

# US Army Announces Plans for CyberQuest 2022

The Cyber Battle Lab at Army Futures Command (Huntsville, AL) has issued a Broad Agency Announcement (BAA) inviting industry and academia, as well as other government organizations, to " ... showcase their emerging cyber, electronic warfare, intelligence, and networking technologies at Cyber Quest 2022." The annual event, which will be held for the seventh time, will be conducted in March 2022 at Fort Gordon, GA, in partnership with the Army Expeditionary Warrior Experiment (AEWE) 2022 at Fort Benning, GA.

CyberQuest 2022 will focus on "the integration of network, cyberspace and electronic warfare capabilities into a CEMA cell's output within a Brigade's or Echelon Above Brigade's Tactical Operations Center undertaking Multi-Domain Operations. It looks to provide the CEMA cell with the ability to provide commanders with non-kinetic options to defeat threats while protecting their own capabilities," according to the BAA.

The Cyber Battle Lab is seeking proposals in several technology focus areas: 1) Electromagnetic Warfare; 2) networks and services; 3) tactical radio; 4) cyberspace operations; 5) intelligence applications (Intel Apps); and 6) Military Information Support Operations (MISO).

In the Electromagnetic Warfare (EW) focus area, the Cyber Battle Lab is seeking "organic, integrated EW capabilities to assist in creation of windows of advantage and multiple dilemmas in support of Multi-Domain Operations," according to the BAA materials. Among the EW capabilities the Army wants to test is a long endurance (>12 hours) UAS flying in a "follow-the-leader" orbit above a ground vehicle using cooperative TDOA for geolocation against a target signals of interest at

long range. In this area, the Army also wants to evaluate alternative TDOA time synchronization approaches for geolocation and test the ability to sense and locate aerial and ground targets via bistatic radar. Finally, the Army wants to demonstrate experimental C5ISR/EW Modular Open Suite of Standards (CMOSS) and PHOTON-compatible capabilities to inform future EW programs.

Another area of interest within the EW topic is the Army's Terrestrial Layer Systems – Echelons Above Brigade (TLS-EAB). At CyberQuest 2022, the Army wants to evaluate technologies that can support its upcoming TLS-EAB program. These include using terrestrial DF angle-of-arrival data to cue non-kinetic responses at long range and high-gain beam-formed electromagnetic attack against aerial signals of interest at long range. The Army also wants to assess operational and technical characteristics (receiver sensitivity, transmitter power) required for a defensive electronic attack (DEA) capability to protect ground assets from adversary threats (SSMs/UAS/RF-Proximity Fuzes) at each echelon and to test the minimum RF engagement range to create an adequate miss angle for RF or PNT guided threats.

The tactical radio focus area will look at several capabilities, including Low Earth Orbit (LEO) / Medium Earth Orbit (MEO) constellations that provide ruggedized, mobile, beyond line of sight (BLOS) communications capabilities with increased bandwidth and low latency. The BAA said, "desired system characteristics include: high throughput with low latency; low EMS signature; spectrum efficiency; and reduced Size, Weight, and Power-Cost (SWaP-C). Ground terminals should be scalable with common components to support users at the tactical edge to division command posts and above." In addition, the Army wants to evaluate resilient network transport capabilities, such as advanced networking waveforms and dynamic spectrum access, that enable soldiers to access reliable information in contested and congested environments.

Lastly, this area will look at solutions that converge capabilities using a standards-based solution, such as CMOSS and CMOSS Mounted Form Factor (CMFF).

The cyberspace focus area concentrates on enabling Offensive Cyber Operations (OCO) expeditionary forces to support Multi-Domain Operations, including “exploiting technologies,” predictive analysis and machine learning. A related area addresses Cyber (CEMA) situational awareness that allows tactical commanders to ingest, correlate, analyze and display relevant cyberspace data into useful, actionable warfighter information. This includes: integration of cyberspace threat intelligence data sources; integration of EW data sources; displaying Blue Order of Battle (e.g. EW forces, CPTs, etc.); integration Gray Space data sources; and displaying lower and upper Tactical Internet (TI) infrastructure (i.e., network topology with geolocation).

CyberQuest will drive requirements definition, inform rapid acquisition initiatives and support acquisition risk reduction activities in support of the Army’s goal to be MDO capable by 2028. – JED Staff