Opportunity Title: Autonomous AI-Powered Red Teaming for Enhanced Cybersecurity
Opportunity Reference Code: ICPD-2025-12

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2025-12

How to Apply **Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 3 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orise.orau.gov/icpostdoc/index.html.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 2/28/2025 6:00:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

In some government and national infrastructure facilities, isolated computer networks exist due to legacy systems or high sensitivity levels. These critical systems must be defended against from cyber-attacks from hostile actors, necessitating rigorous testing of blue cybersecurity teams’ response to potential network breaches and identification of vulnerabilities introduced by the configuration changes or new equipment. While penetration testing can identify existing vulnerabilities and assess blue team response, this research focuses on developing autonomous AI-powered red agents that can comprehensively test entire cybersecurity systems and detect vulnerabilities. To accelerate testing, AI-driven automation of red agent testing is proposed, which may also involve competition with AI-powered autonomous blue agents.

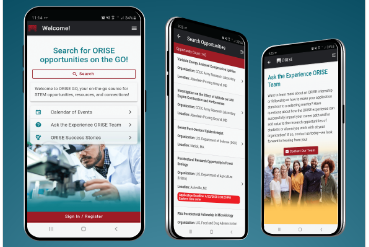
The research question: How can autonomous AI-powered red agents be designed to effectively identify vulnerabilities in isolated computer networks, simulate real-world attack scenarios, and enhance the overall cybersecurity posture of critical facilities?

Example Approaches:

There are two approaches outlined that should be considered:

- Stealthy approach: The red agent operates covertly, using advanced techniques to evade detection while identifying and exploiting vulnerabilities.
- Rapid exploitation approach: The red agent takes a more overt approach, rapidly identifying zero-day vulnerabilities and exploiting them quickly, simulating a real-world attack scenario

The proposed approach may involve the development of a hybrid AI framework that combines traditional cybersecurity techniques with



generative AI and machine learning algorithms. This framework will be designed to simulate various attack scenarios, including network vulnerabilities, phishing attacks and unauthorized device identification.

This research will push the boundaries of current AI-powered red agent technology by developing a novel framework that can adapt to evolving attack scenarios and learn from experience. This will ultimately enable the development of more sophisticated and effective cybersecurity testing and evaluation methods for blue teams.

Key Words: Artificial intelligence (AI), Machine learning (ML), Deep learning (DL), cybersecurity, red teaming, penetration testing, vulnerability assessment, zero-day exploits, autonomous systems, cyber threat intelligence, network security, endpoint security, advanced persistent threats (APTs), Security information and event management (SIEM), intrusion detection systems (IDS), intruder prevention systems (IPS), security orchestration automation and response (SOAR), threat hunting, cybersecurity analytics, generative adversarial networks (GANs).

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the appointment start date
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Point of Contact Keri Tarwater

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (3 👁)
  - **Computer, Information, and Data Sciences** (17 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (11 👁)
  - **Other Non-Science & Engineering** (2 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)

- **Social and Behavioral Sciences** (30 👁)