N252-110: Modeling and Simulation for Multi-modal Exercises

ADDITIONAL INFORMATION
N/A

TECHNOLOGY AREAS:
None

MODERNIZATION PRIORITIES:
Advanced Computing and Software | Integrated Sensing and Cyber | Sustainment & Logistics

KEYWORDS:
Training, exercise, cyber-defense; cyber-attack; information warfare; modeling and simulation

OBJECTIVE:
Develop a simulation model of information warfare that can realistically simulate multi-modal information attacks, in particular cyber-attacks and their precursors in social media campaigns. This model would be used for joint live, virtual constructive exercises to more realistically engage the training audience in scenarios in which information conflict plays important roles. This model be capable of developing and improving scenarios for multi-modal information warfare and provide guidance to planners and trainers to author and manage these exercises. The capability to explain, visualize and provide white cell adjudication support is highly desired in the final product.

DESCRIPTION:
Social media provides cyber-attackers with the affordances to recruit confederates in cyber-attack, track mission execution, and perform other acts of coordination prior to and during these attacks. Currently little training is available to assist cyber-defenders to identify the social media precursors, coordination efforts, and tracking. Most cyber-defense exercises are "tabletop" efforts that are largely controlled through "white card injects," Participants are told something has happened, then they are tasked to explain how they would respond. These exercises fail to prepare the participant in the role of first responder/cyber defender to "train as they fight" – to experience the many cues and tips that precede a cyber-attack or to rehearse the steps that they would take to discover, counter, and defeat cyber-attacks. Simulation exercises are needed to provide the opportunity for cyber-defenders to experience rehearsal and response in a sandbox environment to these types of hybrid attacks. The Navy seeks a model that brings together simulations of cyber-attack with simulated social media precursors and related information flows (i.e., "social-cyber maneuvers"). This would enable exercises to include cyber-attack together with their social-cyber precursors and counter-arts for live virtual constructive training.
The desired deliverable would develop: (1) a collection of related hybrid cyber and social-cyber data indicative of these hybrid maneuvers to provide the foundation for a realistic, validated augmented generation system for scenario data; (2) a framework for information maneuvers that broadly encompass cyber and social-cyber maneuvers that would support scenario development, synthetic data production, and scenario validation (for example, the MITRE ATT&CK framework); (3) authoring tools and decision aids to guide the development of social-media facilitated cyber-attacks; and (4) a simulation model that brings together the data and the framework to enable exercise planners to develop realistic scenarios and vignettes for social media facilitated cyber-attacks. The desired deliverable would be able to produce realistic scenarios in under 1 month. It is highly desired that scenario updates and vignette changes are possible in 24 hours so that training could be changed, with the scenario "sped up" or "slowed down" based on participant performance and with injects that could be created and launched during the exercise itself.

PHASE I:
Collect and validate data relevant to hybrid (cyber and social-cyber) attacks in a particular use case or set of use cases. Determine an initial data synthesis capability (such as a large language model) that can produce synthetic material indicative of an impending cyber-attack. Establish the feasibility of the initial framework for describing relationships, stages, and red flags that suggest cyber-adversaries are active. Prepare a Phase II plan.
For example, a Distributed Denial of Service (DDOS) attack has several stages: the "call to arms" stage in which audiences are enraged and encouraged to support the attack; recruitment of cyber-attackers; the distribution of

tools and resources; the identification of targets and the coordination of “fires” in terms of time and targets. This is an example of an initial use case for Phase I development.

PHASE II:

Enlarge the use cases from Phase I and collection of data relevant to these use cases for inclusion in a realistic augmentation generation system needed to validate synthetic data and conform to the developed framework. Develop a catalog of use cases and related information needed to guide exercise planners. Mature the Phase I data synthesis capability (possibly a special use large language model) to produce realistic volumes of synthetic data for information warfare exercises. Develop authoring tools to assist exercise planners in developing scenarios by using the framework and catalog of use cases. Create a working prototype of the simulation capability capable of a full technical demonstration in a live, virtual constructive exercise for validation of the system.

PHASE III DUAL USE APPLICATIONS:

Support the transition of the simulation model to Navy use. Components of this effort would be useful to cybersecurity companies in developing simulations of cyber-attacks and their precursors for the purpose of training cybersecurity professionals.

REFERENCES:

1. “Information. Marine Corps Doctrinal Publication (MCDP) 8.” United States Marine Corps, 21 June 2022. https://www.marines.mil/Portals/1/Publications/MCDP%208.pdf?ver=6gIvEcD0CUuPAgTSmyDNag%3d%3d
2. “Information in Marine Corps Operations (MDWP) 8-10. United States Marine Corps, 29 February 2024. https://www.marines.mil/Portals/1/Publications/MCWP%208-10%20(SECURED).pdf?ver=c4OjkntxdXoXZ9RvGMaIIA%3d%3d
3. Shu, Kai, Sliva, Amy, Sampson, Justin and Liu, Huan. “Understanding cyber attack behaviors with sentiment information on social media.” Social, Cultural and Behavioral Modeling: 11th International Conference, SBP-BRIMs, Washington DC, USA. Proceedings 11, 2018, pp. 377-388. https://www.cs.emory.edu/~kshu5/papers/sbp_cyber_senti.pdf
4. Khandpur, Rupinder Paul, Alguliyev, Rasim M. et al. “Crowdsourcing Cybersecurity: Cyber attack detection using social media.” Proceedings of the 2017 ACM on Conference and Knowledge Management, November 2017, pp. 1049-1057. https://dl.acm.org/doi/pdf/10.1145/3132847.3132866
5. Sapienza, Anna, Bessi, Allessandro, Damodaran, Saranya, Shakarian, Paulo, Lerman, Kristina and Ferrara, Emilio. “Early Warnings of cyber threats in online discussions.” IEEE International Conference on Data Mining Workshops (ICDMW), 2017, pp. 667-674. https://ieeexplore.ieee.org/document/8215726

TOPIC POINT OF CONTACT (TPOC):

TPOC-1: Rebecca Goolsby
PHONE: N/A
EMAIL: rebecca.l.goolsby.civ@us.navy.mil

TPOC-2: Ralph Wachter
PHONE: N/A
EMAIL: rwachter@nsf.gov