that without stronger ecological validity, cognitive security research may systematically overestimate both susceptibility mechanisms and intervention efficacy.

III. CURRENT STUDY

The current study addresses the gap in operationally relevant cognitive security research by examining cognitive security of

individuals and teams in a simulated Joint Domain Operations Center (JDOC) field-environment. Specifically, we address the following research questions:

- 1) *What is the relationship between judgement accuracy and degree of confidence in the judgement?*
- 2) *What is the distribution of cognitive security and does it vary by team?*
- 3) *What is the relationship between trust in team, psychological safety, workload, and cognitive security?*

A. Data

The Multi-Domain Laboratory (MDL) is a simulated joint-domain operations center (JDOC) at the United States Air Force Academy. The testbed environment contains 24 operations center workstations and multiple communications modalities including voice and chat functionalities providing high ecological validity. Each class using the MDL includes approximately 20-24 undergraduate cadets assigned to different component teams or leadership roles. Each role includes unique subtasks and responsibilities. The teams are air, land, marine, space, cyber, and special operations. Seven participants (two in each participating class section) were responsible for coordination and leadership in the joint operations and joint force commander roles. Teams were assigned during the course and membership was held constant across MDL execution sessions. Table 1 displays the distribution of team membership in the sample.

Data collection was embedded in the simulated wargame of a core curriculum class with strategically designed information supplement messages pushed to each team for veracity discernment. A unique information supplement was pushed to each team at the beginning of each execution session (total 24 information supplements). Three of these information supplements were false and directly contradicted reliable information available in the simulation. During the semester, cadets study military course of action (COA) development and strategy in the classroom and enact these COAs with real time adaptation to enemy attacks initiated by the instructor during execution in the MDL. Mission execution of the wargame simulation occurs in four one-hour blocks of time each followed by a one-hour debrief session to review performance and adjust as needed prior to the next execution session.

TABLE I. DISTRIBUTION OF TEAM MEMBERSHIP (N=86)

	F	Percent
Air	22	25.58%
Land	22	25.58%
Maritime	12	13.95%
Space	5	5.81%
Cyber	8	9.30%
Spec. Ops.	10	11.63%
J3 & JFC	7	8.14%

Across the four MDL debrief sessions, we collected 216 surveys from 86 participants. Surveys asked participants to reflect on their decision making during MDL execution sessions including assessment of the information supplement. All data collection procedures were approved by the United States Air Force Academy Human Research Protections Program (FAC202500012E).

B. Measures

The outcome of interest is a novel measure of cognitive security that combines an assessment of accuracy of veracity discernment and degree of confidence in the assessment (multiplies accuracy by confidence). In line with [22] the component accuracy measure captures the correct identification of both accurate and inaccurate information. Cognitive security ranges from -1 to 1 with -1 indicating an inaccurate assessment and low confidence, 0 indicating medium confidence and chance accuracy, and 1 indicating an accurate assessment and high confidence. The mean cognitive security for this sample was 0.20 indicating at least medium confidence in accurate assessments.

The key independent variables related to the outcomes of interest are based in the teamwork literature and include trust in team [25], psychological safety [26], and workload [27]. The survey items were administered during each of the four debrief sessions. Descriptive statistics are presented in Table 2.

Trust in team and team processes is six item likert scale measure developed by [28] and down selected by [29]. Trust in team ranges from a minimum score of 1 to a maximum score of 5. The mean trust for the sample is 4.18.

Psychological safety is a seven item likert scale measure developed by [30] to assess perceived safety of interpersonal risk taking within a team context. Psychological safety ranges from a minimum score of 1 to a maximum score of 7. The mean psychological safety for this sample is 4.11.

Workload is measured using the 6 primary dimensions of the NASA task load index [31]. Participants rated mental demand, physical demand, temporal demand, performance, effort, and frustration on a 21 point scale from very low to very high demand. Workload ranges from a minimum score of 1 to a maximum score of 21. The mean workload of this sample is 12.10.

