Vision: Profiling Human Attackers: Personality and Behavioral Patterns in Deceptive Multi-Stage CTF Challenges

Khalid Alasiri
School of Computing and Augmented Intelligence
Arizona State University
Tempe, Arizona, USA
kalasir1@asu.edu

Rakibul Hasan
School of Computing and Augmented Intelligence
Arizona State University
Tempe, Arizona, USA
Rakibul.Hasan@asu.edu

***Abstract*—Understanding how psychological traits shape attack strategies of cyber attackers is critical for developing proactive defenses. This paper presents an early-stage study using a controlled, multi-stage Capture-the-Flag (CTF) environment designed to elicit behavioral expressions of persistence, resilience, risk-taking, and openness to experience. Participants complete validated personality inventories before engaging in a cyberattack task within a simulated but realistic environment that mimics a corporate network. That environment contains both real and deceptive vulnerabilities that attackers can exploit to escalate their privilege and access resources in the system. During that time, system logs, continuously taken screenshots, and think-aloud data will capture their actions and strategies. From that data, behavioral indicators, such as retries, strategic pivots, early high-risk actions, and exploration breadth, will be extracted and used to predict traits. The larger goal is to automatically guess attackers' future actions, and proactively deploy defense mechanisms in run time. As a vision-track contribution, this work establishes a methodological foundation for profiling attackers through behavioral telemetry, supporting the future development of human-aware, proactive cyber defense strategies.**

I. Introduction

Cybersecurity research has traditionally been reactive, primarily focusing on patching vulnerabilities and investigating incidents after they have occurred. Recently, however, researchers have increasingly focused on proactive defense strategies to anticipate and mitigate threats before they materialize [1], [2]. To be effective, a proactive defense mechanism must be able to predict attackers' next steps and prepare for it at runtime [3]–[5]. However, progress in determining ways to accurately predict attackers' behaviors has been slow.

Personality traits have been established as reliable predictors of human behaviors, particularly in decision-making under uncertainty [6], [7]. Traits such as persistence, resilience, and risk tolerance play a substantial role in how adversaries interpret signals, respond to failure, and persist through obstacles [8], [9]. In adversarial settings, these traits shape how attackers interpret signals, persist through obstacles, and adapt their strategies over time [5]–[9]. Despite growing evidence that individual differences matter, most cybersecurity defenses continue to model attackers as uniform or purely rational agents [3], [10].

Our vision for this work is to enable *human-aware cyber defense*: adaptive systems that account for attacker traits rather than assuming homogeneous adversaries. By grounding our study design in usable-security methodology—think-aloud protocols, mixed-method behavioral logging, and validated psychometric instruments—we contribute a human-centered perspective to a domain traditionally driven by technical analysis. Understanding how real humans behave under uncertainty, frustration, risk, and misleading cues is essential for designing security mechanisms that interact with—rather than work against—human tendencies.

Deception plays an important role in this vision, not only as a defensive mechanism, but also as a methodological tool for studying attacker behavior. In this work, we use the term *deceptive techniques* to refer to deliberately engineered signals, services, or vulnerabilities (e.g., honeypots, decoy accounts, or non-exploitable "trap" paths) that are designed to shape attacker decisions and elicit observable behavioral responses. While prior work has explored deception primarily as a means to delay or disrupt attacks [11], its potential for revealing how personality traits manifest in attacker decision-making remains underexplored. This gap limits the development of adaptive defenses that can respond dynamically to human adversaries [10].

This work presents the first stage of a larger research effort toward Trait-Oriented Deception Determination and Execution (TODDE), a framework for personalizing defensive strategies based on attacker traits. TODDE will enable us to conduct experiments in a controlled but realistic environment involving cyber professionals and answer foundational questions: **(1)** *How can we reliably learn attacker's personality traits and behavioral dispositions by observing their actions*? **(2)** *How*

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23069
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

can we predict future actions based on the learned traits? and **(3)** *How can we dynamically devise deceptive techniques to thwart those actions*?

