Our Army's reliance on cyberspace for everything from business operations to Mission Command means our readiness is dependent on tailorable and effective cyberspace capabilities at all echelons.

As a baseline, the Army requires capabilities that

1) **Integrate** into our current and future platforms
2) Provide **automated** capabilities to perform routine tasks
3) Provide **real-time** feedback, information, and intelligence to enable secure operation of our network as a weapons platform and as a critical enabler to daily operations
4) **Enhance** situational understanding of cyberspace and across the information environment and the impacts on other domains.
5) **Prevent** adversary information warfare from impacting our network, systems, and data
6) When prevention fails, **counter** adversary information warfare through dynamic maneuver, engagement, and eradication of the threat
7) **Deny** adversary use of the cyberspace domain and information environment by disrupting, degrading, and/or destroying their ability to conduct full spectrum operations in all environments from strategic to tactical.
8) **Build** and retain a world-class cyberspace force with the knowledge, skills, and abilities to effectively execute individual, collective, and unit tasks

To ensure our capabilities are dynamic and evolve to keep pace with emerging missions and threats, the Army is aggressively challenging conventional processes, mindsets, and delivery methods in order to achieve agility and flexibility for capabilities to enable:

- Cyber Situational Understanding;
- Defensive Cyberspace Operations;
- Offensive Cyberspace Operations;
- Information Operations; and
- Persistent Cyber Training Environment capabilities.