ReSCIND Performer HSR Dataset Cover Sheet
In-Person, Lab Cover Sheet – ASCEND Project

ReSCIND

Dataset Details

Dataset Title:	SaikoCTF: In-Person, Lab (I-Lab) Study		
Dataset Citation:	Mather, B., Patterson, J., Raj, A., Vaughan, V., Kelley, C., Klo, J., Lawson, J., McCain, G., Starink, D., Roberts, R., Webber, K., Tinnel, L., & Denker, G. (2025). Adaptive Security through Cognitive Exploitation for Defense (ASCEND), Study SaikoCTF: In-Person Laboratory (I-Lab) [Data set]. SRI, Menlo Park, California, USA. https://doi.org/10.17605/OSF.IO/S3UQ7		
Data Format:	*Raw:* test range, physio, and interview Zip archives; *Clean:* binary, ASCII text, & CSV files	Uncompressed Data Size:	*Raw*: 6.6 GB *Clean (physio only):* 4.0 GB
Dates & Duration:	Four participants between April-May 2025 6 hours per participant	Time Zone:	UTC
How to access dataset:	https://ascend-data.sri.com		
Point of Contact for data questions:	ascend-info@sri.com		

Description of Scenario

Experiment Objectives

The overall objective of this study is to determine how cyber attackers change strategy, behavior, and physiologic response when presented with different cyber-attack countermeasures. ASCEND defines Cognitive Vulnerabilities (CogVulns) as decision-making and cognitive biases plus attacker's culture, cognitive-emotional state, personality traits, and cyber-psychological characteristics.

This study targets Anchoring Bias (AB), Confirmation Bias (CB), Loss Aversion (LA) Bias, Representativeness Bias (RB), and two aspects of Socio-Cultural Bias (SCB), namely Hierarchicalism Bias (SCB-H) and Individualism/Collectivism Bias (SCB-IC).

We conducted in-person lab experiments using targeted challenges in a capture-the-flag (CTF) event to simulate real-world adversarial behavior and hacker club members from the University of West Florida (UWF) and Information Warfare Training Center (IWTC) cyberwarfare technicians at Corry Station as proxies for hackers.

While the CTF challenges are the same as those used in the O-Games, the participants cannot be pooled because the time limits for the in-person ILab experiments for each challenge (most challenges limited to 20 min, one challenge limited to 40 min) differ from those in OGames (each challenge limited to 1 hour). The participants can also not be pooled with In-Person conference SaikoCTF participants, because length of challenges and specific design details were different between in-person conference SaikoCTF events.

Experiment Description

The study begins with consenting, online individual differences measures (IDM) (e.g., demographics, pre-test measure regarding mental state, risk propensity measure, and a CogVuln

measure) and is followed by an online skill-screener provisioned through pwn.college. At the end of the study, participants answer a post-test questionnaire about their mental state.

UWF participants can opt into wearing sensors that detect their brainwaves, heart rate, sweat and respiration while they sit at a table using a laptop to participate in SaikoCTF. Before a participant who opted for physiological sensors starts the CTF cyber-attack challenges, they complete a physio-sensor calibration session to determine their individual baseline values.

IWTC participants are asked to respond to Retrospective Verbal Protocols after each CTF challenge to elicit knowledge, skill, and decision strategies.

Each participant has ten CTF challenges. The CTF challenges are interleaved with nine blocks of IDM and CogVuln Measures.

Participants are pseudo-randomly assigned to be in one of two groups (1 and 2). SaikoCTF uses a within-subjects design. Each challenge has a control (no CogVuln trigger present) and a treatment (CogVuln trigger present) version. There are two CTF challenges (A/B versions) for each CogVuln, thus a total of four challenges per CogVuln (version A control, version A treatment, version B control, version B treatment). The A/B pairs have similar objectives and target the same CogVuln but have enough differences to control for human learning. The order in which control and treatment versions of each CTF challenge is presented is counter-balanced between groups 1 and 2 to control for order of conditions. After each CTF challenge, participants answer additional IDM and CogVuln measures (questionnaires and surveys) to assess their biases, personality traits, cultural values, cognitive-emotional and cyber-psychological attributes. CTF challenges are time limited.

CTF challenges are implemented in the SimSpace Cyber Range Platform (simspace.com/platform). For the three CogVulns tested in this study there are six targeted CTF challenges, each particularly designed to elicit the effectiveness of one CogVuln trigger deployed in the treatment version of the challenge. Furthermore, cyber behavior data is collected to evaluate hypothesized CogVuln sensors in relation to the established methods (IDMs and Bias measures) during analysis.