To investigate these questions, we developed a controlled, human-subject experiment using a multi-stage Capture-the-Flag (CTF) environment enriched with realistic and deceptive tasks. Unlike traditional CTFs that focus exclusively on technical challenge difficulty, our environment is intentionally designed to elicit behavioral signals relevant to traits such as persistence and risk-taking. We combine these behavioral traces with validated psychological measurements—including General Risk Propensity Scale (GRiPS), Big Five Inventory–2 Short Form (BFI-2-S), and resilience/persistence scales—to examine how individual differences shape security-relevant decisions. In this paper, we describe the framework, and methodology to answer the first research question (i.e., learning traits from attacker behaviors).

II. Related Work

Attacker profiling has been informed by personality and motivation research. Canudo et al. [6] applied self-control theory and personality models, including the Big Five and Dark Triad traits (Machiavellianism, narcissism, and psychopathy), to differentiate hacker types. They found that black hats exhibit lower self-control and higher openness, along with stronger sensation-seeking motivations, while white hats tend toward prosocial motivations. Grey hats displayed a blend of these traits, suggesting fluid identities. Relatedly, Hani et al. [7] employed machine learning to classify hackers based on Big Five traits, achieving high predictive accuracy and revealing intra-group distinctions. Gaia et al. [5] examined how Dark Triad traits, opposition to authority, and thrill-seeking drive hacking propensities, offering a multifaceted view of hacker motivations.

Resilience and persistence have been recognized as important traits in cybersecurity contexts. Joinson et al. [8] introduced the Human Cyber-Resilience Scale, measuring an individual's capacity to resist, recover from, and learn following cyber incidents. The PERC (Persistence, Effort, Resilience, and Challenge-Seeking) task developed by Porter et al. [9] provides a performance-based, language-independent method to quantify persistence, effort, resilience, and challenge-seeking. These constructs are particularly relevant to CTF scenarios where attackers may need to reattempt failed paths, adapt to deceptive obstacles, and sustain engagement over multiple stages.

In parallel, researchers have explored structured behavioral datasets to study adversarial operations. Tovarnák et al. [12] released a comprehensive dataset from a two-day cyber defense exercise on the KYPO Cyber Range Platform, including synchronized network flows and system logs from enterprise-like environments. Such datasets enable fine-grained analysis of attacker behaviors, though they often lack the integrated psychological dimensions that the present study incorporates.

Other work has focused on integrating psychological profiling with operational cybersecurity scenarios. Padilla et al. [10] proposed a platform-agnostic experimental methodology to capture real-time human decisions and actions during cybersecurity exercises, bridging the gap between abstract trait profiling and observed attacker behavior. Tshimula et al. [13] explored psycholinguistic analysis with large language models to derive attacker psychological profiles from textual outputs, complementing behavioral profiling with linguistic signals.

Deceptive techniques have been a core strategy in cybersecurity for decades, used to mislead adversaries, delay attacks, and gather intelligence. Early foundational work such as Spitzner's *Honeypots: Tracking Hackers* [1] established the role of honeypots as a means to attract and observe malicious actors in controlled environments. Rowe and Rrushi's *Introduction to Cyberdeception* [2] further expanded this field by formalizing concepts, taxonomies, and implementation strategies for deception in cyber operations, framing it as an interdisciplinary domain involving technical, cognitive, and strategic considerations.

Building on these foundations, Cranford et al. [3] developed a cognitive theory of cyber deception within the ACT-R (Adaptive Control of Thought–Rational) cognitive architecture, using instance-based learning to model attacker decision-making under deceptive signaling. Their behavioral experiments with the Insider Attack Game demonstrated that deception can influence attacker choices by exploiting biases such as confirmation bias, underscoring the importance of considering bounded rationality in cyber defense. This cognitive modeling perspective is directly relevant to environments like multi-stage CTFs, where deception can be systematically embedded to elicit measurable behavioral patterns.

