
Cyber Operations in Strategic Landpower

Army Cyber Operations and Warfighting Functions in Strategic Landpower

MAJ Irvin Oliver, United States Army

★ IRANIAN CYBER ARMY ★

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY



[.com/photos/aziari/4194607094/sizes/o/in/photostream/](https://www.flickr.com/photos/aziari/4194607094/sizes/o/in/photostream/)

**Army Cyber Operations and Warfighting Functions in
Strategic Landpower**

by

MAJ Irvin Oliver

Strategic Context of Cyber Operations

As the world continues to increase its reliance on computer systems and networks, cyberspace only grows in importance. The Army recognizes this and sees a clear link with Strategic Landpower. The human interaction inherent in land operations, and cyberspace makes Strategic Landpower unique. Human interaction in cyberspace influences physical interface, and Strategic Landpower encompasses these interactions.

Historically, the land, sea, and air domains have been the dominant backdrop for military thought and operations. The space domain has also joined this group, but the cyber domain is now a critical portion of the operational environment. Strategic Landpower, the application of land-based military power in the pursuit of national security objectives for a military campaign or operation, demands that the Army is successful in the cyber domain. Today's operational environment is inextricably linked to the cyber domain.

As cyberspace grows more contested and competitive, well-prepared Army operations can successfully support land operations through Army cyber capabilities. With increases in the reliance on information technology future Army operations require effective, unified operations in cyberspace.

Similarly, adversaries increase their use of information technology for offensive operations, to deny information and communications, and influence cyberspace. With the boundary between land and cyber domains becoming irreversibly blurred, Army Cyber enables and protects Strategic Landpower, primarily in Mission Command, Intelligence, and Protection warfighting functions.

Preparation for the Future

Cyberspace continues to grow in importance beyond its current size and scope. Understanding this, the Army's establishment of the Cyber Center of Excellence (CCoE) and Cyber career field brings signal, intelligence, and electronic warfare functions under one collective group for future success. Delineations between these three fields are less clear as technology as intelligence and signal capabilities become more intertwined. While these systems continue to use and exploit the same networks, interdependence is a reality. Integration by the CCoE of signal, intelligence, and electronic warfare functions is a needed migration for the future.

The Army's initial investment of Soldiers in the Cyber career field has come from the signal and intelligence branches of the Army. Eventually though, the Cyber branch will be able to develop Soldiers and leaders in the same way as other Army functions such as combined arms, fire support, or sustainment operations. We can say that the establishment of the Army CCoE and Cyber career field is the first new Army capability developed for Strategic Landpower.

As the Army CCoE and career field mature, so will cyber operations within the Army's warfighting functions and Strategic Landpower. The simultaneous effort allows the institutional Army to support the operational force applying Strategic Landpower at

cyber speed. Parallel approaches like this has been a historical norm, but the speed and imperative of Cyber require such rapid adaptation.

Mission Command

Mission Command requires effective network operations and secured transmission of information and intelligence. Mission Command systems create shared understanding and allow collaboration. Cyber operations organize growing volumes of information available from multiple sources through wide varying inputs. Constructive cyber information sharing ensures unity of effort and commonality of purpose through concise and accurate operations, intelligence and sustainment displays.

As Army forces employ Strategic Landpower, cyber operations become critical to mission command. Cyber operations empower timely decision-making within the art of command and enable the science of control, as reliable, secure and distributive communication systems share vertically and horizontally. The transportation of authority and direction by the commander using cyber systems is today's primary mechanism to deliver mission orders for the execution of Unified Land Operations. The last 13 years of war have been the Army's real-world lab for the integration of cyber-based systems and platforms; video teleconferencing and satellite-based network operations are commonplace today.

Historically, forces attack mission command systems to disrupt enemy operations, and the cyber domain is no different. In fact, the proliferation of technology provides more opportunities for such cyber attacks. As an adversary's use of commercial cyber technologies increase, they will attempt to degrade U.S. technological and doctrinal advantages through such technology. While the Army communication

architecture is vulnerable to attack, cyber operations maintain mission command networks by defending against attacks. Maintaining the integrity of mission command systems against cyber attack by our adversaries is a complex undertaking. As digital systems proliferate, successful attacks on Army systems may prevent exploitation of opportunities arising from decentralized action. This makes the protection of networks and digital architecture an essential requirement for the Army.

Intelligence

Cyber operations enable the Army to collect and analyze information, and produce instantly actionable intelligence. With this high level of competency, Soldiers act more quickly than adversaries can prepare. Army formations can see more clearly with a truer, real-time, common operating picture. Cyber operations improve the intelligence preparation of the operational environment for Strategic Landpower by integrating intelligence, surveillance, and reconnaissance systems with signal and electronic warfare systems. Better situational understanding, information collection, and targeting from streamlined processes and flattened system hierarchies ensure cyberspace dominance.

The cyber domain is a crucial repository for friendly and enemy information. Collection of information, production of intelligence, and timely dissemination will all make use of the cyber domain. Just as important is exploitation. Effective cyber operations require a multi-disciplinary intelligence approach to find and exploit enemy cyber vulnerabilities. Once identified, this allows for effective offensive cyber operations when applying Strategic Landpower.

Protection

As the cyberspace operations increase, so do vulnerabilities. The protection of theater communication and intelligence networks is an essential mission for Army cyber forces. Protection of Army networks and information technology is a clear imperative. Increased leveraging of technology, digital networks, and computer systems prompt cyber operations to strengthen defensive measures to protect networks and systems. Cyber defense requires both constant active and static measures, in which technology determines the balance.

Unique to the cyber domain is that threats are not geographically fixed, nor are threats solely confined to the military. Threats, access points, and their targets may not be strictly military networks. While they originate from a single pinpoint, threats populate across dispersed lines of communication further complicating this set of challenges. Protection, therefore, requires an integrated systems approach under a comprehensive cyber defense structure that includes private-sector participation. Defenses must be in place at all levels and active before threats become obvious. This is an interesting paradigm – to protect before an enemy materializes.

Cyber operations are not dedicated solely to Army Cyber units. All echelons within the Army, and private industry partnered with the Army, are involved to strengthen the overall network and protect digital systems. Additionally, the importance of the digital architecture may weight efforts to prevent exposure of critical vulnerabilities throughout all phases of operations. The technological complexities of cyber defense require the continuous integration of the situation in the cyber domain in commander's updates and forums to ensure the security of systems that touch the domain.

Conclusion

In a world moving at the speed of 1s and 0s, where decision-making moves at the speed of information, and cyberspace occupies a larger portion of the global commons, the Army's ability to build and apply combat power is bound in cyberspace. Generating combat power today is far different from yesterday. Information technology has joined rifles, tanks, and missiles as forms of combat power. With this, cyber's importance has grown exponentially. While employing large formations will be always be a consideration for the Army, the need to adapt to cyber threats and exploit opportunities in cyberspace are requirements for the future. As such, Army cyber is able to take these requirements and convert them opportunities. The Army's seven warfighting functions are wholly reliant of cyber operations. Mission command, intelligence, and protection all rely on effective and secure cyber systems for successful movement and maneuver, fires, sustainment, and engagement.

Cyber operations support the conduct of unified land operations and are yet another form of strategic maneuver and expeditionary warfare. The application of Strategic Landpower is now expanded from the human domain to include cyberspace.

Once professed as futuristic, cyber operations are now the present. The Army's next step is to continue maturing cyber operations across the Army's warfighting functions for unified land operations. Innovation and agility are driving tenets as cyber operations strengthen the application of Strategic Landpower, at the speed of cyber.