Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVAIR 2023-0095

Topic # N202-121
Identifying and Characterizing Cognitive Sensor Systems in Tactical Environments
Vadum

WHO

SYSCOM: NAVAIR

Sponsoring Program: PMA-231 E-2/C-2 Airborne Command and Control Systems

Transition Target: Maritime surveillance radars; Airborne RF ISR across the DoD; platforms such as the MQ-25, MQ-4C, and MH-60R

TPOC: (301) 342-3482

Other Transition Opportunities: The U.S. Department of Defense fields thousands of airborne, sea surface, and terrestrial radar systems, each of which may be vulnerable to cognitive electronic attack. These radars represent the largest market for the Vadum-developed Electronic Warfare Adversary Logic Exploitation System (ALES) algorithms.

Notes: Future cognitive electronic warfare (EW) systems will be capable of not only adapting to their environment, but also assessing their effects on the adversary and modifying their techniques to improve performance. This SBIR effort explores the utility of cognitive electronic protection through the modeling and exploitation of cognitive jammer decision logic to determine an optimal electronic protection (EP) strategy to defeat the jammer, and to develop a framework for the implementation of specific cognitive EP and classification algorithms for future transition.

WHAT

Operational Need and Improvement: A variety of approaches are being employed as the basis for the underlying machine learning. These cognitive systems train continuously while operational in an unsupervised fashion in an effort to gain maximum insight to a dynamic threat environment. For example, concepts for true cognitive electronic warfare systems envision a neural network-driven sensor that “should be able enter into an environment not knowing anything about adversarial systems, understand them and even devise countermeasures rapidly”. As our adversaries field these systems, we will seek methods to counter them and in the same vein as we develop the very adaptive systems, we must understand their vulnerabilities and take steps to mitigate threats.

Specifications Required: In order to be successful in future engagements, we must better understand how to exploit fundamental "blind spots" in adversary training algorithms and system capabilities that the adversary may utilize. To this end, Vadum's research effort considers undetectable adversarial training techniques as well as other approaches when designing a solution. Overall, Vadum seeks to develop innovative and operationally efficient approaches to exploit weaknesses in an adversary’s neural network-based cognitive sensing systems, and by association, techniques to protect defend US DoD systems from deception.

Technology Developed: Vadum is developing the Adversary Logic Exploitation System (ALES), a set of algorithms to identify and characterize capabilities and decision logic of cognitive adversary jammers and support automated selection of electronic protection (EP) techniques to defeat the jammer. ALES provides a sustained competitive advantage that allows maritime ISR platforms to automatically detect and characterize jammer capabilities, and suggest appropriate EP techniques to mitigate jamming effectiveness.

Warfighter Value: Cognitive electronic protection systems will counter the increasing complexity and capability of jammer systems allowing cognitive sensors to prosecute their missions successfully in the presence of advanced electronic attack.

WHEN

Contract Number: N68335-22-C-0238 **Ending on:** Jun 20, 2024

Milestone	Risk Level	Measure of Success	Ending TRL	Date
First Capability Drop	Low	Basic Functionality	4	2nd QTR FY23
Second Capability Drop	Medium	Improved Adversary Capability	5	2nd QTR FY24
Third Capability Drop	Medium	Improved Adversary Capability	6	3rd QTR FY24

HOW

Projected Business Model: Vadum will serve as an cognitive electronic protection algorithm provider supporting integration, test, improvement, and sustainment of cognitive electronic protection algorithms to developers of radar systems which must operate in contested environments.

Company Objectives: Vadum's objective is to protect United States lives and assets by providing warfighters with the most capable cognitive electronic warfare solutions.

Potential Commercial Applications: Implement algorithmic approaches and concepts to defeat adversarial cognitive-based systems into Navy operation systems and concepts of operations. Incorporate methods to protect our own cognitive based sensors from exploitation. The same general techniques are applicable to a wide range of data-driven cognitive systems including commercial applications utilizing internet-based data mining.

Contact: Dr. Laura Tolliver, Business Area Lead
laura.tolliver@vaduminc.com (919) 341-8241 x175