Ferguson-Walter et al. [11] advanced empirical research on deception with the Tularosa Study, a large-scale controlled experiment involving over 130 professional red teamers. By integrating technical deception methods with psychological profiling, cognitive testing, and telemetry collection, they quantified how deception affects attacker strategies, persistence, and decision-making. The combination of behavioral and psychological measures in that work provides a methodological precedent for profiling attackers in CTF environments enriched with deceptive cues.

In summary, prior work has laid foundations in cyber deception, personality-based attacker profiling, and cyber-range data collection; our contribution is to integrate these strands in a trait-informed CTF environment.

III. Methodology

A. Overview

This experiment investigates how individual psychological traits shape attacker behaviors during a controlled multi-stage Capture-the-Flag (CTF) style privilege-escalation challenge. We collect pre-challenge personality measures and detailed behavioral traces (command logs, task choices, and timing information) as participants interact with a mixture of genuine and deceptive attack paths. The overarching goal is to examine whether specific, observable behaviors, such as repeated retries, strategic pivots after failure, or early engagement with

high-risk opportunities—can serve as reliable indicators of underlying personality traits relevant to cyber offense.

B. Selecting Personality Traits

In total, we measure eight personality traits: the five Big Five dimensions (Extraversion, Agreeableness, Conscientiousness, Negative Emotionality, and Openness to Experience) using the BFI-2-S [19], together with domain-general risk propensity (GRiPS) [18], persistence [15], and resilience [17]. The big five traits have been linked to decision-making in cyber security and other contexts by numerous studies [20]–[22]; they also correlate to characteristics that are relevant to cyber attacks: fluid intelligence, problem-solving ability, and susceptibility to deception [23]–[26]. Likewise, persistence and resilience are essential qualities to succeed in cyber-attacks [11], [27]. Finally, we include risk propensity that determine engagement in risky behaviors, cyber attack being a prominent one, and can facilitate developing deception-based defense mechanisms. Due to space limitations, here, we present experimental design focusing on the following four traits: *Persistence*, *Resilience*, *Risk-taking*, and *Openness to Experience*. Our choice of focal traits and their behavioral manifestations in the environment is informed by prior work that connects personality dimensions to hacking propensity and hacker types [5]–[7].

Table I summarises how each focal trait is measured and how we expect it to manifest in the experimental setup in terms of log-based behavioral indicators. These expectations directly inform our hypotheses in Section III-D and the analysis plan in Section III-E

C. Experimental Infrastructure

TODDE has been implemented as an isolated research environment that supports repeatable, fine-grained behavioral logging. It provides a web-based IDE with an interactive terminal for connecting into a dedicated Linux container preloaded with common security tools. Each container is ephemeral and network-isolated from real systems. All shell commands, file accesses, and relevant system events are collected via a logging stack and stored with timestamps for later analysis. Screen and audio recordings from the remote session are captured in parallel to provide context for interpreting behavioral traces (e.g., verbal reasoning, visible search activity). This infrastructure allows us to align psychometric measures, in-game actions, and think-aloud protocols on a shared timeline.

D. Challenge Tasks

1) Environment Overview: Our experimental setup simulates an internal corporate environment with multiple user accounts at different privilege levels (e.g., entry-level employee, IT staff, financial manager, system administrator), realistic business assets (e.g., reports, credentials, configuration files), and several potential escalation paths. Participants start from a low-privilege account and are instructed to "break out of the box" by discovering assets, escalating privileges, and collecting as many flags as possible. Each flag contributes to a cumulative score, while certain actions are treated as being "seen" by a monitoring system (e.g., triggering a logging alert), which results in point penalties or lost bonus opportunities. This scoring and monitoring scheme is intended to partially simulate the feeling of risk and potential loss that attackers face in real environments, while still keeping the scenario safe and self-contained for research. Compared to typical CTF challenges, the environment resembles an internal assessment setting with realistic misconfigurations and overlapping avenues for attack rather than a series of isolated puzzles.

