



# SMALL WARS

---

## JOURNAL

## Strategic Cyber Maneuver

By *Aaron F. Brantly*

Journal Article | Oct 17 2015 - 2:35pm

### Strategic Cyber Maneuver

Aaron F. Brantly

Maneuver warfare is an integral part of the strategy, tactics and operations of the United States military, but what does it mean to maneuver in cyberspace?

Maneuvering with an army is advantageous; with an undisciplined multitude, most dangerous.

– Sun Tzu, *The Art of War*

Maneuver warfare dates back millennia and yet the fundamental goal of maneuver, to provide military advantage in tactical situations, has not changed. There are concrete and identifiable military tactics associated with maneuver each refined through conflict and war and each tailored to the needs of the situation faced by commanders on the frontline. The modern era has seen joint forces maneuvers in which Air, Land, Sea work in tandem to accomplish a mission. The state of maneuver warfare changes as weapons and technology evolve. No longer is it reasonable to maneuver in column in two opposing battle lines as in the Napoleonic Wars, modern weapons have changed the concepts of maneuver and made them increasingly more complex, nuanced and challenging. Five years after the establishment of U.S. Cyber Command the United States is confronted with yet another advance in technology that requires a re-evaluation of the concepts of maneuver in a cyberized<sup>[1]</sup> world with smart bombs, laser guided field munitions, blue force trackers, digital logistic networks, and network command and control centers. The department of defense has a new domain that must be examined, poked and prodded to ascertain the means and mechanisms to achieve advantage. This paper examines the concept of maneuver within cyberspace and attempts to develop an initial framework for maneuver operations to achieve both within and cross-domain effects.

Land, sea, air, space and cyberspace all have similar identifiable characteristics of maneuver.<sup>[2]</sup> Conceptually maneuver in cyberspace leverages many of the same techniques, tactics and procedures (TTPs) as more the conventional domains, however, because it comprises multiple layers of interaction, actions can occur on multiple levels simultaneously to achieve a unified effect. Cyberspace encompasses three primary layers comprised of a physical network layer, the logical network and the cyber-persona layer.<sup>[3]</sup> Each layer has specific attributes, which can be manipulated in different ways to achieve a successful maneuver. All efforts across the layers within the operational environment of the domain are intended to facilitate one or more of primary functions of maneuver including envelopment, turning movements, frontal attacks, penetrations, and infiltrations. These maneuvers can constitute within domain

(i.e. virtual) offensive cyber operations (OCO), defensive cyber operations (DCO), and DOD Information Global Network Operations (DODIN Ops) or cross-domain (i.e. virtual and physical) actions to create standalone physical effects or physical effects in support of non-virtual military elements.[4]

This paper does not consider the nuances of joint planning for cyber operations or the processes by which legal considerations are assessed for any given maneuver. Instead, this paper highlights potential attributes of maneuver in cyberspace both for OCO and DCO to accomplish the stated goals of a commander for virtual and virtual-physical operations. Lastly, both real and hypothetical examples are embedded throughout the analysis to illustrate various types of maneuver within conventional and virtual conflict.

Understanding the role of cyber operations within broader maneuver warfare helps ground in reality the applicability of cyber operations to military commanders and policy-makers alike. The Department of Defense and the policy establishments in Washington are often at a loss to fully articulate where cyberspace operations fit within larger scope of national security. Recent promising thought pieces on cyber support for corps and below (CSCB) provide forward thinking models for the development of embedded cyber units that supports a dynamic and holistic approach to maneuver within cyberspace.[5] By focusing directly on the use of cyber operations as a form of maneuver warfare for both offensive and defensive actions this paper provides an initial starting point for more robust discussions on cyber as a military activity. Furthermore, it provides an accessible vehicle for policy-makers and commanders to begin to assess the importance of cyber operations related to their own roles and responsibilities.

### **What is Maneuver Warfare?**

Maneuver warfare, contrasted with attrition warfare, is predicated on speed, agility, capability, and intelligence to enable war-fighting operations to occur from a position of advantage relative to an adversary. Each service has a slightly different definition of maneuver warfare, yet they all must be compatible with joint concepts of maneuver. Joint Publication 3-0 defines Maneuver as:

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.[6]

The use of joint terminology is important because most non-USCYBERCOM military operations are controlled and managed by a Combatant Commander (COCOM) who directs all services within his or her geographic area. A joint concept of maneuver is applicable because the distribution of units by service can differ between COCOMs. The COCOMs serve as plug and play commands based on situational need, with some obvious areas of specialization. Yet, the associated training of cyber mission teams, the relative skill and capabilities of teams from each of the services should be approximately equivalent. Because each of these teams has a base set of skills they should have generally similar maneuver capabilities which can then be applied to the specific needs of the COCOM.