TABLE II. SAMPLE DESCRIPTIVE STATISTICS

	N	Mean ^a (%)	Std. Dev.	Min.	Max.
Cognitive Security	85	0.20	0.48	-1.00	1.00
Accuracy	86	1.73	0.33	1.00	2.00
Confidence	85	0.68	0.19	0.00	1.00
Trust in Team	86	4.18	0.54	1.78	5.00
Psychological Safety	86	4.11	0.48	2.50	5.79
Workload	86	12.10	3.34	5.33	21.00

^a Means were calculated across responses at all time points excluding missing values

C. Analysis

The current study first visualizes the novel measure of cognitive security by plotting accuracy by degree of confidence and the distribution of cognitive security. Next, we run examine differences in cognitive security by team. Finally, we calculate correlations to assess bivariate relationships between the variables of interest.

D. Findings

To address research question 1, we plot average confidence in assessment by average discernment accuracy in Fig. 1 and draw quadrant lines. Points in the right two quadrants represent mostly accurate judgements while points in the right two quadrants are mostly inaccurate judgements. Points on the y-quadrant axis represent those who were accurate in half of judgements. Points in the upper two quadrants exhibited high or very high confidence while those in the lower two quadrants stated low or very low confidence in their accuracy judgements. Points on the x-quadrant axis represented those with medium confidence in the accuracy judgements. The largest proportion of the sample was accurate and confident in their judgements. However, most of the sample was confident in their accuracy judgements regardless of accuracy potentially revealing over confidence in their veracity discernment abilities.

To address research question 2, we first examine the distribution of a novel measure of cognitive security (comprised of veracity discernment accuracy and degree of confidence in the judgment; $\bar{x}=0.20$) across 85 participants in Fig. 2. The vast majority of the sample exhibits accurate judgements with high or very high confidence (scores above zero). Scores below -0.5 are inaccurate with low or very low confidence. Scores between -0.5 and 0 are either accurate with low confidence or inaccurate with high confidence, both issues for tasks requiring accurate and confident decisions in a timely manner.