Within this environment we embed both genuine escalation opportunities and carefully designed decoy tasks intended to elicit differences in persistence, resilience, risk-taking, and openness to experience.

2) Design Principles: To meet the above stated goals, the environment was constructed around three principles:

- **Realism.** Tasks are framed as plausible corporate misconfigurations (e.g., backup archives, internal web apps, scheduled jobs) rather than abstract puzzles, to encourage naturalistic strategies.
- **Multiple viable options.** At any point, participants can choose among several potential avenues (password cracking, web exploitation, privilege escalation, etc.), enabling us to observe differences in task selection, switching, and abandonment.
- **Embedded deception.** Some ostensibly promising vectors are intentionally difficult or impossible to complete within the allotted time. These "trap" tasks are designed as behavioral probes for our focal traits (e.g., persistence in the face of repeated failure, willingness to pursue high-risk opportunities, or openness to exploring alternative explanations).

The following task descriptions therefore emphasize the behavioral probes and hypothesized indicators rather than technical exploit details.

3) Task-Level behavioral Probes: As stated above, our experimental setup allows multiple paths for the participants to explore. Each of them have various 'Tasks' they need to complete, each task presents participants with a plausible privilege-escalation opportunity accompanied by cues (e.g., through names of the file) that are realistic in the context of penetration testing of a corporate network. The underlying technical configuration is tuned so that the tasks differ in difficulty and in how rewarding or deceptive they are, allowing us to observe how participants react to progress, failure, and uncertainty. The instructions set we have prepared for participants explicitly mentions the risk-reward tradeoffs: successfully accessing potentially higher valued assets (such as credential files or higher privileged user accounts) will provide higher rewards (more points), but those assets are more likely to be monitored for unauthorized accesses, increasing the chance of getting caught.

Below, we summarise the main tasks in terms of their narrative framing and the behaviors they are intended to elicit. For each task, we define a small set of log-based indicators (e.g.,

TABLE I
FOCAL PERSONALITY TRAITS, MEASUREMENT TOOLS, AND EXPECTED BEHAVIORAL INDICATORS IN THE EXPERIMENTAL SETUP.

Trait	Definition	Measurement	Expected behavioral Indicators
Persistence	Sustained effort toward goals despite difficulties [14], [15]	Motivational Persistence Scale (MPS-16) [15]	High counts of repeated attempts on the same task or exploit path; longer time spent before abandoning a deceptive task.
Resilience	Capacity to adapt positively and recover from setbacks [16], [17]	Brief Resilience Scale [17]	Switching to alternative strategies shortly after failures; higher ratio of "fail → new strategy" vs. "fail → stop" behaviors.
Risk-Taking	Willingness to engage in uncertain or high-stakes actions [18]	General Risk Propensity Scale (GRiPS) [18]	Earlier and more frequent initiation of risky actions (e.g., privilege escalation attempts, aggressive scans, or use of high-value accounts).
Openness to Experience	Curiosity and receptiveness to novel ideas and approaches [19]	Big Five Inventory–2 Short Form (BFI-2-S) (Openness domain) [19]	Exploration of diverse tools and paths; greater variety of services, users, and files touched before committing to a single exploit strategy.