The **CTF challenges for AB** target the numeric priming facet of AB. Participants are told to find the target server and port on the network. In the A version of the challenge, participants are given access to an administrator workstation with an admin password that ends in “44,” and there is only one port that contains the number 4. In the B version of the challenge, the participant in the treatment groups are given access to an administrator’s workstation that has the number “9” in its password, and there is only one IP address that contains the number 9.

The **CTF challenges for CB** are testing whether susceptible participants who are initially shown evidence of a network vulnerability and script will continuously attempt to exploit that vector even if a simpler and easier path exists out of sight. In the A version of the CB challenge participants are given network access and login credentials to the target machine which has a directory with potential attack scripts to try. The target machine has the root login credentials stored in a hidden location that linpeas can find. Participants must escalate privileges to get the flag that is only readable by root. In the treatment version, the participants are given a linpeas output that indicates dirtycow vulnerability, but linpeas was disrupted halfway through and is incomplete. The goal is to test whether susceptible participants will assume the output of linpeas to be correct and attempt multiple dirtycow exploits, rather than re-running linpeas to confirm the results. In the B version of the CB challenge, participants are given a file that contains the output of an nmap scan showing port 80/http open and port 445/smb open with port 80 being vulnerable to a number of Apache 2.4.49 exploits. The goal is to test whether susceptible participants will continue to scan and attack

the web server using the provided vulnerability scripts rather than re-scanning the box to see that SMB is enabled and allows anonymous login.

The **CTF challenges for LA** target the loss/gain framing effect facet of LA by informing participants that after three failed login attempts, they will be locked out for 30 seconds and their activities will be logged. The goal is to test whether participants susceptible to loss/gain framing effect take less risky actions when faced with temporary suspended access.

The **CTF challenges for RB** target the Sample Size Insensitivity facet of RB by providing logs with proportionally more alerts for a web-server endpoint or service that is not compromised than for an endpoint or service that is compromised. The goal is to test whether participants who see a lot of mentions of a compromised service are more likely to target that service.

The **CTF challenges for SCB-H** presents participants in the treatment version with hierarchical military organization chart providing ranks from General, to Senior Officer, Officer, and Soldier. Participants need to find sensitive information in one of the backup directories of people belonging to the military organization. The goal is to test whether hierarchicalism affects some cultures more than others in that a person with a hierarchical culture is more likely to investigate higher-ranked personnel before they investigate lower-ranked personnel.

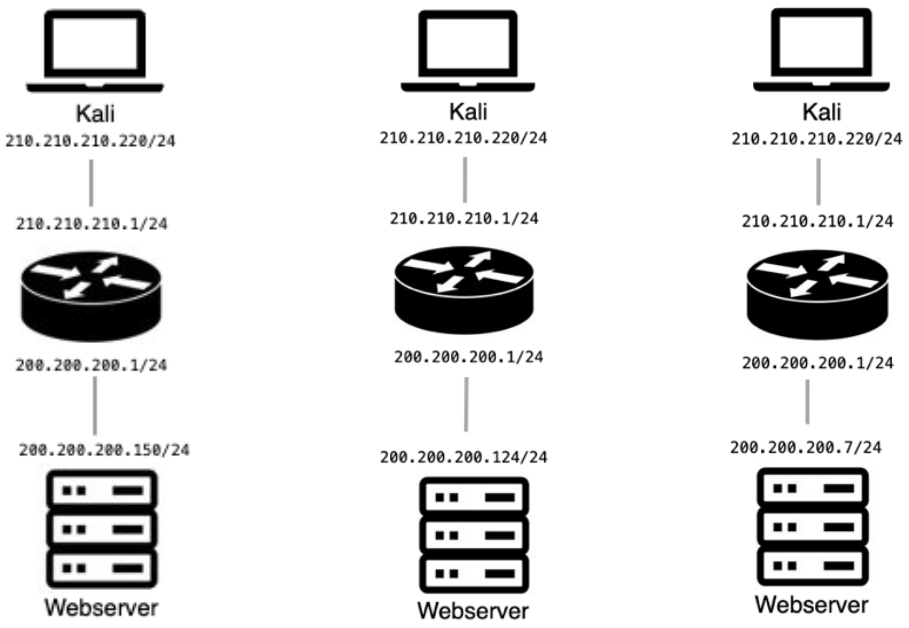
The **CTF challenge for SCB-IC** presents participants in the treatment version with an organization structure that has six locations. Each location has directories for either an individual researcher or for teams of researchers of the sizes 9, 12, or 18 members. The goal is to test whether predisposition toward collectivism or individualism can influence an attacker's approach to exploring files (i.e., choosing team files over individual files or vice a versa).