Within the broad set of cyber teams there are teams that specialize in different forms of maneuver. While most of these teams do not presently refer to their activities as maneuver warfare, they are analogous.

Erick Waage offers the best forward thinking representation of a potential composition of a corps or below cyber team.<sup>[7]</sup> This paper differs from defining the hypothetical composition of teams within current military structures and instead poses broad concepts of maneuver in terms of OCO and DCO operations.

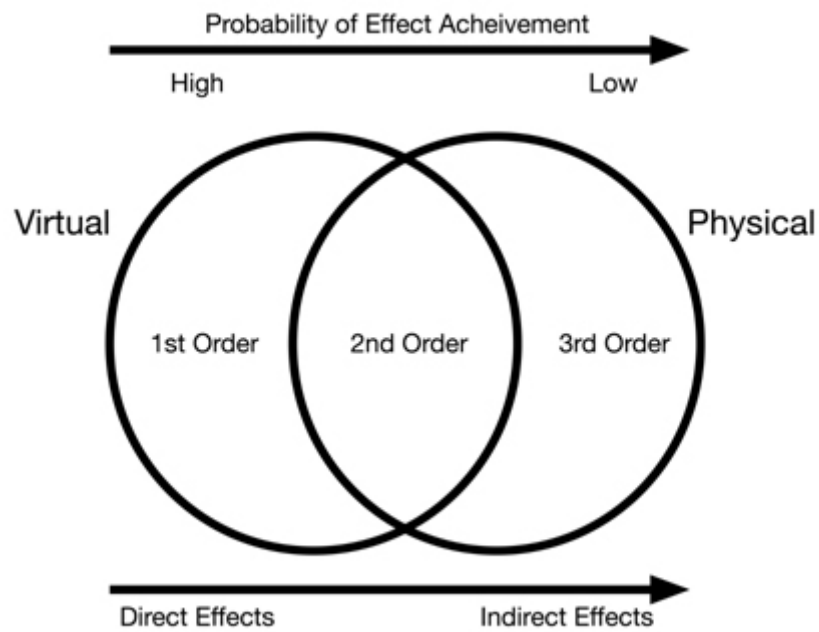
Broadly, there are several typologies of maneuver warfare associated with joint operations. These typologies differ significantly from traditional maneuver activities in that they can often occur in the form of regular, non-war situations. At the highest level is the concept of within domain (within cyberspace) offensive and defensive operations. Offensive operations can occur both within one's own networks and within the networks of an adversary. Likewise, defensive - virtual operations - can also occur within one's own networks or within the networks of an adversary or a third party. In theory something as simple as patching hardware and software vulnerabilities could be constitutive of a defensive maneuver, alternatively tracking, isolating or positioning an adversary into a specified network location to reveal TTPs might also be constitutive of a DCO.

The next generalized type of cyber operations are virtual-physical cyber operations. These types of operations are typically intended to result in physical world effects although they can also occur in the reverse direction with physical maneuvers designed to achieve virtual effects. An example of a physical to virtual effect would be in line with the 2014 sniper attacks against power substations in California.<sup>[8]</sup> These attacks while entirely physical could have achieved virtual world effects.

Both physical-virtual of operations can be both offensive and defensive are possible. Unlike in conventional warfare where effects are almost always direct, the effects achieved through the cyber domain are likely to be what Herb Lin refers to as "indirect effects."<sup>[9]</sup> Within this typology are two broad branches of activities. The first type of operation seeks to achieve standalone effects, while the second facilitates effects across operational units also known as enabling effects. Enabling effects can also serve the role of "Fires", a military term meant to denote the support of an operation from a non-proximate element (i.e. artillery). An example of a stand alone indirect effect would be Stuxnet's manipulations PLCs controlling centrifuges in Iran's Natanz nuclear facilities resulting in the degradation of the Uranium Enrichment process. The corruption of GPS targeting systems in an adversary's counter artillery radar would serve as an enabling indirect effect for the advancement of infantry as well as the protection of friendly artillery units.

It should be noted that here that the use of cyber for for the sole purpose of intelligence as constitutive of maneuver is not included. Instead, intelligence maneuvering in cyberspace can facilitate or lay the foundation for both cyber operations designed to generate effects or facilitate the effects of other non-cyber units. Cyber exploitation (CE) falls more directly within intelligence, surveillance and reconnaissance models than within traditional maneuver warfare. This does not undermine the value that CE can provide to Cyber and non-cyber forms of maneuver.