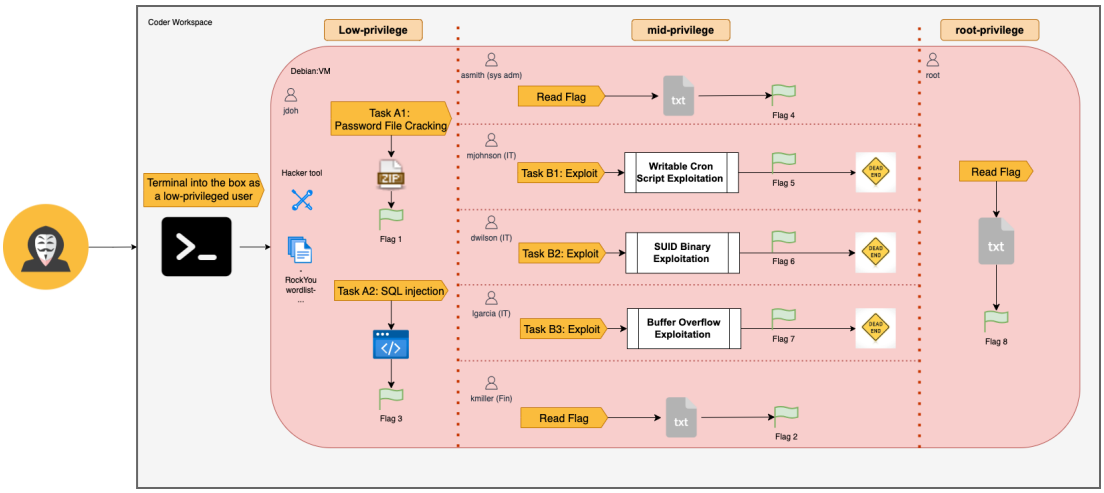

Fig. 1. The network structure, assets, and (real and fake) vulnerabilities in the system that attackers can exploit. Dead-end icons mark decoy exploit paths that reveal a flag but do not provide additional privileges or access to new assets.

number of retries, switches to alternative strategies, or timing of high-risk actions) that form the basis of our hypotheses about persistence, resilience, risk-taking, and openness.

a) Task A1: Password Cracking.: Participants discover an encrypted archive labeled as a corporate credentials backup in a low-privilege user's home directory. Supporting artefacts (onboarding notes, internal documentation) suggest that it may contain valuable information, and that standard password-cracking tools could be used to access it. In reality, the archive is protected by a long, cryptographically random password that does not appear in any provided or common wordlists, making practical cracking within the session time infeasible and turning it into a deceptive "time sink".

Trait measures. Risk-taking (willingness to invest in a high-reward but uncertain path) and Persistence (time and number of retries spent on an ultimately uncrackable archive).

b) Task A2: SQL Injection and Database Exploration (Risk-Taking and Persistence).: A web application exposed within the environment contains a login form that can be bypassed using SQL injection, granting access to an internal employee database. Once inside, participants can enumerate accounts, extract password hashes, and choose which user accounts to target.

Trait measures. Risk-taking (pursuing high-value but risky accounts, attempting risky actions such as modifying records), Persistence (iterative refinement of payloads and cracking strategies).

c) Task B1: An (apparently) exploitable Cron Script (Persistence vs. Exploratory Resilience).: Participants will find a root-owned scheduled backup script that appears to be a classic privilege-escalation vector: the script is writable and executed periodically by a privileged user. However, we have another process, hidden from the attacker, that monitors any edit to the script and automatically restores it to its original state, thus, preventing the expected escalation but leaving a trace in the logs.

Trait measures. Persistence and Resilience(repeated overwriting of the script despite the lack of success), Openness to experience / exploratory behavior (stepping back to investigate the hidden mechanism, e.g., inspecting running processes or related files; knowing when to abandon the path).

d) Task B2: SUID Binary Honeypot.: A SUID binary named *vim.basic*, which is owned by a high-privileged user, presents a potential opportunity for privilege escalation. Its

name and basic functionality, which can be explored by executing and interacting with it, suggest that it might be exploitable. However, any attempts to misuse the binary are detected through input validation and checks for injection attempts. Instead of allowing actual privilege escalation, these attempts are logged.

Trait measures. Risk-taking: risk-seeking participants execute the binary quickly and experiment with potentially dangerous arguments, whereas others spend more time on reconnaissance (e.g., inspecting permissions or documentation) before executing it, or defer it until later.

e) Task B3: An Apparent Buffer Overflow Vulnerability.: Participants encounter a privileged program that behaves like a simple note-editing tool (e.g., opening and appending text), and basic inspection reveals cues such as references to *strcpy()* that typically indicate unsafe memory handling. These signals make the binary appear vulnerable to a classic buffer overflow. However, the program includes a hidden length check that terminates execution before any unsafe function is reached, meaning the apparent vulnerability cannot actually be exploited despite the convincing surface indicators.

