Request For Information – Deception for Cyber Defense Research
RFI Number: IARPA-RFI-16-07
Agency: Office of the Director of National Intelligence
Office: Intelligence Advanced Research Projects Activity

IARPA-RFI-16-07

Synopsis

Request for Information (RFI): Deception for Cyber Defense Research

The Intelligence Advanced Research Projects Activity (IARPA) is seeking information on research efforts in the area of deception for cyber defense. This request for information (RFI) is issued solely for information gathering and planning purposes; this RFI does not constitute a formal solicitation for proposals. The following sections of this announcement contain details of the scope of technical efforts of interest, along with instructions for the submission of responses.

Background & Scope

Historically, denial and deception (D&D) has been used by militaries for defense, whether it be to instill uncertainty, or to provide misinformation. D&D can also be looked at similarly for increasing cyber defense posture and resiliency. Adapting D&D to support the engagement of cyber adversaries is a concept that has been gaining momentum, although, the current state of research and practice is still immature: many techniques lack rigorous experimental measures of effectiveness, information is insufficient to determine how defensive deception changes attacker behavior or how deception increases the likeliness of early detection of a cyber attack. For present purposes, "deception" is the deliberate action taken by a cyber defender to mislead and gain an advantage over a cyber adversary through a variety of tactics such as manipulation, distortion, or falsification of evidence[1].

The purpose of this RFI is to identify existing capabilities and emerging methods related to deception for cyber defense and approaches for assessing the performance of these methods.

Responses to this RFI should answer any or all of the following questions:

1. Existing Deception Methods
    a. What are the existing methods for deception to support cyber defense? Provide specific examples (capability names and references) that implement these methods. What are the limitations of these methods? Are these methods fully automated or do they require human operation?

[1] Heckman, K.E., Stech, F.J., Thomas, R.K., Schmoker, B. Alexander, W. T. (2015) Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense, Advances in Information Security, Vol 63, Springer, NY.

b. What is/are the main goal(s) of deception activities for the capabilities provided in 1.a (e.g., threat intelligence/observation, deterrence, delay, confuse, misinform, redirect, denial, detection, frustration, etc.)? Please describe all that apply.
c. What types of deception does the research/capability identified in 1.a investigate and employ (e.g., denial through blocking/blacklisting/firewalling, detection, decoys, honey pot/traps/nets, honey tokens/fakes/misrepresentations/forgeries, etc.)? Please describe all that apply.
d. Where in the cyber kill chain does the research or capabilities identified in 1.a focus and where does it have the greatest impact (reconnaissance, weaponize, deliver, exploit, install, command, act, etc.)? Please describe all that apply.
e. What are the primary target(s) of interest of relevant research/capabilities (e.g., network, data, user spaces, kernel, mobile/wireless, etc.)? Please describe all that apply.
f. What methods or research exists for influencing cyber attackers? Do any of them leverage game theory or related concepts?

2. Test and Evaluation of Methods
    a. What metrics and evaluation methods do you employ in your research or for your deception capability?
    b. How accurate are these methods? What approaches have been used to validate or assess the accuracy and/or usefulness of these methods? What are their strengths and limitations?
    c. What environments were used to evaluate these methods?
    d. More generally, how can these approaches be evaluated, given practical limits to study duration and cost?
    e. Were human science researchers used for evaluation? What specific approaches leveraged human subjects for research and evaluation?

3. Emerging Methods
    a. What novel methods could be developed/expanded or adapted to improve or replace existing methods for deception to support cyber defense?
    b. What recent or underappreciated publications and technical developments are of critical relevance to the development, improvement, or evaluation of deception for cyber defense?

4. Organizational/Services Information
    a. How long has your organization been engaged in deception research or capability development?
    b. Is your technology integrated with adjacent deception technology solutions? If yes, please specify the type of adjacent deception capability.
    c. Please provide references to research publications and/or cases which demonstrate the utility and application of your research/capability.
    d. Do you provide courses or customer education products related to deception management?

The responses to this RFI may be used to support a one-day workshop on deception for cyber defense. An expected result for such a workshop is the identification of promising areas for research investment.

Preparation Instructions to Respondents

IARPA requests that respondents submit ideas related to this topic for use by the Government in formulating a potential program. IARPA requests that submittals answer questions concisely, briefly and clearly describe the potential approach 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. This announcement contains all of the information required to submit a response. No additional forms, kits, or other materials are needed.

IARPA appreciates responses from all capable and qualified sources from within and outside of the US. Because IARPA is interested in an integrated approach, responses from teams with complementary areas of expertise are encouraged.

Responses have 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 RFI-16-07;
2. A substantive, focused, one-half page executive summary;
3. A description (limited to 5 pages in minimum 12 point Times New Roman font, appropriate for single-sided, single-spaced 8.5 by 11 inch paper, with 1-inch margins) of the technical challenges, answers to RFI questions, and suggested approach(es);
4. A list of citations (any significant claims or reports of success must be accompanied by citations);
5. Optionally, a single overview briefing chart graphically depicting the key ideas.

Submission Instructions to Respondents

Responses to this RFI are due no later than 4:00 p.m., Eastern Time, on July 01, 2016. All submissions must be electronically submitted to dni-iarpa-rfi-16-07@iarpa.gov as a PDF document. Inquiries to this RFI must be submitted to dni-iarpa-rfi-16-07@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. Respondents are advised that IARPA is under no obligation to acknowledge receipt of the information received, or 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. Neither proprietary nor classified concepts or information should be included in the submittal. 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:
Robert Rahmer
Intelligence Advanced Research Projects Activity
dni-iarpa-rfi-16-07@iarpa.gov