ReSCIND

REIMAGINING SECURITY WITH CYBERPSYCHOLOGY-INFORMED NETWORK DEFENSE

INTELLIGENCE VALUE

Solutions from the ReSCIND program will provide defenders a much-needed advantage by expanding the traditional cyber defense toolkit to leverage well-established cognitive biases and human limitations that can be intensified and manipulated to impede cyber attackers. This will help to rebalance the asymmetry of cyber defense, providing a low-risk force-multiplier to help protect National Security Systems and other intelligence community (IC) assets across various phases of a cyber attack.

In the cyber domain, it is often harder to defend than it is to attack. The ReSCIND program looks to rebalance this asymmetry by exploring novel methods for manipulating the human behind the attack during various stages of a cyber attack. Rather than just detecting and stopping suspicious movement on the network, performers will develop solutions to increase the effort and resources spent by cyber attackers by impacting their decision-making. To support and protect the IC mission, the ReSCIND program's objectives are to: 1) identify cognitive biases or human limitations relevant to cyber attack behavior, 2) develop technology to induce these biases in the cyber domain and measure the effects of the bias on cyber attacker behavior and successes, 3) provide algorithms for automated adaptation of the solutions, 4) supply cyber-specific computational cognitive models based on observed cyber operations cognition and behavior.

Utilizing the scientific foundation of cyberpsychology and how attacker cognition and behavior can be influenced, performer solutions will take advantage of psychological vulnerabilities, such as innate decision-making biases and human limitations, to manipulate an attacker's judgement and reaction, potentially causing long-term effects. Performers will create bias sensors that can measure the presence of a bias using typically available cyber data, as well as cyber triggers that create an on-network situation to increase or exacerbate the biases. These sensors and triggers will be combined to create cyberpsychology-informed defenses (CyphiDs). ReSCIND seeks to augment traditional cyber defenses to help rebalance the asymmetry of cyber defense by imposing a cyber penalty on attackers--causing wasted time and effort--thus delaying and thwarting attacks.

Performer solutions are submitted to the ReSCIND Testing & Evaluation (T&E) teams for controlled experimentation through human subjects research (HSR) with cyber experts. The ReSCIND program begins in late 2023 and has a duration of 45 months. The program comprises three phases, including an 18-month long phase one, a 15-month long phase two, and a 12-month long phase three.

PRIME PERFORMERS

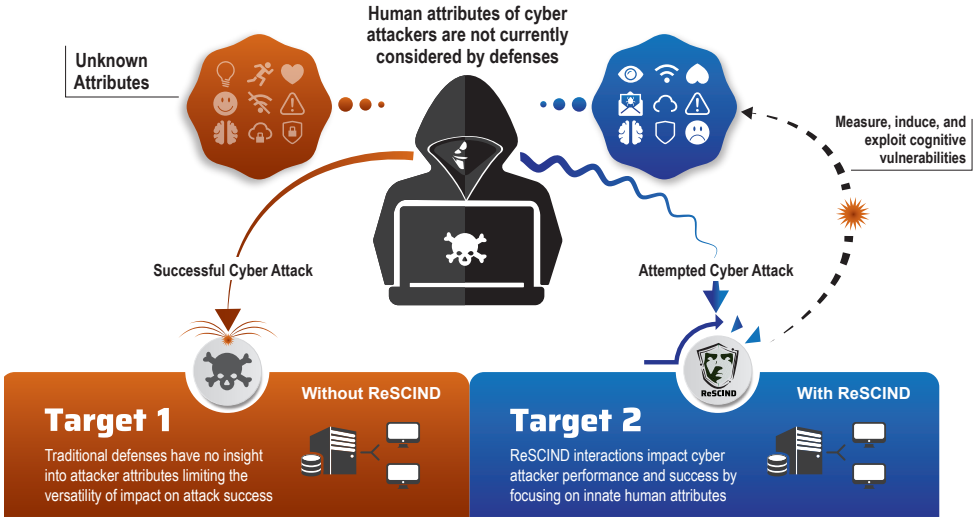
- Charles River Analytics, Inc.
- GrammaTech, Inc.
- Peraton Labs
- Raytheon Technologies Research Center
- SRI International

TESTING AND EVALUATION PARTNERS

- University of Maryland's Applied Research Laboratory for Intelligence and Security
- MIT Lincoln Laboratory
- Lawrence Livermore National Laboratory (U.S. Department of Energy)
- MITRE

KEYWORDS

- Cyber Defense
- Advanced Persistent Threat
- Psychology
- Cognitive Bias
- Human Behavior
- Human Computer Interaction



ReSCIND

PROGRAM MANAGER
Kimberly Ferguson-Walter, Ph.D.
kimberly.ferguson-walter@iarpa.gov