Figure 1 illustrates the relationship of virtual and physical effects in the context of cyber maneuver. The figure does not illustrate the reverse relationship of physical to virtual effects, but rather focuses on the achievement of effects originating in cyberspace and either remaining virtual or creating a virtual to physical effect. It should be of note that as the relationship between the originating action and the effect increase in distance and complexity from virtual to physical the probability of effect achievement decreases and the causal relationship cyber action and physical effect becomes increasingly difficult to accurately measure.



**Figure 1: Cyber maneuvers and the relationship to effects.**

Cyber maneuver warfare is contrasted with cyber attrition warfare, which is constitutive of operations such as Distributed Denial of Service (DDoS)[10] or similar "mass-centric" approaches. Attrition warfare constitutes frontal operations by two opposing forces each attempting to degrade the opposing forces capabilities until one side is unable to continue due to a lack of capability. Although brute-force attrition has a record of success in the Cyber domain, the virtual nature of the domain makes attrition warfare an inefficient allocation of resources and unlikely to achieve sustained effects on agile targets. Cyber maneuver warfare is by contrast a more efficient use of use of resources capable of achieving sustained and relevant effects. Attrition aspects of cyber warfare could be used as enabling functions of cyber maneuver warfare in some instances.

### **Hypothetical Attributes of Maneuver in Cyberspace Explained**

Leveraging mission essential task capabilities and intelligence and analysis conducted prior to a mission, what are the core attributes of a maneuver operation for cyberspace operations?

Maneuver operations in the cyber domain have six primary attributes. The first attribute of maneuver is the deception of the enemy as to the location of massed or massing forces both within cyberspace and in the physical world. The second and third are the identification of vulnerabilities for exploitation and defense leveraging prior traditional intelligence, surveillance, and reconnaissance (ISR) as well as CE. The fourth is the movement of sufficient forces into position to engage those adversary vulnerabilities and defend one's own vulnerabilities in response to an adversaries preemptive or retaliatory strike. These forces can be remote, i.e. back at Fort Meade, or proximate, within embedded within the units on the ground or anywhere in between. Fifth, forces must execute mission objectives through the engagement of vulnerabilities to achieve desired effect. Sixth, during the execution of a given mission, the preparation of units to defend and hold or relinquish acquired terrain in accordance with mission objectives becomes necessary. Combined these attributes constitute a rough framework for conceptualizing maneuver across the typologies of maneuver identified in the previous section.

Executing maneuvers in the cyber domain involves positioning and likely re-positioning forces or assets to exploit the enemy's weaknesses or vulnerabilities through the cyber maneuver framework. The framework as indicated above begins with deception. Deception (as distinct from security as well as intelligence collection) helps to obfuscate the intentions of OCO and DCO maneuvers and increase the probability of success. By confusing adversary offensive and defensive cyber as well as physical units as to the intent of a given operation, space and time constraints can be eased and afford units "breathing room" to accomplish stated mission objectives. The absence of deception in the planning and implementation of maneuver operations is likely to expose operational units in both cyberspace and in physical domains to undo risk.

Second, a thorough understanding of the operational environment (OE) is vital to engaging in successful maneuver operations. JP 3-12 establishes the operational environment as "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."<sup>[11]</sup> A robust understanding of the OE for maneuver operations is facilitated by intelligence collection on the cyber environment of the adversary (ICE-A) facilitates vulnerability and weakness identification across physical network, logical network and the cyber-persona layers. ICE-A is best achieved through a process of mapping out, testing and evaluating adversary responses. The objective of ICE-A is to identify the attributes and limitations of an adversary's ability to observe, orient, decide and act loop (OODA-loop), pre-positioned insiders, open source intelligence (OSINT), signals intelligence (SIGINT), and forensic analysis of previous adversary engagements combined with and other relevant forms of intelligence to improve the probability for success of a given cyber maneuver. ICE-A requires advance collection on the use and attributes of the physical, logical, and persona layers as employed by the adversary. Insufficient ICE-A prior to maneuver operations reduces the probability of mission success.

In conjunction with ICE-A preparations for counter attack/intelligence should be undertaken. Sufficient intelligence on the cyber environment for defense (ICE-D) is of critical importance to the maintenance of terrain gained during a given maneuver in cyberspace. Just as physical units must be able to defend acquired positions after successful maneuver operations, cyber units must be able to defend or safely relinquish terrain within the virtual world. ICE-D facilitates DODIN Ops, DCO-Internal Defensive Measures (DCO-IDM) and DCO-Response Actions (DCO-RA). Successful ICE-D also establishes a firm baseline for potential future operations by ensuring against potential existing vulnerabilities.