Experimental Results

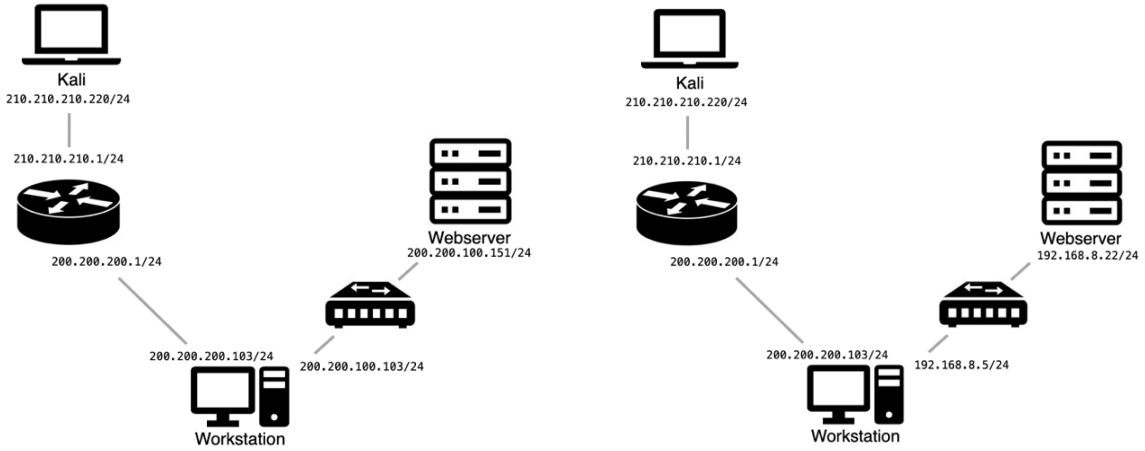
The analysis for this was not conducted as this smaller dataset was deprioritized in favor of the other larger datasets. However, using the data analysis pipeline, other researchers should be able to conduct analysis semi-automatically.

Cyber Environment

The CTF challenges are carefully designed to target a specific CogVuln (or facet thereof) and test a specific CogVuln Trigger. To achieve this, the CTF challenges are tailored, and the cyber range comprises a small set of virtual machines implemented in the SimSpace Cyber Range Platform. The CTF challenge network topology for LA, RB, CB version B and SCB-H challenges is the same and illustrated at left in the picture below. The network topology for CB version A is illustrated in the middle, and the network topology for SCB-IC is on the right



The network topology for AB version A is below on the left and version B below on the right



Data

Primary Data Sources

Collected directly from the experiment environment.

Category	Data Source	Examples of Select Data Features
Physio Data	Wearable sensing DSI-24 headset w/ external heart rate, GSR, & respiration sensor, N-back test results	Electroencephalogram (EEG), electrocardiogram (ECG), galvanic skin response (GSR), and respiration are correlated with a timestamped actions taken during each CTF challenge.

