



The Cyber Defense Review

[Home](#)

[About CDR](#)

[The Journal](#)

[CDR Content](#)

[ACI](#)

[Home](#) > [CDR Content](#) > [Articles](#) > [Article View](#)

Can the Warfare Concept of Maneuver be Usefully Applied in Cyber Operations?

By [Dr. David Gioe](#) | January 14, 2016

PRINT



Although the cyber domain has several unique characteristics, the timeless principles of maneuver warfare can still be readily applied as in the conventional domains of land, maritime, air, and space.^[1] Maneuver in cyberspace also leverages many of the same techniques, tactics and procedures (TTPs) as the conventional domains, but with some notable difference, herein explored. For the purpose of this article, the intent of maneuver warfare is to ensure the tactical mobility of capable friendly forces and deny it to the adversary in order to place him at a tactical disadvantage. I also stipulate that movement to and within a theater is a given, thereby focusing our analytical effort on cyber maneuver at the tactical within a theater of operations, though crossing domains. Because cyberspace is a man-made domain that is both virtual and physical, the specific TTPs are distinct, yet they can largely exist within established conceptions of maneuver warfare. As cyberspace is physical, logical, and human in nature, it is possible to maneuver to exploit vulnerabilities at each of these levels.

A first principle must be that maneuver across the conventional domains should incorporate cyber operations as interchangeably as any cross-domain coordinated action. Further, consistent with existing Army doctrine, the principles of coordinated and joint maneuver are facilitated by cyber operations, to include across domains. Finally, cyber operations represent an integration element as well as a force-multiplier in joint and combined operations, provided they are properly considered in the initial planning phases, such as the Joint Operational Planning Process (JOPP). If only considered as an afterthought, however, cyber operations will likely be substantially less fruitful yield diminished effects. Subsequent to the planning process, cyber maneuver is an iterative effort and must be continually synchronized with the joint force and other related elements both during the planning process and execution phase.

There are many more similarities than differences and the majority of maneuver principles in the physical realm have surprisingly close virtual analogs. The concept of key terrain is a crucial one for any study of maneuver principles. In land warfare, identifying, seizing and holding key terrain is of critical importance. This remains true in the cyber realm, but with some notable caveats. First, cyber operations can help commanders actually change some of the virtual key terrain itself. Secondly, unlike land warfare, cyber operations can be present on key terrain (and perhaps hold it) without the enemy identifying this presence, or understanding its hold over the key terrain. In this sense, the maneuver principle of observation can be both closer and concealed in the virtual realm. Further, maneuver is often considered as the opposite side of the warfare spectrum from attrition. In the Cyber domain, attrition might be considered as persistent DDoS attacks or similar “mass-centric” approaches. For instance, saturating a particular target with field artillery or requests for data or service (DDoS) yields a similar result when the target becomes ineffective at performing its key function (mission incapable). While brute-force attrition has a record of success in the cyber domain, arguably maneuver is a more sophisticated and efficient use of use of resources.

Executing cyber maneuver involves positioning (likely re-positioning) forces or assets to exploit the enemy’s weakness or vulnerability. This requires several steps: First, understanding how and where enemy is vulnerable. This can be accomplished through previous intelligence collection, or by going through a testing process (probing networks and connections) and evaluating responses. This step might be called Intelligence Preparation in the Cyber Domain (IPCD). Notably, ISR as a pre-requisite for tactical maneuver is also distinctive in cyber operations because the coordination process and domain are shared with other intelligence agencies. Second, initiation of maneuver requires the strength and capacity to execute so that vulnerability may be exploited with follow on operations. This requires the speed and agility to position and reposition forces within the limited time the identified vulnerability is exploitable. If too much time elapses, the advantage is lost. ^[2] The physical analog may be the maneuver principle in which exploitation of gains is possible after penetration of enemy defenses. Notably, in the cyber realm capital assets can often be replicated and repaired faster than capital assets in traditional warfare, as well as dispersed for force protection considerations. Third, in order to be able to move faster than the enemy, command and control (C2) must be properly functioning and, of course, redundant. Fourth, there is a counter-intelligence function: keeping friendly vulnerabilities and limitations hidden from the enemy. Finally, cyber deception (as distinct from security as well as intelligence collection) has a role to play in masking movement that is either “on network” or physical.^[3]

Maneuver principles also assume a larger strategy at work, with a pre-identified end state. Cyber maneuver also requires identification of its role in the desired outcome. For instance, in traditional conflict, success might be defined as killing or capturing an enemy and/or impeding its will or ability to fight. However, in cyber operations it may be best to consider a spectrum of degradation instead of kill / capture / hold terrain. A cyber maneuver may involve degrading enemy network operations, plans, C2, (lines of communication, or similar) which would retard the enemy’s operational tempo, which, in turn, retards initiative. Once the opponent loses the initiative, other forms of warfare can exploit the reversal of fortune. In this way cyber operations can be understood as more than its own form of maneuver, but as an integrated piece of the combined effort.^[4] Thus, maneuver in cyberspace, while possible in a vacuum, should principally be understood as both a force multiplier for joint warfare, as well as an integration element in as much as the virtual and physical domains consistently intersect with each other.