Trait measures. This task probes how participants respond when a textbook exploit path fails, contrasting high persistence (sustained debugging and multiple exploit attempts) with openness to experience (willingness to reconsider assumptions, check compilation flags, and pivot to alternative explanations or attack vectors).

E. Data Sources and Planned Analysis

Each session yields three data streams: (1) system logs with time-stamped shell commands, file accesses, and relevant system events; (2) self-report measures from the pre-challenge personality inventories (MPS-16, BRS, GRiPS, BFI-2-S) and a brief post-challenge survey on strategies, reactions to deception, and persistence / pivot decisions; and (3) think-aloud screen-and-audio recordings that provide qualitative context for interpreting log-derived behaviors.

From the logs we derive behavioral metrics aligned with our focal traits, such as number and duration of retries on deceptive tasks (persistence), frequency of "fail $\rightarrow$ new strategy" transitions (resilience), time to first high-risk action (risk-taking), and diversity of tools and paths explored (openness). These metrics are synchronised with personality scores and post-challenge responses to examine correlations between traits and behaviors, complemented by exploratory mixed-methods inspection of notable outlier cases using the think-aloud data.

F. Experimental Procedure

We are currently collecting pilot data to test if the experimental environment works as expected and the logs are complete and properly formatted. For the pilot, we plan to invite 8–10 participants who are actively involved in CTF games. Each session will be conducted remotely; before connecting to the environment, participants will complete the pre-survey containing the personality measures described above. During the session, participants will be encouraged to *think aloud* and verbalize their reasoning. Afterwards, they will complete a brief post-challenge survey about their strategies, reactions to deception, and decision-making.

G. Ethical Considerations

The study protocol was approved by our institution's IRB, and all procedures comply with ethical guidelines for human-subject research. Participants provide informed consent before beginning the study and are explicitly told that the environment may contain deceptive elements similar to those used in real-world penetration testing (e.g., honeypots and decoy services). During the session they interact only with isolated research infrastructure, and no real organizations or third-party systems are affected. After the session, participants are debriefed about the specific deceptive mechanisms used and the goals of the study, and they are given the opportunity to withdraw their data. All collected data are stored securely, pseudonymized before analysis, and used only for research purposes.

IV. Conclusion

This work presents the first stage of an ongoing effort to link psychological traits with attacker behavior in realistic cyber-attack scenarios. We introduced a multi-stage CTF environment that embeds genuine and deceptive escalation paths, together with a measurement framework that combines validated personality inventories, fine-grained behavioral logging, and think-aloud protocols. From this design, we derived concrete hypotheses connecting persistence, resilience, risk-taking, and openness to specific log-based indicators such as retries, strategic pivots, risk onset, and exploration breadth.

The next step of this effort is to collect data and validate those hypotheses, and study mechanisms to dynamically generate proactive defense strategies. Besides advancing state of the art in proactive cyber defense, this project will make a realistic dataset and a reusable framework accompanied by and validated methodology available to the community.

Acknowledgment

This research was supported by the Air Force Office of Scientific Research (AFOSR) under Award FA9550-24-1-0227. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the Air Force Office of Scientific Research (AFOSR).

REFERENCES

[1] L. Spitzner, *Honeypots: tracking hackers*. Boston: Addison-Wesley, 2003.

[2] N. C. Rowe and J. Rrushi, *Introduction to Cyberdeception*. Cham: Springer International Publishing, 2016. [Online]. Available: http://link.springer.com/10.1007/978-3-319-41187-3

[3] E. A. Cranford, C. Gonzalez, P. Aggarwal, M. Tambe, S. Cooney, and C. Lebiere, "Towards a Cognitive Theory of Cyber Deception," *Cognitive Science*, vol. 45, no. 7, p. e13013, Jul. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1111/cogs.13013