Category	Data Source	Examples of Select Data Features
Survey/ Questionnaires	Demographics	Age, gender, country of origin, and more
	Individual Difference Measures	Big Five (BFI-2) Personality (Soto & John, 2017); Portrait Values Questionnaire (TWIVI-20) (Sandy et al., 2017); Hacker Overclaiming (Paulhus et al., 2013); Cognitive Reflection Test (CRT-3) (Fredrick, 2005); Stress States for Human Performance (DSSQ-3 Pre and Post) (Matthews, 2021); English Proficiency Test (C-Test) (Norris, 2018); General Risk Propensity Scale (GRiPS) (Zhang et al., 2019)
CogVuln Established Measures	RB	Base Rate Neglect (BRN); Sample Size Insensitivity (SSI); Non-random Sequence Fallacy (NRF); Conjunction Bias Fallacy (CBF). (Gertner et al., 2016) for all RB facets
	LA (SC and LFE – also Gov mandated)	Understanding Strategies / Loss Reflection Effect (LRE) (Ruggeri et al., 2020); Loss Framing Effect (LFE) (Bruine de Bruin et al., 2007); Loss Sunk Cost (SC) (Bruine de Bruin et al., 2007);
	SCB	Positive Illusion (PI) Bias & Knowledge Projection Bias (Gertner et al., 2016); Fundamental Attribution Error (FAE) (Gertner et al., 2016); Country of Origin (COO) Bias (Zaromb et al., 2018);
	CB	Evaluation/Weighing of Facts/Evidence (EWE) and Evaluation/Weighing of Questions (EWQ); (Gertner et al., 2016) for all CB facets
	AB	Comparative Judgement Anchor (CJA); Numerical Priming Anchor (NPA); Self-Generated Anchor (SGA); Selective Accessibility Method (SAM) (Gertner et al., 2016) for all AB facets
Cyber User Data	Kali Linux (participant workstation) Instrumentation	
	• Screen capture	Full session video capture of participant desktop
	• Terminal logger (using *script* command)	All terminal commands entered and responses provided by the system. Captures stdin and stdout plus timing data. This data includes all activity conducted in remote ssh sessions.
	• Keylogger	Delta time key press events in all applications (extract rates, commands)
	• Click logger	Mouse clicks
	• Cursor logger	Movements and actions of mouse cursor
	• Clipboard logger	Copies of clipboard contents
	• Menu logger	Command invocations from menu bar
	• Web logger	Browser mouse clicks mapped to tabs, plus keys pressed
	• *Snoopy*	System processes started
Cyber User and Server Data	Target System Syslog	
	• Journal	All system events, including logins
Cyber Server Data [Target Instrumentation (Syslog)]	• auth.log	Successful and failed login attempts via console, terminal, and ssh
	• nginx/access.log • php.log	Web server logs, including pages accessed, data served (including flags)
	• Roundcube.log	Successful and failed email login attempts by account
Cyber Network Data	Kali Linux VM, *tcpdump*: PCAP full packet capture data	Timestamped network communication packets, including payloads. Where possible, unencrypted communications were used to enable extraction of remote logins and information accesses.

Derivative Data Sets

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

Category	Data Source	Examples of Select Data Features
Metadata and Summarization	1. Experiment control data (e.g., event name, de-identified participant IDs P#s, challenge name, treatment vs control group); 2. Raw cyber data extracted from SimSpace range.	Automated scripts uncompress and restructure data into form suitable for analysis, extracts screen video capture for human analysis, summarizes and creates metadata for use by humans and automated analysis tools. Also validates trigger presence/absence in treatment and control groups and flags errors for adjudication such as missing data, no user login into the SimSpace range, timestamp issues. Summarization automatically calculates and reports initial statistics. Example metadata: control treatment status per participant and challenge, CTF performance information (start/end times, flag posted?, flag time, forfeit time, leaderboard time and rank per challenge/event, total flags per event). Example summary data: Usable data sample (e.g., per challenge: Total# C/T, #C, #T), capture rates (all, C, T), mean capture time)
IDM and CogVuln STEN and Z scores	1. IDM and CogVuln measures 2. Experimental control data (e.g., event, P#)	STEN and Z scores per participant for various facets of the five investigated CogVulns as well as for IDMs (e.g., Worry_Pre/Post, Engage_Pre/Post, Distress_Pre/Post, CTest, GRIPS, CogReflect, Openness, Communication, and so on)
CogVuln Sensor Data	1. Cyber data (pcap, nginx, webserver logs, keylogger, terminal logger) 2. Physio data	Produces various CogVuln Sensor candidates of both individual cyber data and combinations of cyber data. Produces discrete measures (e.g., counts) and continues (e.g., rates) for various cyber data (e.g., commands, clicks, keystrokes). Produces also cyber timelines. Compares established methods with CogVuln sensors for SD. Produces metrics of cyber data with significant effect sized between C&T (e.g., Cohen's d, Hedge's g, p-value) Produces other metrics for cyber data thresholds that predict CogVuln (per established methods) with high f1, precision, recall and accuracy. Aligns physiological data with cyber data to detect significant deviations between C & T groups (e.g., p-value, Cohen's d, Hedge's g) to identify cyber data that may be candidates for CogVuln Sensor
CogVuln Trigger Data	1. Cyber data 2. Experimental control data (e.g., event, P#, C/T) 3. CogVuln measures (STEN scores)	Produces per event, participant, challenge, and C/T group, the number of participants that chose biased (fell for CogVuln Trigger) vs unbiased path. Also produces several non-binary CogVulnTrigger metrics such as time on biased vs unbiased path, mean time between login tool invocation, average challenge response time or number of distinct login tools or configurations.
Performance Data	Metadata and summary	Produces general performance measures such as avg_secs_to_flag. Combines demographics with leaderboard data (e.g., COO, region, CTF skill, age, gender, language skill, leaderboard rank)
Physiological Data	Physio data	Extracts features such as heart rate and variability, tonic and phasic GSR measurements, respiration rate and amplitude, stress, engagement, and workload.