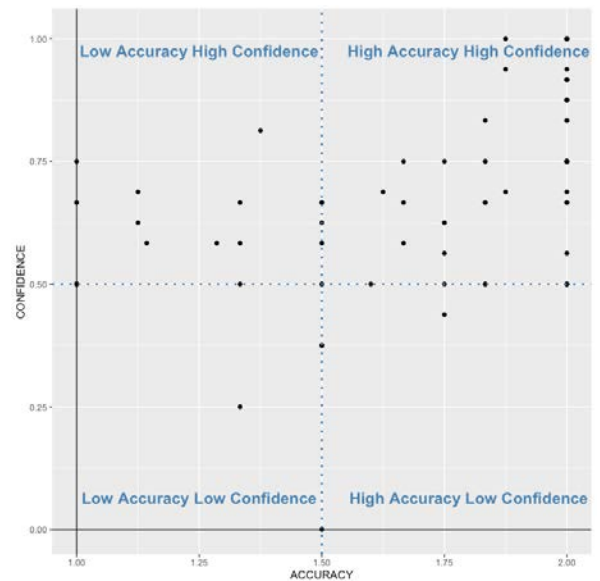


Fig. 1. Confidence by Accuracy Plot

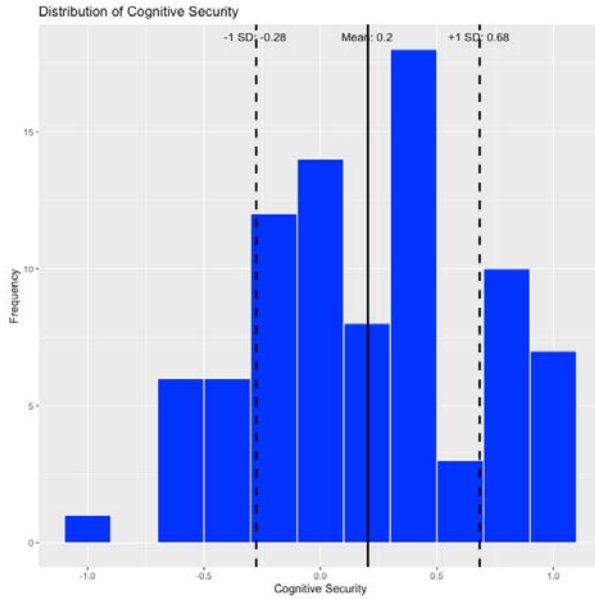


Fig. 4. Distribution of Cognitive Security

Finally, we examine the mean cognitive security by team. Only the Air, Cyber, and Space teams received inaccurate information. Leadership positions (J3 and JFC) were able to see each team’s information supplement in a global view. Fig. 3 presents mean cognitive security by team. Teams with a higher mean cognitive security score are both more accurate and more confident in their judgements. The leadership and coordination positions (J3 and JFC) have the highest cognitive security scores (J3 $\bar{x}=0.47$; JFC $\bar{x}=0.36$) while maritime has the lowest score ($\bar{x}= -0.05$). While theoretical cognitive security scores can range from -1 to 1, all teams except maritime have positive cognitive security scores indicating better than chance veracity discernment accuracy and high confidence. While maritime’s

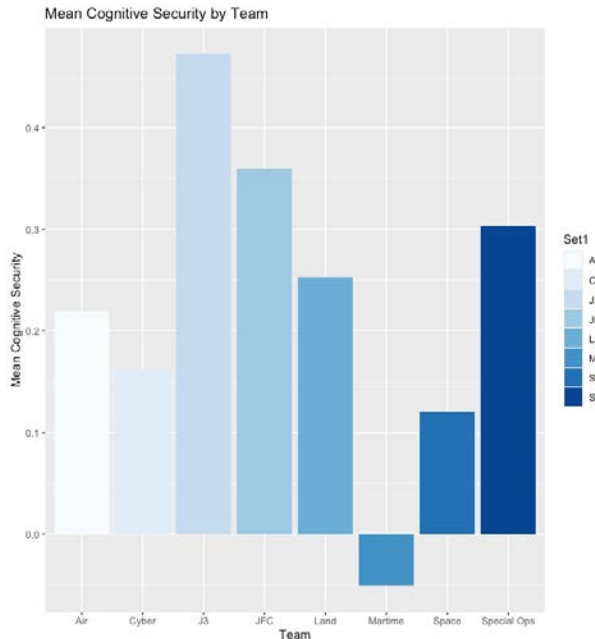


Fig. 3. Mean Cognitive Security by Team

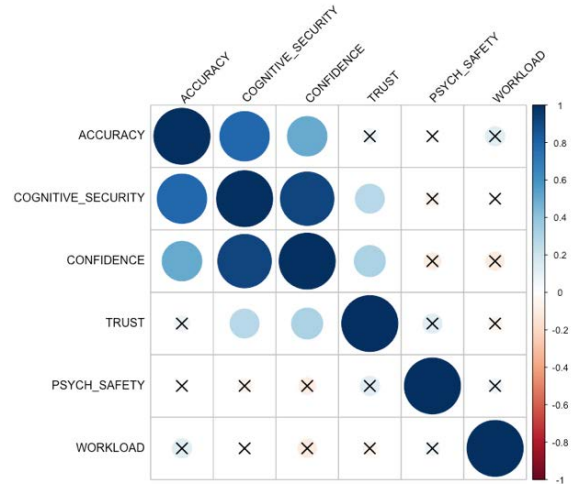


Fig. 2. Correlation Matrix

mean cognitive security score is the lowest, it is very close to zero. For this team, the low score reflects lower than chance veracity discernment ($\bar{x}=1.44$) and above medium confidence ($\bar{x}=0.61$) in their judgements despite receiving accurate information supplements.

We calculate Pearson correlations across the variables of interest to determine bivariable relationships to address research question 3. The correlation matrix is presented in Fig. 4. Notably, there are moderate relationships between judgement accuracy and degree of confidence ($r=0.50$, $p<0.001$) and trust in team and degree of confidence ($r=0.31$, $p<0.01$). There is a weak relationship between trust in team and cognitive security ($r=0.27$, $p<0.05$). We ignore the substantial correlations between cognitive security and both accuracy and confidence as these variables are used to calculate cognitive security. Unfortunately, low sample size ($n=85$) prevents us from further investigating the Maritime team’s low mean cognitive security score by trust in team, the next step suggested by the bivariate findings.

IV. DISCUSSION

Much cognitive security research takes place in lab-based settings that measure cognitive security as veracity discernment [7] [8] [18] [22]. This study uses an ecologically valid simulated JDOC environment with realistic teams and roles to study cognitive security. Embracing the naturalistic environment has consequences for measuring cognitive security. In alignment with [10]’s call, this study moves beyond veracity discernment uses a novel measure of cognitive security that considers both veracity discernment and degree of confidence in accuracy judgements, both crucial components of leadership and role responsibilities in JDOC environments.

