



### Cyber Quest Focus Areas

Below are the experimentation Focus Areas for CQ23. Each objective has been produced by a capability sponsor and aligned with a required capability which will ultimately yield materiel solutions to the Warfighter.

#### Networks and Services

Focus Area Title	Focus Area Description
Transport Agnostic / Software Defined / Intent Based Network	<b>Intent-based networking (IBN)</b> is an emerging technology concept that aims to apply a deeper level of intelligence and intended state to replace the manual processes of configuring networks and reacting to network issues. Instead, network administrators define an outcome or business objective—the intent—and the network’s software figures out how to achieve that goal. As the Army builds the Unified Network, Intent-based networking (IBN) systems are needed to automate time-consuming tasks and provide real-time visibility into a network’s activity to validate a given intent, they also predict potential deviations to that intent, and prescribe the action required to ensure that intent. This greater intelligence makes the network faster and more agile and reduces errors.
	<b>Transport Agnostic / Software Defined WAN:</b> The Army is moving their network infrastructure and applications to a Unified Network, grounded in a transport agnostic, data-centric, Zero Trust enabled hybrid-cloud architecture. This trend, combined with the rapid growth in multitenant Local Area Networks (LAN), media-rich applications, and networked devices, is placing increasing demands on Wide Area Network (WAN) service delivery. Applications—both in the cloud and on premises—need predictable and fast performance. We must evolve to handle this activity efficiently across cloud, data center, hub, branch, and remotely deployed sites.  The WAN must shift from playing a supporting role in the network to being a leader and provider of innovation. The Unified Network WAN must find a balance between providing customers dynamic access while achieving the agility it needs to respond to changing War Fighter demands. In addition, the Unified Network must deliver: <ul style="list-style-type: none"><li>• Transport Agnostic: A consistent WAN that can be built on any type of transport. Transports can be considered networks with similar attributes, such as performance, geographic paths, or security postures (SATCOM / 5G / LOS / ISP / TROPO).</li><li>• Zero Trust Enabled: All components mutually authenticate each other, and all of the edge devices are authorized before they are allowed onto the network. Every packet that flows through the network across data plane, control plane, and management plane is encrypted.</li><li>• Reliable application performance and availability: Mission-critical applications require predictable performance, and these applications must meet Service-Level Agreements (SLAs) even in Denied, Disrupted, Intermittent and Limited (DDIL) environments.</li><li>• Optimized cloud access: An agile solution to onboard public cloud access on Amazon Web Services (AWS) and Microsoft Azure Gov and public offerings.</li></ul>



### Tactical Radio

Focus Area Title	Focus Area Description
<b>Converged Modular Form Factor (CMFF)</b>	<p>The Army wants to leverage a CMFF architecture utilizing various “card slot” solutions that provide:</p> <ul style="list-style-type: none"><li>• MUOS, HF, SINCGARS, and other tactical voice and data networks for mounted and dismounted forces.</li><li>• Crypto Sub-systems for protected CUI or encrypted SECRET level tactical voice and data networks for mounted and dismounted forces.</li><li>• Protected Coalition and Mission Partner Environment (MPE) interoperability supporting tactical voice and data networks for mounted and dismounted forces.</li></ul> <p>Terminals should be scalable, using common components and flexible configurations that support users to the tactical edge, including Dismounted CMFF utilized to streamline dismounted devices and enhance interoperability</p>
<b>Tactical Position and Navigation</b>	<p>Future Warfighters will increase their awareness on the battlefield by leveraging network solutions to share, distribute and improve trust in assured Position Navigation and Timing (PNT) capabilities such as Dismounted Assured PNT System (DAPS) and Mounted Assured PNT System (MAPS).</p>
<b>SATCOM and BLOS Communications LEO/MEO</b>	<p>Beyond Line of Sight (BLOS) technologies that utilize Low Earth Orbit (LEO) / Medium Earth Orbit (MEO) SATCOM must be able to transport mission command system data and sensor data around the battlefield for the Warfighter. Future Army BLOS capabilities need to have the following characteristics:</p> <ul style="list-style-type: none"><li>• Ruggedized and mobile with low Size Weight and Power-Cost.</li><li>• Increased bandwidth, high throughput, low latency, low EMS signature and high spectral efficiency.</li><li>• Support mounted, dismounted and C4ISR/EW Modular Open Suite of Standards (CMOSS) compliant capabilities allowing integration onto various combat platforms, including aviation and command posts.</li></ul>



### Cyberspace Operations

Focus Area Title	Focus Area Description
<b>DCO - Cyberspace Incident Response Actions Automation.</b>	The Army wants emerging cyberspace technologies and procedures that will provide a team of cyberspace defenders (e.g., Cyber Protection Team (CPT), a DISA incident response team, or the local (unit) cybersecurity team) with the ability to plan, coordinate, and synchronize cyberspace incident response actions (e.g., according to defined accuracy and timeframe requirements) in support of defensive cyberspace operations to address a specific use case (e.g., task a team to [secure, protect, defend, survey] a KT-C).

