**CIMoRE: Developing a Framework for a Critical Infrastructure Modeling and Response Environment**

Activities for individuals, organizations, and government agencies to plan for, protect from, and respond to cases of emergency or attack generally focus on paper and pencil planning sessions that don’t include computer simulated information or decision data. Modeling critical infrastructures and cyber physical systems have become a growing research area, as well as a common theme in training activities for cyber security practitioners and first responders over the past decade. One approach to modeling multiple critical infrastructures is to model all critical infrastructures in a single environment by converting them into a single standard protocol and implementing them in a single testbed.

This dissertation provides the road map of how the Critical Infrastructure Modeling and Response Environment (CIMoRE) could be developed to allow all critical infrastructure subsectors to be modeled in a single TCP/IP testbed. The Internet Scale Event and Attack Generation Environment (ISEAGE) is the testbed that was used as the backbone of this framework.

This dissertation addresses three main problems with using a unified TCP/IP testbed for modeling. First, the physical world critical infrastructure subsectors must be turned into network representations of themselves. This includes transforming the characteristics of their traffic into TCP/IP traffic and node data, as well as representing interdependencies between the critical infrastructure subsectors. Second, the ISEAGE testbed, its operational software ISEFLOW, and the ISEFLOW configuration file needed to be modified to allow for critical infrastructure subsector modeling. Additionally, the concept of network delay had to be added to ISEAGE. And, third, concept of traffic generation had to be added to ISEAGE to allow modeling of increases and decreases of traffic volumes for critical infrastructure subsectors. Along with traffic generation is the need to introduce events that simulate real world disruptions that could stem from that traffic generation.