Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
ONR Approval #43-3252-17

Topic # N141-078

Develop a Methodology for Cyber-Electronic Warfare Battle Damage Assessment (BDA) using Game Theory

Vigilant Cyber Systems, Inc.

WHO

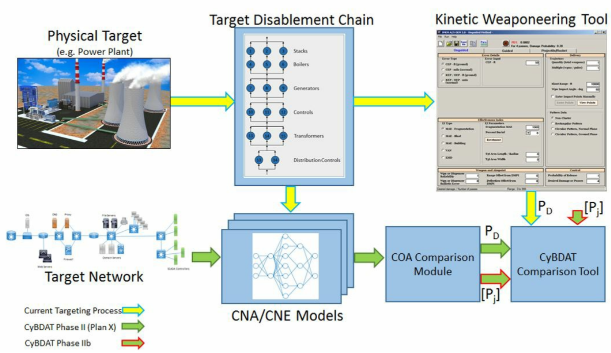
SYSCOM: ONR

Sponsoring Program: Cyber Battle Damage Assessment

Transition Target: SPAWAR, NAVAIR, T&E Community, TRADOC

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

Other transition opportunities:
Future Marine Corps Air Ground Task Force (MAGTF) operations, Army Cyber Command, US Cyber Command for both training and analysis tool development.



Copyright 2015, Vigilant Cyber Systems, Inc.

Notes:

Cyber Battle Damage Assessment Concept of Operations - VCS has developed the Cyber Battle Damage Assessment Tool (CyBDAT). A modeling tool that enables a comparative analysis between information related capabilities and traditional kinetic fires during mission planning. A methodology was developed to quantify the value of cyber exploits and electronic attacks within the relevant mission threads to inform decisions made on the battlefield.

WHEN

Contract Number: N00014-16-C-1044 **Ending on:** December 31, 2017

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Completed SBIR Phase I Proof-Of-Concept	High	Successful demonstration of comparison tool and results of thought experiments	3	November 2014
Complete Phase II Prototype of Comparison Tool and CPS Automated Range	Med	Working Prototype of Range and Comparison Tool	4	December 2017
Comparison Tool and CPS Range Fully Functional and Working in Relevant Environment	Med	Successful integration and results in established test such as Bold Alligator	6	December 2020
Integrated Comparison Tool with Existing Planning Software	Med	Transition to Prime for integration and Warfighter use.	8	December 2021

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 proof-of-concept comparison tool mockup, as well as several thought experiments to identify relevant factors to feed the comparison tool. Implementation has begun on an automated Cyber Physical System range, which will be used for testing to generate and capture the data required to feed the probability models. The work to develop the algorithms that will feed the Course-of-Action (CoA) tool is ongoing, as well as integration with DARPA's Plan-X program.

Warfighter Value: The tactical commander who has decision authority for a mission will now have a toolkit where he can accurately assess the probabilities and outcomes of using different cyber weapons and directly compare them to the kinetic alternatives.

HOW

Projected Business Model: The business case for CyBDAT is to identify and integrate with a prime integrator who is already providing software to the mission planning community or training community. We will subcontract to them and continue development and support under a CPFF subcontract with our established labor rates for support engineers. The automated range can be developed as an integrated part of the comparison tool, or as a separate project supporting stand-alone CPS automated testing for private and public sector customers.

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: In terms of commercialization outside of DoD, the best fit is in the industrial control space penetration testing for large cyber physical systems such as traffic infrastructure networks, and power plants. The automated CPS range could support a virtual clone of these systems, allowing for rapid and risk free testing with a medium fidelity.

Contact: Dustin Heath, Chief Operating Officer
dheath@vigilantsys.com 3367696600