



The Cyber Battle Lab (CBL) leads Cyberspace Operations concepts and capabilities experimentation for the Army. The CBL performs analysis, prototyping, assessment, and experimentation as a federal laboratory in order to determine and validate operational and conceptual requirements through current and future force warfighting experiments. Additionally, the CBL partners with sister Army R&D labs, Industry, and Academia to synchronize, coordinate, and accelerate the development process while codifying user, developer, and industry efforts to exploit technological advancements. The CBL is organized into six branches that provide current and the future force experimentation support.

1. The **Operations** branch supervises and coordinates CBL efforts, resources and assigned tasks.
2. The **Live Experimentation (LE)** branch plans and executes live experiments, builds and integrates working prototypes, and provides risk mitigation for both the requirements and acquisition communities. The LE branch also provides technology solutions for COCOM immediate operational needs.
  - a. The CYBER branch plans, coordinates and executes exercises aimed at informing TCM CYBER requirements, modifying DOTMLP processes, and development of TTPs/CONOPS to support operational CYBER mission threads. Intent is to simulate operational environments to perform testing and evaluation of CYBER capabilities while helping to inform the CEMA construct.
  - b. The EW branch plans, coordinates and executes exercises aimed at informing TCM EW requirements, modifying DOTMLP processes, and development of TTPs/CONOPS to support operational EW mission threads. Intent is to simulate operational environments to perform testing and evaluation of EW capabilities.

Intent is to simulate operational environments to perform testing and evaluation of EW capabilities while helping to inform the CEMA construct.

1. The **Regional Hub Node – Experimentation (RHN-E)** branch is a unique TRADOC enterprise satellite communications capability which facilitates Joint, Army, and TRADOC experimentation, including persistent support to NIE and AEWE, as well as reach back and DoDIN services to beyond line-of-sight EXFOR. The RHN-E extends Cyber range capabilities to Operational Forces in CONUS, Hawaii, and Alaska.
2. The **Concepts Experimentation (CE)** branch informs the Army Concept Framework (ACC, AOC, AFC) through a continual process of assessing current Army Operating Concept Required Capabilities (Cyber/EW), determining proponent learning demands based on Warfighting Challenges, and conducting Simulation and Analysis to further refine the concept framework. An array of live, virtual, and constructive (LVC) simulation venues are employed to achieve these goals, including SIMEXs, Wargames, GAMEXs, MAPEXs, and seminars.
3. The **Modeling and Simulation (M&S)** branch provides communications realism for ARCIC experimentation campaigns and analyses through the use of high fidelity network simulation suites with an emphasis on Cyber effects. The M&S branch also collects and characterizes functional proponent network demands for integration within simulations to determine gaps between capabilities and requirements of the tactical network.
4. The **Battle Lab Collaborative Simulation Environment (BLCSE) Cyber Enterprise Services Center (CESC)** branch provides the underlying closed IT enterprise, management, and collaboration services used by for the entire ARCIC concepts and capability development communities for distributed simulation and collaboration. The CBL operates the Army's Global Cyber Range NOSC to integrate Joint Cyber Range capabilities IOT establish a cyber range community unity of effort, experiment with Cyber NetOPS toolsets, develop analytics supporting cyber range and toolset requirements, and provide range access to the resident/institutional training mission of the CoE.  
The CBL drive the innovation of emerging capabilities to support the warfighter by enabling the experimentation and analysis of new networks, cyberspace operations and electronic warfare capabilities. Results of our experimentation, assessments, and analyses validate proposed technical solutions to resolve known DOTMLPF-P capability gaps within the cyberspace operations and EW force modernization lines of effort.