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

ReSCIND

Dataset Details

Dataset Title:	Situated 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:	346.2 KB
Dates & Duration:	October 2024 – December 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 study the effects of cognitive vulnerabilities (CogVulns) and bias triggers in the context of cyber activities within a cyber kill chain by evaluating the choices that participants with some cyber experience make in a questionnaire designed to simulate a cyber-attack.

Experiment Description

This experiment was designed as a survey with 111 participants with cyber security background and had passed a screening test on theoretical knowledge of cyber security. Participants played the role of an adversary and were provided with the high-level objective of the simulated attack campaign. They were presented with a series of cyber-specific choice-based tasks to progress through a fictitious network and reach the goal of the attack campaign. 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. Six scenarios with different objectives were created with each scenario containing cyber context(s) covering a subset of the CogVulns. Participants in this experiment were presented with variations of the same cyber kill chain narrative that included a mix of bias trigger scenarios and corresponding control scenarios (with no bias trigger). This experiment was designed such that there

approximately half the participants experienced bias trigger scenario, and half experienced the control condition scenario.

Experimental Results

We observed that effectiveness of triggers depends on the context they are presented and the expertise required. For instance, the same manipulation of denominator neglect generates more biased responses in one situation (Email: 74%) compared to another (Ping outcome: 54%). We observed a variation of the stake effect – which we refer to as the stage effect – wherein participants exhibit greater risk aversion at later stages even when they are faced with similar choices. We also observed a new effect – which we refer to as the goal formulation effect – wherein participant's loss aversion tendencies will vary based on the final goal of the attack campaign even presented with the same choices. In choice overload, we observed that, with more options and information, people are closer to optimality but take longer to make a choice. In anchoring bias, we observed that the participant's familiarity with task impacts the effectiveness of trigger for anchoring effects. For instance, we observed participants showed more tendency to be influenced by anchoring values observed in the crontab file compared to participants who observed anchors in hostnames during port scan. In availability heuristic, we observed that the placement of the CogVuln in a kill chain influenced its effectiveness. In sunk cost fallacy, we observed uncertainty influenced the participant's decision the stay and complete a task.

Cyber Environment

The participants were provided with an online survey in which they were asked to make decisions as they were progressing through a cyber kill chain. The questionnaires included screen captures from a real range to support the narrative and promote realism. For each cyber kill chain, participants were provided with a final goal and based on the decisions taken during their progression, they were led to different attack paths.

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 2 dataset was used to answer the following hypotheses:

[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. 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.
2. 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

1. 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
2. Roccas, Sonia, et al. "The big five personality factors and personal values." Personality and social psychology bulletin 28.6 (2002): 789-801.