A. Implications for Cognitive Security

In plotting degree of confidence by judgement accuracy, the majority of the sample displayed at least medium confidence in their judgements regardless of the actual judgement accuracy. This aligns with literature that states that individuals often

exhibit a fallacy of expertise and overestimate their ability to correctly discern accurate from inaccurate information [32] [33]. Within this sample, this finding could be related to cadet's relatively low level of operational experience despite being knowledgeable regarding the parameters of the wargame simulation.

There is also a subset of participants that make correct accuracy judgements but exhibit low confidence. These participants may be guessing at information discernment and are also a problematic or less cognitively secure group. While not a large portion of the sample, it is still important to recognize that both accuracy and confidence are important aspects of cognitive security in simulated Joint Operations Center environments requiring accurate decisions made in a timely manner [9]. Good leaders in these environments need to be confident in the decisions they are making and conveying to other team members.

While this measure of cognitive security is an advancement, it is not a fully comprehensive measure (limited to veracity discernment and confidence without including behavior or propagation). Future work should validate this measure, compare it to existing measures, and develop a validated fully comprehensive measure of cognitive security. This could serve as the basis for the integration of academic research and military theory with abstract cognitive security concepts and measures translating into operationally relevant outcomes [10] [11]. This integration enables research in military contexts to define, measure, and evaluate cognitive security in applied, naturalistic environments allowing a greater understanding of how beliefs are shaped by information environments and how they affect judgment and decision-making under operational conditions.

B. Limitations and Future Research

While this study makes important contributions to cognitive security research in Joint Operations Center environments, it does have some limitations. First, the current study presents only descriptive and bivariate statistics due to the low sample size. While 86 participants across the span of four data collection sessions is impressive, it does not reach the threshold for more complex multivariate models. This limits our ability to unpack the low maritime cognitive security score by trust in team or other key predictors. Future research should complete similar work with the larger sample sizes needed for multivariate statistical models. This can move beyond describing cognitive security in operationally relevant environments to predicting it.

Next, this study's participants are non-expert undergraduate cadets. While they are experts in the scenario and have some operational training, they do not have prior operational experience working in a JDOC. The findings regarding cognitive security may not generalize to those that routinely work in Joint Operation Center environments. [34] demonstrates that expertise is a critical factor to decision-making in chaotic and fast paced environments. Future work should extend this study to a simulated Joint Operations Center environment with participants that have relevant operational experience.

Finally, this study takes place in a simulated JDOC field environment with many design components outside the control

of the research team. This includes the number of participants on the fourth execution day (e.g., two instructors cancelled the fourth execution day due to class performance) and challenges tied to observational data collection during planned class lessons (e.g., inability to fully pilot the data collection procedures prior to the start of data collection and inability to keep data collection window open to increase sample size based on course lesson scheduling/ requirement to wait until next semester for additional rounds of data collection). To address these limitations, future research should consider designing an ecologically valid and operationally relevant task and testbed in a lab-based environment. Such a testbed could bridge the gap between the need for ecologically valid and real world data and the need for researcher control of experimental design and sample size.

C. Contributions and Conclusion

Despite its limitations, this study makes three important contributions. First, the descriptive and bivariate findings present an exploratory look at cognitive security in an operationally relevant simulated JDOC environment, a research space often overlooked by existing research. In our examination of veracity discernment, we highlight the importance of both correctly identifying inaccurate and accurate information. Further we examine the relationship between veracity discernment and other variables of interest including confidence in accuracy judgements. Finally, we explore a novel measure of cognitive security that considers both veracity discernment and degree of confidence. It is crucial for operators in Joint Operation Center environments to safeguard their cognitive security to make high confidence accurate decisions in a timely matter particularly given the increasing threats to the cognitive domain.

