Geoffrey B. Dobson
gdobson@cs.cmu.edu

Prof. Kathleen M. Carley
Kathleen.carly@cs.cmu.edu

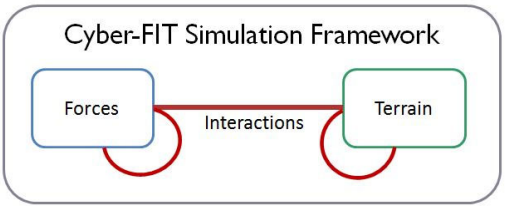
Carnegie Mellon University
www.casos.cs.cmu.edu

Cyber-FIT Simulation Framework

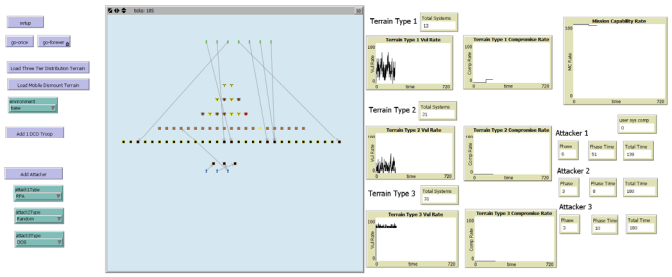
An agent-based modeling approach to simulating cyber team performance

PROBLEM STATEMENT:

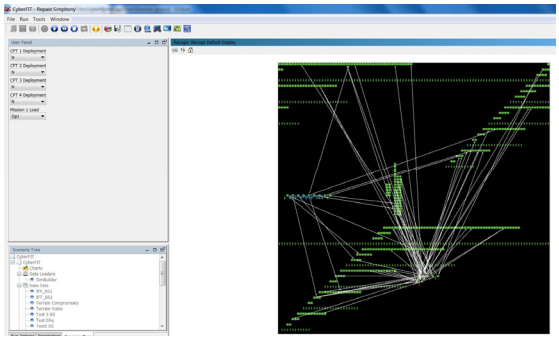
How can we project the effectiveness of cyber force packages against simulated enemies in cyberspace? Militaries all over the world are struggling with this question. It's very difficult to predict how cyber forces will perform against varying adversaries (numbers, sophistication levels, etc.), on varying terrain (system types, vulnerability rates, architecture, etc) when confronting varying attacks (denial of service, phishing, malware, etc). The Cyber-FIT framework is an agent-based modeling and simulation tool that provides a mechanism to manipulate agent rulesets, and then conduct virtual experiments. The virtual experiments address issues of military significance such as expected asset degradation, mission capability rate, time needed to repair, and terrain maneuverability.



NetLogo Dashboard View:



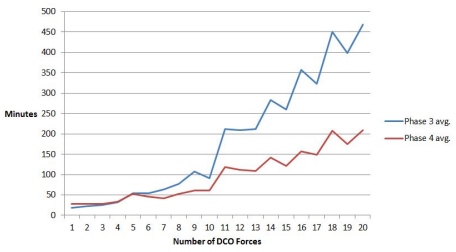
Repast Dashboard View:



Example Virtual Experiment:

How How many DCO forces should we deploy to maximize the time to complete phases three and four during a routing protocol attack with exploitation success rate of 15%?

Results:



This work was supported in part by the the Center for Computational Analysis of Social and Organization Systems (CASOS) and the SEI Software Scholars Program. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the U.S. government.

isr institute for SOFTWARE RESEARCH