Broader Concept of Combined Arms/Information Warfare

The 21st century concept of combined arms includes complementary effects from actions in and across the space and cyberspace domains. In future conflicts, the Marine Corps will have to fight *for* information and *with* information. We will confront adversaries who seek to disrupt, degrade, or destroy our information capabilities and systems. We will counter them with an information warfare approach integrated with C2, ISR, and precision fires from the MEF to the small-unit level. Our portfolio will include information operations (IO) that encompass the integration of: military information support operations (MISO); military deception (MILDEC); operations security (OPSEC); electronic warfare (EW); physical attack; special technical operations (STO); information assurance (IA); computer network operations (CNO); public affairs (PA); and civil-military operations (CMO). To enhance our ability to conduct information warfare in the future, we must:

- Develop an organizational and employment construct for information warfare efforts to ensure the MAGTF has a cohesive, organic capability to operate equally well across the five domains.
- Provide all MAGTFs with an information warfare capability and generate the capacity to task-organize it in subordinate echelons.
- Integrate a 21st century combined arms approach into our education, training, exercises, and organizations.
- Create enduring, professional organizations that can consistently provide the MAGTF with combined arms effects across all domains.
- Keep pace with ever-changing technologies to succeed on a battlefield where the ability to conduct cyberspace operations is as important as the ability to perform C2, maneuver, or fires.
- Develop tools and methods to identify strengths, weaknesses, threats, and opportunities in the information environment.
- Continue to mature our global cyberspace operations capabilities to include employment of Cyberspace Protection Teams as maneuver elements.
- Develop processes and authorities for releasing information and participating in the social media spaces in order to inform and influence audiences.
- Develop tools and equipment that detect and attack adversary use of the electromagnetic spectrum.
- Understand the relevant information environment in pre-crisis and during expeditionary operations through integrated and continuous monitoring of social media and use of open source intelligence.
- Enhance our ability to identify and oppose adversary narratives through methods for counter-narrative, competing narratives, and reducing voices contributing to those narratives.
- Deliver cyberspace and electronic warfare fires via a wide variety of MAGTF ground and air platforms.
- Create capabilities that deny the enemy access to critical information and associated systems/capabilities, and constrain the effectiveness of adversary decision-making processes.
- Maintain access and control of cyberspace, the electromagnetic spectrum, and space at decisive times and places to achieve MAGTF objectives.