Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
ONR Approval #43-4388-18

Topic # N141-078
Develop a Methodology for Cyber-Electronic Warfare Battle Damage Assessment (BDA) using Game Theory
Vigilant Cyber Systems, Inc.

WHO

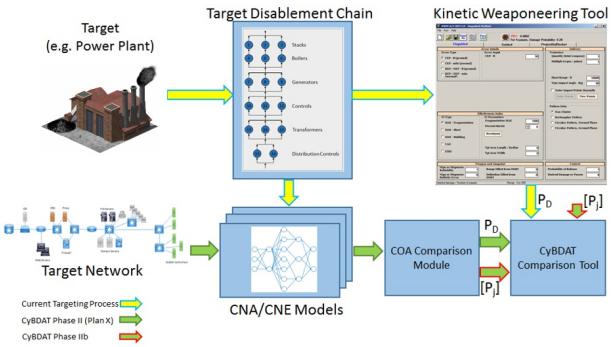
SYSCOM: ONR

Sponsoring Program: Code 30

Transition Target: JTCG-ME

TPOC:
Dr. Waleed Barnawi
waleed.barnawi@navy.mil

Other transition opportunities: Army Cyber command, US Cyber Command



Concept of Operations for CyBDAT

WHAT

Operational Need and Improvement: Current mission planning toolkits do not include the ability for planning staff to compare kinetic and cyber fires, especially against cyber physical systems. CyBDAT provides a comparison tool based on probability models that allow mission planners to set their preferences across 20 different success measures including probability of kill, attribution, persistence, and many others. Current planning methods require intensive research on an individual case by case basis for inserting cyber fires into mission planning, whereas CyBDAT will pull from a database with dozens of preassigned mission templates, weapons, and the statistical data behind each attack.

Specifications Required: - This tool must be able to quantify the contribution of Computer Network Attack (CNA), Computer
Network Exploitation (CNE), and Electronic Attack (EA) to the warfighting outcome in the physical realm.
- Design and implement an automated range for experiment, measurement and test of attacks on Cyber Physical Systems (CPS)
- Design a tool to perform the Course-of-Action (CoA) analysis for cyber attacks
- Design a tool to enable the comparative analysis between cyber and kinetic attacks on Cyber-Physical Systems

Technology Developed: VCS has successfully developed a range capable of standing up virtual targets for cyber physical systems. We have successfully demonstrated this capability on military and civilian vehicles, as well as a simple industrial control system (chemical plant). We are currently working on a higher fidelity virtualized system based on Siemens PLCs replicating a power distribution station.

Warfighter Value: Rapid virtual capability to test industrial control systems both offensively and defensively on the CPS range.

Toolkit for tactical commanders to allow them to accurately assess the probabilities and outcomes of using different cyber weapons and directly compare them to the kinetic alternatives.

WHEN

Contract Number: N68335-18-C-0048 **Ending on:** June 10, 2022

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Virtual Range Demonstration on Realistic ICS Target	Low	PM Opinion of Demonstration	5	2nd QTR FY19
Classified Option Exercised with Classified DD254 and SCIF	Med	Contract modification executed and SCIF approved	N/A	3rd QTR FY19
Incorporation and validation of JTCG-ME Data Standards into CyBDAT tests	Med	JTCG-ME Sign-Off on Test Results and Test Reports using their standards	6	1st QTR FY20
Participate in classified military training exercise	Low	Successful participation as determined by PM	5	1st QTR FY19

HOW

Projected Business Model: Sell CyBDAT directly to JTCG-ME as completed product, and incorporate into their mission planning suite of tools for cyber BDA and cyber mission planning.

Utilize CyBDAT and support cyber testing via virtual range to setup and run tests both offensively and defensively for DoD customers who care about medium fidelity virtual versions of ICS and other CPS.

Company Objectives: The VCS core competencies are DoD Cyber Testing and Evaluation support, software development, and penetration testing. We primarily focus on providing SME level consulting to DoD customers, including the testing and training communities. We feel that CyBDAT could be marketed directly to this community, leveraging our existing competencies and relationships. We also anticipate the automated range piece of this research can support future penetration testing and validation testing efforts for cyber physical systems. As the automated CPS range becomes more robust we see a strong commercialization path of hosting testing exercises on the range, or taking the Range Management Software Suite and incorporating it into larger tests and training exercises such as Bold Alligator.

Potential Commercial Applications: Virtual range supporting commercial ICS customers such as oil and gas industry, and automobile industry for cyber testing CPS assets.

Contact: Dustin Heath, COO
dheath@vigilantsys.com 336-769-6600