

STUDIES

Victory Over and Across Domains: Training For Tomorrow's Battlefields

January 25, 2019 | Jennifer McArdle

Resources: Future Warfare & Concepts

Today's U.S. military is an information-dependent force, one that is wholly reliant on information communication technology (ICT) for current and future military operations. The adaptation and integration of ICTs into weapons platforms, military systems, and concepts of operation has put the battle for information control at the heart of military affairs. Although the use of ICT exponentially increases the lethality of the U.S. military, the dependence on these technologies is, in many ways, also a vulnerability. U.S. competitors plan to employ a range of cyber and informationized capabilities to undermine the confidentiality, integrity, and availability of U.S. and allied information.

It is impossible to deny an adversary's ability to shape aspects of the information environment, to include spoofing and sabotaging ICT-based warfighting systems. The U.S. military's goal should instead be to sustain military operations in spite of a denied, disrupted, or subverted information environment. This requires a paradigm shift away from information assurance to mission assurance. U.S. warfighters should be trained to fight in and through an increasingly contested and complex battlespace saturated by adversary cyber and information operations. This report engages in a detailed analysis of current and future cyber and informationized training for the non-cyber warfighter. It provides initial recommendations as to how training systems, scenarios, models, and simulations can evolve to better reflect the complexities of a rapidly changing information-rich combat environment.