Research

Hypotheses

The SaikoCTF ECSC dataset was used to answer the following hypotheses:

[H1] RB: The hypothesis of the bias trigger is that a hacker who sees a lot of mentions of a service without any other supporting evidence is more likely to target that service.

[H2] LA: Participants who are susceptible to loss/gain framing effect will take less risky actions when faced with temporarily suspended access due to password attempt failures and will attempt an alternative approach that has no such consequences.

[H3] CB: The hypothesis of the bias trigger is that a hacker who is initially shown evidence of a privilege escalation path will continuously attempt to exploit that vector even if a simpler and easier path exists just out of sight.

[H4] AB: Participants who are susceptible and who are initially shown and engage with a number will be more likely to unconsciously select something containing that number when faced with multiple choices.

[H5] SCB-H: Participants with influence from a hierarchical culture will be influenced as they are more likely to investigate higher-ranked personnel before investigating lower-ranked personnel.

[H6] SCB-IC: Participants predisposed toward collectivism or individualism will be influenced in their approach to exploring files (either the order or the number of individual/team files).

[H7] All challenges and CogVulns: Physio data and cognitive-emotional states derived from physio data correlate with CogVuln trigger effectiveness or supports identification of cyber surrogate data/measures for CogVuln Sensors.

Publications

See http://ascend-data.sri.com/docs/publications.

Attachments

See http://ascend-data.sri.com/docs/scorecards for IDM and CogVuln Established Measures Score Cards.

See https://ascend-data.sri.com/experiment-ilab-2025/ for blank surveys and challenge descriptions (note: OGames challenges and surveys were used for ILab).

References

1. Bruine de Bruin, W., Parker, A. M., & Fischhoff, B. (2007). Individual differences in adult decision-making competence. *Journal of Personality and Social Psychology, 92*(5), 938-956.
2. Frederick, S. (2005). Cognitive reflection and decision making. *Journal of Economic perspectives*, *19*(4), 25-42.
3. Gertner, A., Zaromb, F., Schneider, R., Roberts, R. D., & Matthews, G. (2016). *The Assessment of Biases in Cognition*. MITRE Technical Report. McLean, Virginia: The MITRE Corporation.
4. Matthews, G. (2021). Stress states, personality and cognitive functioning: A review of research with the Dundee Stress State Questionnaire. *Personality and Individual Differences, 169,* 110083.
5. Menon, T., Morris, M. W., Chiu, C. Y., & Hong, Y. Y. (1999). Culture and the construal of agency: Attribution to individual versus group dispositions. *Journal of Personality and Social Psychology*, *76*(5), 701.
6. Norris, J. M. (2018). *Developing C-tests for Estimating Proficiency in Foreign Language Research*. New York, NY: Peter Lang.

7. Paulhus, D. L., Harms, P. D., Bruce, M. N., & Lysy, D. C. (2003). The over-claiming technique: Measuring self-enhancement independent of ability. *Journal of Personality and Social Psychology, 84*, 890–904. https://doi.org/10.1037/0022-3514.84.4.890.
8. Ruggeri, K., Alí, S., Berge, M. L., Bertoldo, G., Bjørndal, L. D., Cortijos-Bernabeu, A., ... & Folke, T. (2020). Replicating patterns of prospect theory for decision under risk. *Nature human behaviour*, *4*(6), 622-633.
9. Sandy, C. J., Gosling, S. D., Schwartz, S. H., & Koelkebeck, T. (2016). The development and validation of brief and ultrabrief measures of values. *Journal of Personality Assessment*, DOI: 10.1080/00223891.2016.1231115.
10. Soto, C. J., & John, O. P. (2017). The next Big Five Inventory (BFI-2): Developing and assessing a hierarchical model with 15 facets to enhance bandwidth, fidelity, and predictive power. *Journal of Personality and Social Psychology, 113*, 117–143.
11. Zaromb, F. M., Liu, J. H., Páez, D., Hanke, K., Putnam, A. L., & Roediger, H. L. (2018). We Made History: Citizens of 35 Countries Overestimate Their Nation's Role in World History. *Journal of Applied Research in Memory and Cognition, 7*, 521-528.
12. Zhang, D. C., Highhouse, S., & Nye, C. D. (2019). Development and validation of the General Risk Propensity Scale (GRiPS). *Journal of Behavioral Decision Making*, 1–16. https://doi.org/10.1002/bdm.2102.