### Electronic Warfare

Focus Area Title	Focus Area Description
<b>Electromagnetic Support</b>	Emerging electromagnetic support (ES) technologies are needed that can: <ul style="list-style-type: none"><li>• Provide the Army enhanced sensing of the electromagnetic environment (EME) at extended ranges.</li><li>• Provide the EW personnel with the ability to sense EMS signals between 2Mhz and 40Ghz, to include frequency hopping technologies, at a range greater than 50km.</li><li>• Provide a man portable system to sense and geolocate EMS signals from HF to EHF, and the ability to create an internally linked geolocation network between systems.</li><li>• Provide a small UAS (group1-2) capable of sensing the EMS that can perform EA missions and transmit data back through the tactical network.</li><li>• Transport ES data through the provided tactical network to EWPMPT.</li></ul>
<b>Electromagnetic Protection</b>	Technologies are needed by the Army that can: <ul style="list-style-type: none"><li>• Display frequency occupancy and use in near real time preferably imported into a mapping and propagation format like Google Earth, RaptorX, and EWPMPT.</li><li>• Automatically identify spectrum interference and EMCON status.</li><li>• Simulate communications infrastructure for EMS emulator/obscuration system between multiple nodes with input from spectrum awareness system in real time.</li></ul>
<b>Electromagnetic Attack</b>	The Army is seeking emerging technologies that can: <ul style="list-style-type: none"><li>• Provide a low cost capability to accurately replicate HF, and Non Communications equipment such as RADAR and JBCP. Desired but not required is the ability to remotely control the system via LPI/LPD wireless means.</li><li>• Deliver distributed and phase coherent electromagnetic attack capabilities reduce the chance of adversary location of the original source, and increase the J/S for maximum effectiveness and range.</li></ul>
<b>Air Launched Effects/Ground Launched Effects</b>	Electromagnetic Warfare capabilities carried by Soldiers, overland robotics, short and long-range unmanned aerial systems with cognitive electromagnetic warfare techniques and remote reprogramming capabilities that: <ul style="list-style-type: none"><li>• Provide information advantage at machine speed to tactical operations center command and control system(s) with limited human in the loop.</li><li>• Can stimulate and counter adversary sensors and/or create false targets.</li></ul>



### Intel - CDID

Focus Area Title	Focus Area Description
<b>Intelligence Support to Sustainment and Protection</b>	An emerging focus of Military Intelligence is to provide dedicated support to sustainment and rear-area force protection operations. The goal of this focus area is to identify automated collection and/or intelligence analysis capabilities that can identify both lethal and non-lethal threats to sustainment (logistic lines from CONUS production to the battlefield) and to force protection (CONUS to the battlefield).
<b>Collection Management Tools</b>	<p>Currently, there is no automated capability for collection managers from brigade to corps level to request mission collection support from Army to Joint and National levels. The goal of this focus area is to identify emerging automated capabilities for collection managers to request mission support up to Joint and National levels with a single entry.</p> <p>Future collection management applications must be able to tip and cue dynamically between intelligence/cyber/EW/information operations and special operations collection systems.</p> <p>Another objective is to identify emerging capabilities that allow the collection manager and commander to easily visualize the disposition and status of collection assets supporting current and future missions.</p>
<b>Open Source Intelligence Management Tools</b>	<p>Open Source Intelligence (OSINT) is an important emerging intelligence discipline. Currently, there is limited availability of tools and applications to allow the intelligence analyst the capability to adequately and accurately filter available data or exploit opportunities presented by IoT devices.</p> <p>The Intelligence Battle Lab is interested in reviewing tools/applications that take advantage of emerging AI/ML technology to filter available OSINT data, allowing the analyst to focus on priority intelligence requirements, and to take advantage of potential intelligence data sources from IoT devices</p>