Request for Information (RFI) on Cognitive Effects in Cyber Operations
IARPA-RFI-22-07

IARPA is seeking information on methods, studies, findings, approaches, and appropriate metrics for characterizing the cognitive effects in cyber operations. This RFI is issued for planning purposes only and does not constitute a formal solicitation for proposals or suggest the procurement of any material, data sets, etc.

Definitions

- Cyber Operations: The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.
- Cyber Operators: The humans performing cyber operations, both defensive (e.g., Incident Response Team, Blue Team, security operations center, Cyber Protection Team) and offensive (e.g., unauthorized hacker, advanced persistent threat (APT), Red Team).
- Cognitive Effects: A cognitive bias, innate human limitation, or psychological/physiological vulnerability.
- Cyberpsychology: The scientific field that integrates human behavior and decision-making into the cyber domain, allowing us to *understand*, *anticipate* and *influence* cyber operator behavior.

Background

Cyberpsychology is the emerging scientific field that integrates human behavior and decision-making into the cyber domain [1]. Techniques currently used in online advertising, political campaigning, e-commerce, and online gaming successfully profit from vulnerabilities in human psychology. Cyber attackers often take advantage of similar human limitations through social engineering. Cognitive effects relevant to cyber attackers have begun to be hypothesized [2] [3], but only a few have been validated in cyber scenarios [4] [5]. Recent experiments demonstrating the power of framing effects were investigated, indicating that attackers who were provided information that deceptive technology was present on a network had less forward progress [6]. Additional work has examined the effect factors like uncertainty have when interacting with other cognitive effects [7].

IARPA has shown success in reducing cognitive biases in intelligence analysis [8]. However, research into cognitive effects in the cyber domain has been less prolific. Some aspects of cyber defense team decision-making have been studied [9] and mitigations of biases leading to issues in sharing and collaboration have been recommended [10]. It has been suggested that cognitive effects can be used to thwart cyber attackers, building on concepts like oppositional human factors [11]. However, investigations into cyber attack teams and their biases have been less examined [12]. A deeper look at the advancements that have been made to understand the cognition of cyber operators may enable the research objectives this RFI seeks to identify.

Scope

For IARPA to evaluate if there have been sufficient advancements to support a research effort aligning with examining cognitive effects in cyber operations, it is necessary to ask the following questions:

1. What emergent findings or approaches are most likely to enable a better evaluation of cyber operator decision-making and cognitive effects?
2. What confounders are likely to obfuscate efforts to experimentally evaluate cognitive effects in cyber scenarios? What approaches could mitigate these confounders?
3. What cognitive effects are known or are likely linked to behavioral changes in cyber operators? What individual measures, cultural factors, or other specific attributes are important factors to study alongside the cognitive effect and why?
    a. Defensive operators
    b. Offensive operators
4. What metrics and established methodologies are most appropriate for evaluating cognitive effects in cyber operations?
    a. Defensive operations
    b. Offensive operations
5. Which phases of the cyber kill chain are most appropriate for studying these innately human cognitive effects and why?
6. What datasets, testbeds or cyber ranges exist which could inform understanding cyber operator decision-making and cognitive effects, and support experimentation?
7. What specific cyber operations skills are necessary in participants to experimentally evaluate these cognitive effects? How can these skilled participants best be recruited and retained?
8. What kinds of intrinsic and extrinsic motivators drive cyber operator behavior? What kinds of experimental designs can best approximate these motivators in recruited participants?

Preparation Instructions to Respondents:
IARPA requests that respondents submit responses to the above questions for use by the Government in formulating a potential program. IARPA requests that submittals address one or more of the above questions and include a brief technical description of potential approach(es) or concept, outline critical technical issues/obstacles, describe how the approach may address those issues/obstacles and comment on the expected performance and robustness of the proposed approach. If appropriate, respondents may also choose to provide a non-proprietary rough order of magnitude (ROM) estimate regarding what such approaches might require in terms of funding and other resources for one or more years to execute the respondent's vision for understanding and modifying cognitive effects in cyber operators. This announcement contains all of the information required to submit a response. No additional forms, kits, or other materials are needed.

IARPA welcomes responses from all capable and qualified sources including academia, industry, government, national laboratories, and other federally funded research entities from within and outside of the U.S. This includes perspectives and associated capabilities for effectively evaluating potential research approaches.