ACKNOWLEDGMENTS

The views expressed in this publication are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government. PA # USAFA-DF-2026-108

REFERENCES

- [1] M. Havlík and J. Horáček, "War is a mind game: Countering weaponized information," *Cognitive Warfare Perception*, issue 7, pp. 6-8, March 2026.
- [2] H. Le Guyader, "Cognitive domain: A sixth domain of operations," *Cognitive Warfare: The Future of Cognitive Dominance*, NATO Collaboration Support Office, pp. 3, 1-5, April 2022.
- [3] J. M. Blatney and S. Søndergaard, *Cognitive Warfare: NATO Chief Scientist Research Report*, 2025, pp. 4-21.
- [4] R. M. Santini, D. Salles, and G. Tucci, "When machine behavior targets future voters: The use of social bots to test narratives for political campaigns in Brazil," *Int. J. Commun.*, vol. 15, pp. 1220-1243. 2021.
- [5] W. Hersh, and M. McLain, "Inside the gates: Cultivating cognitive security to defend the homeland," *JIPA*, vol.7, pp. 125-147. July-August 2024
- [6] Army Cyber Institute, "Army Cyber Institute Research Lab Overview," October 2024. [Online]. Available: <http://cyber.army.mil/Research/Research-Labs/Cognitive-Security/>
- [7] J. Crum, C. Spencer, E. Doherty, E. Richardson, S. Sherman, A. W. Hays, N. Saxena, R. E. Niemyer, A. P. Anderson, M. Cecko and L. Hirshfield, "Misinformation research needs ecological validity," *Nat. Hum. Behav.*, pp. 1-4. October 2024

