One of the critical functions executed by the Cyber Battle Laboratory Facility is to provide **Modeling and Simulation (M&S)** support to validate current and future Command, Control, Communications and network related concepts, technologies and architectures. The Cyber Battle Lab is the TRADOC proponent for Communications Network Modeling and Simulation. The M&S functional area includes the execution of four (4) primary functions: traffic development, model development, network analysis, and Cyberspace and Electronic Warfare Operations (CEWO) analysis.

The first function is to provide the U.S. Army network modeling and simulation analytical community with validated Network Traffic data to feed U.S. Army models and simulations. Traffic development is based upon doctrinal rules which govern the manner in which Warfighters will execute their mission. The Cyber Battle Lab is recognized as the expert for telecommunications traffic data development within the U.S. Army.

The second function is to provide technical expertise in the area of communications network model development, testing, configuration management and integration. Model development includes the development of individual waveform models, integration of individual waveform models to make network models, model testing, model verification and validation as well as overall configuration management of these models. Current high fidelity models developed at the Cyber Battle Lab include EPLRS, NTDR, WNW, SRW, KASAT and an FCS SOS model.

The third function is to conduct communications network performance analysis using the traffic and models described in the first two functions. Communications Network Analysis includes operational architecture analysis, experimentation/demonstration support and combat developments concept and requirements analysis. The Cyber Battle Lab is also the Network Proponent for the Battle Laboratory Collaborative Simulation Environment (BLCSE) and therefore charged to ensure that realistic communications and network effects are realized within the TRADOC simulation environment.

The fourth function is to conduct Cyberspace and Electronic Warfare Operations (CEWO) capabilities performance analysis using the traffic and models described in the first three functions. CEWO Analysis includes Communications Network under threat analysis, operational architecture under threat analysis, experimentation/demonstration support and CEWO combat developments concept and requirements analysis.

A high level of preparation, detail and accuracy are the cornerstones of effective simulation based performance analysis tools and services provided and supported by the Cyber Battle Lab M&S.