ReSCIND Performer HSR Dataset Cover Sheet
General Cyber CogVuln Study (PsyCCDef)

ReSCIND

Dataset Details

Dataset Title:	General Cyber CogVuln Study (PsyCCDef)		
Dataset Citation:	Gonzalez, C., Aggarwal, P., Rajivan, P., Venkatesan, S., Aggarwal, A., José Ferreira, M. ReSCIND-PsyCCDef-Common Data Repository. https://osf.io/834at/files/osfstorage		
Data Format:	csv and xlsx file formats	Data Size:	721.4 KB
Dates & Duration:	August 2024 - September 2024	Time Zone:	Multiple
How to access dataset:	https://osf.io/834at/files/osfstorage		
Point of contact for data questions:	Dr. Sridhar Venkatesan (svenkatesan@peratonlabs.com), Dr. Cleotilde Gonzalez (coty@cmu.edu), Dr. Palvi Aggarwal (paggarwal@utep.edu), Dr. Prashanth Rajivan (prajivan@uw.edu)		

Description of Scenario

Objectives

This experiment was designed to relate established biases to cognitive vulnerabilities (CogVuln) in cyber contexts by evaluating the choices that cyber-aware participants make when presented with bias triggers in cyber scenarios as compared to equivalent established methods.

Experiment Description

This experiment was designed as a survey with 420 participants who had passed a screening test on theoretical knowledge of cyber security. The survey was composed of questions that have been established in the literature to elicit a biased response in non-cyber settings as well as a new questionnaire containing specific cyber scenarios that were designed to elicit a similar biased response in cyber settings. The new cyber-specific questionnaire was referred to as cyber isomorphs of the established questionnaire. The experiment was designed to provide a baseline comparison for identifying biased behavior in the cyber context.

The CogVulns that were considered in this experiment included loss aversion, representativeness bias, availability heuristic, default effect, anchoring bias, recency bias, choice overload, Peltzman effect and sunk cost fallacy. For loss aversion, we considered five variations including mixed gamble setting, certainty effect, endowment effect, aversion to ambiguity and gain/loss framing. For representativeness bias, we considered three variations including base-rate neglect, hot hand

fallacy and denominator neglect. For availability heuristic, we considered recall-based and frequency-based variations and finally, for default effect, we considered position effect and association effect. For each variation, an established method questionnaire and a corresponding cyber isomorph questionnaire were identified for the survey.

Experimental Results

Analysis of the Exp 1 survey data indicated that 81% of the cognitive vulnerabilities tested are ecologically valid in the cyber context. 60% of the triggers tested showed medium to large effect size. It was observed that the loss aversion bias triggers were more effective when there was a high chance of large loss or gain. In general, the effectiveness of the trigger depended on whether expertise was required in the context where it was presented. Several examples are provided in the full dataset. Analysis of the Qualtrics timing data revealed that when participants were biased, they spent more time on the cyber isomorph problem than in the equivalent established method problem. There were mostly non-significant correlations between cognitive vulnerabilities and the self-reported individual characteristics in the pre and post questionnaires.

Cyber Environment

The participants were provided with an online survey in which they were asked to make decisions for a series of cyber tasks under different settings. Settings included a variety of cyber contexts that mirrored the characteristics of decisions used in established cognitive bias studies. To promote realism, the questionnaire also included screenshots from a cyber range in addition to the textual descriptions of the cyber context. These decision tasks centered on activities across the cyber kill chain, and were presented in random order as independent decisions.

DATA

DATA SOURCES

Primary Data Sources

Collected directly from the experiment environment.

Category	Data Source	Examples of Select Data Features
Psychometric Data	Experience Questionnaire	Questions relating to practical and theoretical knowledge of networks and cyber security systems [1]
	Demographics	Age, gender, education level
	Big Five (BFI)	Big Five Indices as defined by [2]
Questionnaires	GRIPS questions	Questions that indicate the individuals risk taking propensity, resistance to sunk cost, resistance to framing effect, and reflectiveness and intuitiveness [3]
Qualtrics	Timing information	Timing of answer submissions throughout the experiment

**Provide a citation for each psychometric assessment in the References section below.*

Derivative Data Sets

Datasets created from aggregating, analyzing, curating, and labeling the source data.

Category	Data Source	Examples of Select Data Features
Self-Reports	Scores for individual participant characteristics	The scores extracted per participant from the GRIPs questions

RESEARCH

Hypotheses

The Experiment 1a dataset was used to answer the following hypotheses for each CogVuln:

[H1] Performer sensors provide similar estimates of CogVuln susceptibility to established sensors.

[H2] Performer triggers activate attacker CogVulns, with a medium or high effect size.

Publications

1. [1] C. Lim, J. Diaz, S. Venkatesan, J. Pfautz, J. Banya, P. Aggarwal, C. Gonzalez, P. Rajivan. *When the Attacker Has a Hot Hand: Cognitive Bias in Cyber Decisions*. In USENIX SOUPS 2025.
2. [2] Aggarwal, A., Ferreira, M. J., Aggarwal, P., Rajivan, P., & Gonzalez, C. *Cognitive Biases in Cyber Attacker Decision-Making: Translating Behavioral Insights into Cybersecurity*. In Active Defense & Deception (AD&D) Workshop 2025.
3. [3] Nazim, M.T.B., Deng, S., Romero, D., Venkatesan, S., Pfautz, J., Rajivan, P., Gonzalez, C., Kiekintveld, C., & Aggarwal, P. *Understanding Cyber Attackers Through Behavioral Science: A Systematic Study of the Representativeness Heuristic*. In Adaptive Cyber Defense (ACD) Workshop, 2025.

References

Include references to psychometric or research-backed methods used to collect data

1. Roccas, Sonia, et al. "The big five personality factors and personal values." Personality and social psychology bulletin 28.6 (2002): 789-801.
2. Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51–61. https://doi.org/10.1016/j.chb.2015.01.039

Note: Additional references will be included as publications are accepted.