Reponses must meet the following formatting requirements:

1. A one-page cover sheet that identifies the title, organization(s), respondent's technical and administrative points of contact - including names, addresses, phone and fax numbers, and email addresses of all co-authors, and clearly indicating its association with IARPA-RFI-22-07;
2. A substantive, focused, one-half page executive summary;
3. A response to one, some, or all of the questions posed above with a maximum of five pages;
4. A description (limited to two pages) of the technical challenges associated with the above topic and potential research approaches to address the interests described;
    a. A single quad-chart depicting the described approach, key ideas, and potential impact – may include supportive figures or illustrations. This quad chart can be submitted as a single slide Power Point or single page PDF. This does not count against the page limit.
5. A list of references (any significant claims or reports of success must be accompanied by citations – citations do not count against the 7-page limit; and
6. All documents are limited to 12-point Times New Roman font, appropriate for single-sided, single-spaced 8.5 by 11-inch paper with 1-inch margins.

Submission Instructions to Respondents:
Responses to this RFI are due no later than 5:00 p.m., Eastern Time, October 4, 2022. All submissions must be electronically submitted to dni-iarpa-rfi-22-07@iarpa.gov as a PDF document. Inquiries to this RFI must be submitted to dni-iarpa-rfi-22-07@iarpa.gov. Do not send questions with proprietary content. No telephone inquiries will be accepted.

Disclaimers and Important Notes:
This is an RFI issued solely for information and planning purposes and does not constitute a solicitation or authority to enter into negotiations for a contract. Respondents are advised that IARPA is under no obligation to acknowledge receipt of the information or to provide feedback to respondents with respect to any information submitted under this RFI. Responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Respondents are solely responsible for all expenses associated with responding to this RFI. IARPA will not provide reimbursement for costs incurred in responding to this RFI. It is the respondent's responsibility to ensure that the submitted material has been approved for public release by the information owner. The Government does not intend to award a contract on the basis of this RFI or to otherwise pay for the information solicited, nor is the Government obligated to issue a solicitation based on responses received. **No proprietary and no classified concepts or information shall be included in the submittal.** However, should a respondent wish to submit classified concepts or information, prior coordination **must** be made with the IARPA Chief of Security by emailing dni-iarpa-rfi-22-07@iarpa.gov with a request for coordination with the IARPA Chief of Security. Input on technical aspects of the responses may be solicited by IARPA from non-Government consultants/experts who are bound by appropriate non-disclosure requirements.

Contracting Office Address:
Office of the Director of National Intelligence, Intelligence Advanced Research Projects Activity
Washington, District of Columbia 20511 United States

Primary Point of Contact:
Dr. Kimberly Ferguson-Walter
Program Manager
Intelligence Advanced Research Projects Activity

References

[1] J. McAlaney, L. A. Frumkin and V. Benson, Psychological and Behavioral Examinations in Cyber Security, IGI Global, 2018.

[2] C. Johnson, R. Gutzwiller, K. Ferguson-Walter and S. Fugate, "A cyber-relevant table of decision making biases and their definitions," ResearchGate, 2020.

[3] C. K. Johnson, R. S. Gutzwiller, J. Gervais and K. J. Ferguson-Walter, "Decision-Making Biases and Cyber Attackers," in *IEEE International Conference on Automated Software Engineering, Workshop on Human Centric Software Engineering and Cyber Security*, 2021.

[4] J. Dykstra and C. L. Paul, "Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations," in *11th USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2018.

[5] C. K. Johnson, "Decision-Making Biases in Cybersecurity: Measuring the Impact of the Sunk Cost Fallacy to Delay and Disrupt Attacker Behavior," Arizona State University, doctoral dissertation, 2022.

[6] K. Ferguson-Walter, M. Major, C. Johnson and D. Muhleman, "Examining the Efficacy of Decoy-based and Psychological Cyber Deception," in *USENIX Security Symposium*, 2021.

[7] E. Cranford, C. Gonzalez, P. Aggarwal, M. Tambe and C. Lebiere, "What Attacks Known and What They Have to Lose: Framing Effects on Cyber-attacker Decision Making," in *Human Factors and Ergonomics Society Annual Meeting*, 2020.

[8] "SIRIUS," [Online]. Available: https://www.iarpa.gov/index.php/research-programs/sirius.

[9] V. Mancuso, G. J. Funke, V. Finomore and B. A. Knott, "Exploring the Effects of "Low and Slow" Cyber Attacks on Team Decision Making," in *Human Factors and Ergonomics Society Annual Meeting*, 2013.

[10] P. Rajivan, "Information Pooling Bias in Collaborative Cyber Forensics," Arizona State University, Doctoral Dissertation, 2014.

[11] R. Gutzwiller, K. Ferguson-Walter, S. Fugate and A. Rogers, ""Oh, Look, a Butterfly" A Framework For Distracting Attackers To Improve Cyber Defense," in *Human Factors and Ergonomics Society*, 2018.

[12] C. Johnson, K. Ferguson-Walter, R. S. Gutzwiller, D. Scott and N. J. Cooke, "Investigating Cyber Attacker Team Cognition," in *Human Factors and Ergonomics Annual Meeting*, 2022.