Although this article seeks to emphasize that cyber maneuver has similar characteristics to land maneuver, it is useful to highlight the following important distinctions: expect that land warfare maneuver, with certain emergency contingencies, will not take place on sovereign US territory. In contrast, cyber maneuver is likely to be initiated in the United States if led by a national level organization. However, it will more than likely take place on commercial assets that will not be wholly owned or controlled by the US government or US-based corporations. Additionally, because the US military controls the overwhelming majority of kinetic functions, coordination

and synchronization on the battlefield can be accomplished only partially by the JOPP process. Thus, when a land warfare commander seeks to maneuver land-based forces, it is understood he controls all military elements in the operational area. However, in the case of cyber operations, deconfliction must also include consideration of other federal agencies and departments. This is a unique characteristic of maneuver in cyber operations and thus, the JOPP process, while necessary, is insufficient for cyber maneuver coordination. Finally, the diffused nature of the internet and DoD networks means that it is highly likely that cyber maneuver will span multiple geographic combatant commanders Areas of Responsibility (AORs). This is simply due to the physicality of networked cables and lines, most cyberspace operations are trans-regional, even if their intended effects are localized. As with UAVs, although the operators may be geographically removed, they must be as closely looped into the planning process as if they were physically proximate.

Cyber operations can have outsized effects on the battlespace when employed effectively with other DoD assets. For instance, cyber operations can pre-empt an enemy's command and control nodes, can supplement intelligence collection, and can disrupt an opponent's strategy by wreaking havoc in an enemy's decision-making centers. In isolation, there are acceptable outcomes depending on the desired end state, but in coordination with land maneuver, cyber operations yield synergistic results.

As with any type of warfare, considerations of the capabilities that cyber operations offer as well as an appreciation of its distinctions and limitations is key for maximizing maneuver in the cyber domain. The more cyber operations are seen by commanders as artificially distinct from the other conventional domains, the more likely this is to be the case, and with a corresponding degradation in synergistic real-world effects. Consideration of the basic principles of maneuver warfare should be part of every movement and strategy at every level of level of warfare. The challenge — like operating in other domains — is integration, cooperation (including OPCON, TACON, identifying supported and supporting commanders) and unity of effort. Application to the cyber domain requires each supporting and supported commander to consider their cyber limitations as well as how their opponent may present exploitable cyber vulnerabilities. Thus, military commanders should consider maneuver in cyberspace as an element of combat power to seize and exploit the initiative. With the creation of U.S. Cyber Command and the various service cyber commands, cyber operations are on the precipice of changing our understanding of cross-domain warfare. Although increasingly recognized as an essential tool in the commander's arsenal, deliberate consideration of cyber maneuver in the initial planning process remains a core task. Without a solid grasp of what cyber maneuver can (and can't) do for the battlespace commander, cyber operations will be limited not by resources or technical limitations, but by the imagination of those who wield it. The author extends his appreciation to Dr. Aaron Brantly for his invaluable advice over many drafts.

Endnotes

[1] For the purposes of this discussion I am using the Department of Defense Joint Publication 3-0 definition of Maneuver found on pages 27-28: The movement and maneuver function encompasses a number of tasks including:

(1) Deploy, shift, regroup, or move joint and/or component force formations within the operational area by any means or mode (i.e., air, land, or sea). (2) Maneuver joint forces to achieve a position of advantage over an enemy. (3) Provide mobility for joint forces to facilitate their movement and maneuver without delays caused by terrain or obstacles. (4) Delay, channel, or stop movement and maneuver by enemy formations. This includes operations that employ obstacles (i.e., countermobility), enforce sanctions and embargoes, and conduct blockades. (5) Control significant areas in the operational area whose possession or control provides either side an operational advantage.

[2] For historical context, the use of cavalry may be instructive. Napoleon was able to use speed in order to disrupt his enemy — attacking or flanking them before they were “ready” or “set” for battle. In this way, he used speed in synergistic ways.

[3] For instance, ostensible interest could be shown by attempted network infiltration of a certain enemy command and control system, where in fact other systems are actually higher collection and targeting priorities. Allied deception campaigns in World War II, particularly Operation Bodyguard — the grand deception operation in the lead up to D-Day — reveal how effective deception can be in forcing the enemy off guard and thus liable to misplace or misdirect key assets.

[4] Such as the mutually supporting tactical maneuver of Infantry and Armor units in breakout from Normandy in June 1944.

 PRINT



US Army Comments Policy 

0 comments Sort by

Add a comment...

 Facebook Comments Plugin

Help & Support

Contact Us
U.S. Army FAQs

Resources

Army A-Z
USA.gov

Legal

Accessibility
FOIA
No FEAR Act

Other Army Sites

Army
Army Knowledge Online
Army National Guard

Other DOD Sites

Department of Defense
Forces Command
Installation Management Cmd

[Terms of Use](#)

[Army Reserve](#)
[Go Army](#)

[iSALUTE](#)
[Ready Army](#)
[Ready and Resilient](#)

Hosted by Defense Media Activity - WEB.mil

