Call For Papers
Journal of Defense Modeling and Simulation
Special Issue: Cyber Modeling and Simulation

Special Issue Editors

J. Todd McDonald
University of South Alabama
jtmcdonald@southalabama.edu

Todd R. Andel
University of South Alabama
tandel@southalabama.edu

Mikel D. Petty
University of Alabama in Huntsville
pettym@uah.edu

Modeling and simulation has a long and studied history with mature theory and practice in a wide variety of computing domains. As a relatively young discipline, cyber security is still developing its own theory and practice of M&S and even its definition is fluid. Because of their kinship with network models in general, cyber M&S has benefited from the mature foundation of network models that allow for evaluation of defensive techniques and diagnostic prediction for botnets, worms, and network-based malware. Along manual analysis lines, virtualized environments have provided a great vehicle for penetration and security testing to probe the weaknesses of applications based on known threat models. M&S has centered also on development of frameworks to capture and describe attacks, threats, and mitigations for software vulnerabilities and malware artifacts. New technologies such as mobile devices, embedded systems, and cloud computing have further complicated the ability to realize simulation environments for cyber attacks.

In the realm of military thought, cyber has now become an operational warfighting domain of consideration and thus a new domain of knowledge, tools, and capabilities has emerged. Standardization of offensive and defensive cyber techniques and nomenclature as well as evaluation of cyber effects alongside other conventional munitions has now become part of DoD focus. Cyber M&S theory and practice must also support rapid configuration of simulated software, hardware, and networks to evaluate cyber impacts alongside traditional attacks as well. As a result of these emerging trends, both military and industrial sectors have great need for cyber M&S tools, techniques, and methodologies.

This special issue is devoted to publishing practical and theoretic approaches to measuring, modeling, simulation, and evaluation of cyber protection and defensive tools, methodologies, and techniques. Surveys on current trends, frameworks, and applications for cyber M&S are appropriate as well as recent developments in nomenclature, modeling frameworks, and classification to support cyber M&S applications. Articles with specific focus on integration of simulation techniques for the purpose of verification, validation, or testing are of particular interest. Case studies describing practical applications of modeling and simulation to hard problems of interest such as digital forensics, cloud computing, botnet-detection, malware analysis, software vulnerabilities, denial of service, and situational awareness are also in view.

Topics of interest to the special issue include, *but are not limited to*, the following:

- Analysis frameworks and theoretical models for cyber attack and defense
- Case studies of practical application of cyber M&S theory
- Models of cyber situational awareness and applicability to defensive or offensive operations
- Model applications for malicious software behavior, classification, spread, mitigation, and recovery

- Theory of cyber effects as munitions or in development of defensive strategies
- Cyber attack and threat modeling including attack trees and applications of graph theory
- Verification, validation, and testing of cyber defense or attack models against known cyber threats and vulnerabilities
- New cutting edge techniques or tools for cyber modeling visualization, response, and course of action selection

Submission and Review Process

Papers submitted to this special issue should be original and must not be under review elsewhere. Papers will be peer-reviewed in the same manner as other submissions to The Journal of Simulation. Full author instructions can be found at www.scs.org/jdms?q=node/95. Papers must be submitted electronically via http://mc.manuscriptcentral.com/jdms. Please indicate in the cover letter that the paper is intended for this special issue. Further information can be found at the Society for Modeling and Simulation at http://www.scs.org.

Important Dates

Submission: February 15, 2016
Notification of Acceptance/Rejection: June 15, 2016

For questions, contact the special issue editors shown above.