[4] M. Taneem Bin Nazim, S. Deng, D. Romero, S. Venkatesan, J. Pfautz, P. Rajivan, C. Gonzalez, C. Kiekintveld, and P. Aggarwal, "Understanding Cyber Attackers Through Behavioral Science: A Systematic Study of the Representativeness Heuristic," in *2025 IEEE Conference on Artificial Intelligence (CAI)*. Santa Clara, CA, USA: IEEE, May 2025, pp. 1142–1149. [Online]. Available: https://ieeexplore.ieee.org/document/11050558/

[5] J. Gaia, B. Ramamurthy, G. Sanders, S. Sanders, S. Upadhyaya, X. Wang, and C. Yoo, "Psychological Profiling of Hacking Potential," in *Proceedings of the Annual Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences, 2020, iSSN: 2572-6862. [Online]. Available: https://hdl.handle.net/10125/64014

[6] M. Canudo, S. Moreira, R. Solymosi, and I. Guedes, "Differentiating Hackers and Hacker Types: The Role of Self-Control, Personality, and Motivations," 2025. [Online]. Available: https://www.ssrn.com/abstract=5217224

[7] U. Hani, O. Sohaib, K. Khan, A. Aleidi, and N. Islam, "Psychological profiling of hackers via machine learning toward sustainable cybersecurity," *Frontiers in Computer Science*, vol. 6, Apr. 2024, publisher: Frontiers Media SA. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fcomp.2024.1381351/full

[8] A. N. Joinson, M. Dixon, L. Coventry, and P. Briggs, "Development of a new 'human cyber-resilience scale'," *Journal of Cybersecurity*, vol. 9, no. 1, p. tyad007, Jan. 2023. [Online]. Available: https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyad007/7130095

[9] T. Porter, D. Catalán Molina, L. Blackwell, S. Roberts, A. Quirk, A. Lee Duckworth, and K. Trzesniewski, "Measuring Mastery Behaviors at Scale: The Persistence, Effort, Resilience and Challenge-Seeking Task (PERC)," *Journal of Learning Analytics*, vol. 7, no. 1, Mar. 2020, publisher: Society for Learning Analytics Research. [Online]. Available: https://learning-analytics.info/index.php/JLA/article/view/6759

[10] "Cybersecurity Methodology for Specialized Behavior Analysis," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Cham: Springer International Publishing, 2021, pp. 237–243, iSSN: 1867-8211, 1867-822X. [Online]. Available: https://link.springer.com/10.1007/978-3-030-68734-2_14

[11] K. Ferguson-Walter, T. Shade, A. Rogers, E. Niedbala, M. Trumbo, K. Nauer, K. Divis, A. Jones, A. Combs, and R. Abbott, "The Tularosa Study: An Experimental Design and Implementation to Quantify the Effectiveness of Cyber Deception," in *Proceedings of the Annual Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences, 2019, iSSN: 2572-6862. [Online]. Available: http://hdl.handle.net/10125/60164

[12] D. Tovarňák, S. Špaček, and J. Vykopal, "Traffic and log data captured during a cyber defense exercise," *Data in Brief*, vol. 31, p. 105784, Aug. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2352340920306788

[13] J. M. Tshimula, D. K. Nkashama, J. T. Muabila, R. M. Galekwa, H. Kanda, M. V. Dialufuma, M. M. Didier, K. Kalala, S. Mundele, P. K. Lenye, T. W. Basele, A. Ilunga, C. N. Mayemba, N. M. Kasoro, S. K. Kasereka, H. Mikese, P.-M. Tardif, M. Frappier, F. Kabanza, B. Chikhaoui, S. Wang, A. M. Sumbu, X. Ndona, and R. K.-K. Intudi, "Psychological Profiling in Cybersecurity: A Look at LLMs and Psycholinguistic Features," 2024, version Number: 3. [Online]. Available: https://arxiv.org/abs/2406.18783