- [8] J. Roozenbeek, M. Remshard and Y. Kyrychenko, "Beyond the headlines: On the efficacy and effectiveness of misinformation interventions," vol. 2, pp. 1-17. July 2024
- [9] G. L. Kaempf, G. Klein, M. L. Thordsen, and S. Wolf, "Decision making in complex naval command-and-control environments," *Hum. Factors*, vol. 38, issue 2, pp. 220-231, June 1996.
- [10] A. R. Allred, E. E. Richardson, S. R. Bostrom, J. Crum, C. Spencer, C. Tossell, R. E. Niemeyer, L. Hirshfield and A. Hayman, "Decision-making amid information-based threats in sociotechnical systems: A review," 2025, arXiv:2511.11595. [Online]. Available: <http://arxiv.org/pdf/2511.11595>
- [11] S. R. Bostrom, R. E. Niemeyer, M. Heusler, J. Darlington, A. H. Sandate, G. Bradley, B. Kilgore, R. Powers, M. McLain, A. Fry, A. Dunn, E. Safranek, T. Dunn, Z. Kaufman, K. Duong, D. Cox, S. Siefker, L. Cella, B. Botes, K. R. Proctor, C. Tossell and L. Hirshfield, "techno, social, techno-social: Examining information disorder literature using deductive qualitative analysis and flexible pattern matching," 2025. SocArXiv. [Online]. Available: http://doi.org/10.31235/osf.io/8w2yv_v1
- [12] U. K. H. Ecker, S. Lewandowsky, E. P. Chang and P. Rekha, "The effects of subtle misinformation in news headlines," *J. Exp. Psychol. Appl.*, vol. 20, pp. 323-335. December 2014.
- [13] L. S. Stotzer and F. Zimmermann, "A representative survey experiment of motivated climate change denial," *Nat. Clim. Chang.*, pp. 1-7. February 2024
- [14] F. Jia, "Misinformation literature review: Definitions, taxonomy, and models," *Int. J. Social Sci. Educ. Res.*, vol. 3, pp. 85-90. 2020.
- [15] E. J. Newman, B. Swire-Thompson and U. K. H. Ecker, "Misinformation and the sins of memory: False-belief formation and limits on belief revision," *J. Appl. Res. Mem. Cogn.*, vol. 11, pp. 471-477. December 2022
- [16] G. Pennycook and D. G. Rand, "The psychology of fake news," *Trends Cogn. Sci.*, vol. 25, pp. 388-402. May 2021.
- [17] J. Crum, A. R. Allred, S. R. Bostrom, E. Doherty, M. McLain, E. Richardson, C. Spencer, R. E. Niemeyer, A. P. A. Hayman, C. Tossell, M. Čeko, and L. Hirshfield, "Understanding the neurocognitive mechanisms of cognitive security," *Neurosci. Biobehav. Rev.*, vol. 179, 106448, October 2025.
- [18] G. Murphy, C. de Saint Laurent, M. Reynolds, O. Aftab, K. Hegarty, Y. Sun and C. M. Greene, "What do we study when we study misinformation? A scoping review of experimental research (2016-2022)," *HKS Misinformation Review*, vol. 4, pp. 1-57. November 2023
- [19] I. Bachmann and S. Valenzuela, "Studying the downstream effects of fact-checking on social media: Experiments on correction formats, belief accuracy, and media trust," *Soc. Media Soc.*, vol. 9, issue 2, pp. 1-13, April-June 2023.
- [20] S-H. Kessler and E. Bachmann, "Debunking health myths on the internet: The persuasive effect of (visual) online communication," *J. Public Health*, vol. 30, issue 8, pp. 1823-1835, January 2022.
- [21] R. McPhedran, M. Ratajczak, M. Mawby, E. King, Y. Yang, and N. Gold, "Psychological inoculation protects against the social media infodemic," *Sci. Rep.*, vol. 13, article 5789, April 2023.
- [22] R. Maertens, F. M. Götz, H. F. Golino, J. Roozenbeek, C. R. Schneider, Y. Kyrychenko, J. R. Kerr, S. Stieger, W. P. McClanahan, K. Drabot, J. He, and S. van der Linden, "The misinformation susceptibility test (MIST): A psychometrically validated measure of news veracity discernment," *Behav. Res. Methods*, April 2023.
- [23] A. R. Allred, E. E. Richardson, S. R. Bostrom, J. Crum, C. Spencer, C. Tossell, R. E. Niemeyer, L. Hirshfield, and A. Hayman, "Behavioral outcomes of human cognitive security within an integrative modeling framework," 2026, arXiv:2603.01355. [Online]. Available: <http://arxiv.org/pdf/2603.01355>
- [24] E. K. H. Ecker, S. Lewandowsky, J. Cook, P. Schmid, L. K. Fazio, N. Brashier, P. Kendeou, E. K. Vraga, and M. A. Amazeen, "The psychological drivers of misinformation belief and its resistance to correction," *Nat. Rev. Psychol.*, vol. 1, pp. 13-29, January 2022.
- [25] D. Henshel, M. G. Cains, B. Hoffman, and T. Kelley, "Trust as a human factor in holistic cyber security risk assessment." *Procedia Manuf.*, vol. 3, pp. 1117-1124, 2015.
- [26] C-Y.Huang and Y-C. Liu, "Influence of need for cognition and psychological safety climate on information elaboration and team creativity," *Eur. J. Work Organ. Psychol.*, vol. 31, issue1, pp. 102-116, May 2021.
- [27] G. J. Funke and S. M. Galster, "The effects of cognitive processing load and collaboration technology on team performance in a simulated command and control environment," *Int. J. Ind. Ergon.*, vol. 39, pp. 541-547, December 2008.
- [28] M. M. Luciano, L. A. DeChurch and J. E. Mathieu, "Multiteam systems: A structural framework and meso-theory of system functioning," *J. Manag.*, vol. 44, pp. 1065-1096, March 2018.
- [29] M. A. Marks, J. E. Mathieu, and S. J. Zaccaro, "A temporally based framework and taxonomy of team processes," *Acad. Manage. Rev.*, vol. 26, p. 356. July 2001
- [30] A. Edmondson, "Psychological safety and learning behavior in work teams," *Adm. Sci. Q.*, vol. 44, pp. 350-383. 1999
- [31] S. G. Hart and L. E. Staveland, "Development of NASA-TLX (task load index): Results of empirical and theoretical research. *Adv. Psychol.*, vol. 52, pp. 139-183. 1988
- [32] B. A. Lyons, J. M. Montgomery, A. M. Guess, B. Nyhan, and J. Reifler, "Overconfidence in news judgements is associated with false news susceptibility," *Proc. Natl. Acad. Sci.*, vol. 118, issue 23, article e2019527118, May 2021.
- [33] D. Markowitz, "Self and other-perceived deception detection abilities are highly correlated but unassociated with objective detection ability: Examining the detection consensus effect," *Sci. Rep.*, vol. 14, article 17529, 2024.
- [34] R. Lipshitz, G. Klein, J. Orasanu, and E. Salas, "Taking stock of naturalistic decision making," *J. Behav. Decis. Mak.*, vol. 14, pp. 331-352, December 2001.