During mission execution the cyber teams must leverage established deception, intelligence and movement capabilities to execute a mission and engage a target or targets. Mission execution for the creation of effects might rely on pre-established "Fires" to facilitate deception, access within virtual or physical environments. Fires could be within domain fires within or on a different layer of cyberspace, they could be the result of attrition based cyber methods such as DDoS, or they could be the result of physical attacks against the physical infrastructure of the network. Here fires serve as a supporting actions of a given maneuver.

Cyber teams must also subsequently adapt to changes in the target's environment and behavior until the desired effect has been achieved. Changes in target behavior can be the result of inadvertent cyber environment changes, deliberate attempts by an adversary to defend its network or potentially a combination of the two in response to unknown attacks. OCO and DCO maneuvers require the movement of sufficient, capable and agile forces with speed and agility to execute a given mission. Whereas conventional targets can place one munition on one target, a Linux cyber weapon system (think cyber munition) will be ineffective against a Windows environment. This example is overly broad as within the Linux and Windows ecosystems are numerous variations of both the base operating systems and their subsequent configurations. The point is that in training warfighter for infantry and other positions the

military can be relatively broad in its soldier preparation. While there are specific skill sets, these can be generalized across large populations. Within the cyber domain, to accomplish specific missions, these skill sets are likely to be quite narrow.

Due to the narrowness and tailored nature of each munition to each operation, the successful execution of a mission requires substantial analytical and technical skills, both to assess the target and to develop specific weapon systems capable of achieving effect or have on hand the personnel capable of exploiting weaknesses across the layers of cyberspace. Analysis and technical tool use/development must occur quickly as the environment is constantly changing and vulnerabilities and weaknesses are time sensitive. Efficient movement is predicated on an organized command and control (C2) structure with the prerequisite authorities to act and adequate operational planning to achieve a mission. When executing an OCO or DCO maneuver the cyber teams and conventional units in the case of virtual-physical effects driven operations must have sufficiently prepared for all reasonable outcomes including counter attack and counterintelligence operations.

### **Virtual Offensive Cyber Operations Maneuvers**

OCO can include multiple types of attack to include movement to contact, attack, exploitation, and pursuit. Within attack it is possible to engage in various subsets of operations to include ambush, spoiling attacks, counter attacks, raids, feints and demonstrations. Focusing on these typologies of attacks within the cyber maneuver framework below is a hypothetical case example for the offensive maneuver in cyberspace leveraging the forms of maneuver into the types of offensive operations.

A commander who wants manipulate the key terrain of the layers in cyberspace to position an adversary to engage in DCO activities from a point of weakness might also work with coordinating units to establish a dominant multi-layer maneuver capability within corresponding physical, logical and persona layers of of the target systems or networks. Successful OCO necessarily includes offensive actions against key nodes in networks (Choke Points), logical vulnerabilities in software and firmware of the logical environment (Zero-Day Exploits or Security Weaknesses), or direct manipulation by inside actors with sufficient access to achieve desired effects.

Recognizing the need to gain cyber dominance over an adversary at a strategic choke point on their network infrastructure, mission forces can leverage the persona layer of the network to induce a specific target to attack a honeypot.<sup>6</sup>[12] This inducement, with sufficient incentive, could force the enemy to position its forces forward revealing Techniques, Tactics, and Procedures (TTPs) thereby providing the time and opportunity to envelop and exploit the flanks (the logical and physical layers). Similarly, a maneuver to deliver a concealed cyber weapon package through a honeypot to exploit what is best thought of as an offensive mitigation of threat through deception. The attacker steals a 'desired' file with an embedded cyber weapon package and delivers this package back to their cyber environment unknowingly. Upon opening the document the weapon package is initiated resulting in self-induced damage. Such a maneuver could exploit all three layers of cyberspace and create a significant deterrent.

Both these tactics have been employed previously. The first maneuver is akin to a classic pincer movement dating back to 490 B.C.E. and the Battle of Marathon.[13] The second maneuver is similar to a tactic employed by Russian soldiers in World War II. Russians strapped improvised explosive devices to specially trained "tank-dogs" who were kept hungry and taught to lie beneath tanks.[14] These dogs were then sent them towards German lines. German soldiers welcomed the dogs into their camps at which time the improvised explosive detonated killing or maiming individuals or damaging tanks/armor within range of the blast.

