Department of the Navy SBIR/STTR Transition Program

STATEMENT A. Approved for public release; distribution is unlimited. ONR Approval # 43-1256-16

Topic # N132-132

Modeling of Cyber Behaviors to Wargame and Assess Risk (MOC-WAR)

Charles River Analytics Inc.

WHO

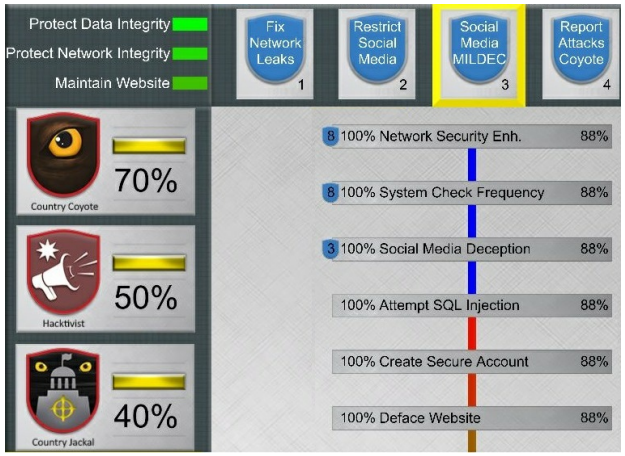
SYSCOM: ONR

Sponsoring Program: ONR Warfighter Performance Department (Code 34), Capable Manpower (CMP) Future Naval Capability

Transition Target: US Cyber Command (USCYBERCOM) Cyber Immersion Lab

TPOC:
Dr. Amy Bolton
amy.bolton@navy.mil

Other transition opportunities: US Air Force 547th Intelligence Squadron Threat Analysis Shop/Cyber Flag Exercise; DARPA Active Cyber Defense program; US Special Operations Command cyber defense applications; Raytheon Integrated Defense Systems (IDS) and Navy War College training applications; National Security Agency (NSA); Office of Naval Intelligence (ONI)



Notes: Modeling Cyber Behaviors to Wargame and Assess Risk (MOC-WAR) allows analysts to explore and wargame interactions between adversary socio-cognitive behaviors and proactive defensive mechanisms.

WHAT

Operational Need and Improvement: Cyber warfare has become a central concern for the US Navy. Understanding the behaviors and limitations of cyber adversaries can enable the Navy's cyber analysts, defenders, and policy makers to not only reduce the facets of the battlespace they must protect, but also to proactively exploit attacker weaknesses and biases in the process. Augmenting Naval cyber defenses with tools to proactively analyze the goals and decision-making processes of adversaries can enable Intelligence Community (IC) cyber defenders to aggressively manipulate those adversaries, reducing the threat on our infrastructure.

Specifications Required: Providing cyber analysts and policy makers with a deep understanding of adversary behaviors requires: (1) a modeling framework that provides flexible and extensible models for representing cyber behaviors; (2) a simulation-based wargaming capability to evaluate the range of possible adversary behaviors and outcomes; and (3) tools that help them to understand possible adversary behaviors and the defensive measures needed to drive more favorable outcomes.

Technology Developed: MOC-WAR merges disparate modeling formalisms into executable agents that can be deployed in wargaming exercises. It provides a mature visual programming environment designed for users without modeling experience to build effective behavior models. MOC-WAR incorporates a Futures Analyzer for exploring possible outcomes of behaviors, and a course-of-action explorer that shows the most likely, most threatening, and most beneficial behavioral sequences.

Warfighter Value: MOC-WAR combines multiple modeling approaches to provide cyber analysts with the flexibility to accurately assess behaviors of attackers. MOC-WAR allows analysts to apply their domain expertise in a cost-effective way by providing intuitive authoring tools without requiring modeling experience. By exploiting adversary socio-cognitive limitations, analysts will be able to drive novel and proactive cyber defenses, influence operations, and military deception operations.

WHEN

Contract Number: N00014-15-C-0115 **Ending on:** September 30, 2016

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Prototype MOC-WAR tool for analysts to explore cyber adversary behaviors	Med	Positive expert evaluation	4	January 2016
Demonstrate MOC-WAR prototype in USCYBERCOM Cyber Immersion Lab	Med	Successful formative evaluation with analysts	5	September 2016
(Option 1) Integrate MOC-WAR with Joint Enterprise Modeling and Analytics (JEMA) for IC applications	Med	Integrated JEMA/MOC-WAR system	6	June 2017
(Option 2) Integrate MOC-WAR in IC analysis environment	High	Successful integration into IC transition environment	7	January 2018

HOW

Projected Business Model: Our business model will focus on developing a MOC-WAR cyber analysis and defense application that can be directly licensed to cyber analysts or sold to larger businesses that provide complete cyber analysis and defense capabilities. We will include a basic license that includes the use of the MOC-WAR decision aid, using pre-constructed models, and a "Pro" version of the license that includes the use of the MOC-WAR authoring tool for constructing new models. We anticipate the Government having Government Purpose Rights for MOC-WAR; our future business model is to support the construction of new models and the extension of MOC-WAR to support future modeling needs.

Company Objectives: Our objective is to find partners in the cyber security space to further develop, and eventually integrate, MOC-WAR technologies into the existing tools used by cyber defenders, analysts, and policy makers, for both industrial and military applications. More broadly, we hope to use this as an opportunity to build upon our developing expertise in the cyber security domain, as well as to forge ongoing industrial and military relationships for related projects going forward.

Potential Commercial Applications: We will pursue relationships with companies focused on the development of existing cyber defense tools and intrusion detection systems (IDSs), offering MOC-WAR as a means to make these tools more proactive. MOC-WAR is particularly relevant to Managed Security Service Providers (MSSPs) who perform test and evaluation of cyber defenses, and would use MOC-WAR to both explore attacks that might be made against these systems and to defend against true cyber adversaries. The global MSSP market reached $6.67 billion in 2011, and is expected to reach $35.57 billion by 2021, providing a promising path for commercializing MOC-WAR.

Contact: Sean Guarino, Principal Scientist
sguarino@cra.com 617-491-3474x561