[14] A. L. Duckworth, C. Peterson, M. D. Matthews, and D. R. Kelly, "Grit: Perseverance and passion for long-term goals." *Journal of Personality and Social Psychology*, vol. 92, no. 6, pp. 1087–1101, 2007. [Online]. Available: https://doi.apa.org/doi/10.1037/0022-3514.92.6.1087

[15] T. Constantin, A. Holman, and M. Hojbotă, "Development and validation of a motivational persistence scale," *Psihologija*, vol. 45, no. 2, pp. 99–120, 2012, publisher: National Library of Serbia. [Online]. Available: https://doiserbia.nb.rs/Article.aspx?ID=0048-57051202099C

[16] S. S. Luthar, D. Cicchetti, and B. Becker, "The Construct of Resilience: A Critical Evaluation and Guidelines for Future Work," *Child Development*, vol. 71, no. 3, pp. 543–562, May 2000. [Online]. Available: https://srcd.onlinelibrary.wiley.com/doi/10.1111/1467-8624.00164

[17] B. W. Smith, J. Dalen, K. Wiggins, E. Tooley, P. Christopher, and J. Bernard, "The brief resilience scale: Assessing the ability to bounce back," *International Journal of Behavioral Medicine*, vol. 15, no. 3, pp. 194–200, Sep. 2008, publisher: Springer Science and Business Media LLC. [Online]. Available: http://link.springer.com/10.1080/10705500802222972

[18] D. C. Zhang, S. Highhouse, and C. D. Nye, "Development and validation of the General Risk Propensity Scale (GRiPS)," *Journal of Behavioral Decision Making*, vol. 32, no. 2, pp. 152–167, Apr. 2019, publisher: Wiley. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/bdm.2102

[19] C. J. Soto and O. P. John, "Short and extra-short forms of the Big Five Inventory–2: The BFI-2-S and BFI-2-XS," *Journal of Research in Personality*, vol. 68, pp. 69–81, Jun. 2017, publisher: Elsevier BV. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0092656616301325

[20] H. K. Jach and L. D. Smillie, "To fear or fly to the unknown: Tolerance for ambiguity and Big Five personality traits," *Journal of Research in Personality*, vol. 79, pp. 67–78, Apr. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0092656619300236

[21] K. A. Byrne, C. D. Silasi-Mansat, and D. A. Worthy, "Who chokes under pressure? The Big Five personality traits and decision-making under pressure," *Personality and Individual Differences*, vol. 74, pp. 22–28, Feb. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0191886914005595

[22] M. Babaei, M. Mohammadian, M. Abdollahi, and A. Hatami, "Relationship between big five personality factors, problem solving and medical errors," *Heliyon*, vol. 4, no. 9, p. e00789, Sep. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405844018337381

[23] J. Anglim, P. D. Dunlop, S. Wee, S. Horwood, J. K. Wood, and A. Marty, "Personality and intelligence: A meta-analysis," *Psychological Bulletin*, vol. 148, no. 5-6, pp. 301–336, 2022, place: US Publisher: American Psychological Association.

[24] T. Chamorro-Premuzic, J. Moutafi, and A. Furnham, "The relationship between personality traits, subjectively-assessed and fluid intelligence," *Personality and Individual Differences*, vol. 38, no. 7, pp. 1517–1528, May 2005. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0191886904002910

[25] T. Halevi, N. Memon, and O. Nov, "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks," Jan. 2015. [Online]. Available: https://papers.ssrn.com/abstract=2544742

[26] J.-H. Cho, H. Cam, and A. Oltramari, "Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis," in *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, Mar. 2016, pp. 7–13, iSSN: 2379-1675 Citation Key:. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7497779

[27] O. Hjemdal, O. Friborg, S. Braun, C. Kempenaers, P. Linkowski, and P. Fossion, "The Resilience Scale for Adults: Construct Validity and Measurement in a Belgian Sample," *International Journal of Testing*, vol. 11, no. 1, pp. 53–70, Feb. 2011, publisher: Routledge _eprint: https://doi.org/10.1080/15305058.2010.508570. [Online]. Available: https://doi.org/10.1080/15305058.2010.508570