Many common street scam strategies are applicable OCO as well. While one attacker loudly makes his or



her way through a network or system drawing in attention, another uses the diversion to essentially steal access to the target, akin to a pick-pocket gang working in teams. Done properly across multiple systems and networks, the defending parties become uncertain as to which is the true target of attack providing them with the challenge of defending multiple perceived “best shots” against many “weakest links”.[15]

### **Virtual Defensive Cyber Operations Maneuvers**

The volume of attacks against U.S. systems also establishes the need to maneuver against adversaries who are attempting to penetrate or who have already penetrated such systems. While it is often thought of as within network defense, the reality of defensive operations is far different. Proactive DCO differs from OCO in its intent to mitigate threats prior to their intrusion into U.S. Systems as well as once those systems have been penetrated. Malware is distributed through a variety of different vectors and access is likewise gained through a variety of different avenues for exploitation. At their most basic penetration occurs through either point-source or point-source-progressive infections or manipulations.[16] Point source would be contraction of a virus from a compromised website, where the website is the source of the infective agent. Whereas a point-source-progressive might be a worm or trojan acquired through a similar point source, website, flash-drive, email etc, but that also contains the ability to replicate and spread itself between systems within a networked environment. Moreover, both types of infections can lead to autonomous, i.e. pre-structured or delineated actions, guided, continuously manipulated actions, or some combination therein. A typical key logger will log and exfiltrate the results of its query via established coding parameters, whereas a worm or trojan that elevates or establishes rogue credentials within a system might provide an adversary a means to manipulate/exploit systems in ways beyond those of its initial infective agent.

The point is that DCO can leverage either the penetrated or the point sources to move an adversary into positions advantageous for the defense not only of the present system being exploited, but also for future engagements as well. Similar situations are common in counter-intelligence operations. One of the more famous counter intelligence operations being the Double Cross (XX) agents run during World War II.[17] By systematically manipulating the intelligence assets of the Nazis within the United Kingdom, MI5 was able to achieve both tactical and strategic advantage. It should be noted however, that although there were great successes, such as operation Fortitude, which facilitated the deception associated with the D-Day landings, there was also a willingness to accept losses such as the managed impacts of V-weapons.

DCO is not all about eliminating adversaries, it is about using the adversaries self-perceived advantages for defensive gains. Successful DCO maneuvers can facilitate enhanced attribution, TTP identification, and provide intelligence on the strategic and tactical objectives of adversaries, it might even provide ICE-A when DCO-RA actions provide access to adversary systems. Cyber maneuvers for virtual defensive cyber operations require creativity, and the ability to engage in all aspects of maneuver.

### **Virtual-physical Offensive Cyber Operations Maneuvers**

More and more frequently the question that comes before cyber thinkers is how can cyber be used to affect physical environments to enable war fighting missions. There are at least three relevant examples of virtual-physical OCO operations that have each had varying degrees of success. The first is the compromise of Iraqi email servers to send soldiers emails requesting and providing information on how to properly surrender prior to the invasion of Iraq in 2003.[18] The second is the 2007 propriety cyber attack against Russian made Syrian air defense systems that spoof the systems and allowed for unimpeded Israeli air strikes against a suspected nuclear site in the Deir ez-Zor region.[19] The third virtual-physical cyber incident is widely considered to be the use of decentralized cyber mobs to attack specific targets within the Republic of Georgia prior to and during the Russo-Georgian War of 2008.[20] While each has

its own merits, the indirect effect of spoofing Syrian air-defense systems, if accurate, is likely the most applicable most modern militaries. By disrupting ISR and allowing unimpeded access to airspace without traditional Electronic Warfare (EW) operations sets a new precedent in tactical usefulness of cyber weapon systems was established. In the Syrian case in particular the use of EW would have alerted Syrian defense forces of an imminent or ongoing attack, but the spoofing of their systems allow planes to essentially fly undetected through enemy airspace.

While it is difficult to think of ways a cyber weapon could significantly impede the tactical operations of land forces, the potential effects on air and naval forces due to their increased reliance on digital systems for everything from navigation and targeting, to communications and movement make cybered conflict particularly pertinent to these services. After many discussions with both armor and field artillery personnel, the common sentiment remains that while a well executed cyber attack might affect the efficiency of their operations on certain weapon or targeting systems, the function of those systems is likely to remain unaffected. To date no conversations on counter artillery or counter missile systems have been examined. Due to their heavy reliance on digital components and computations it is likely that these would be the areas of traditional land warfare most affected by cross-domain cyber operations, although there is evidence other creative uses of cyber are just on the horizon.[21] Truthfully counter missile platforms such as the patriot system have found themselves vulnerable to digital problems even in the absence of deliberate attack. In 1991 Patriot Missile targeting systems failed due to computational problems caused by coding schema selections.[22]

Speculating on the future it is not inconceivable that U.S. cyber warriors could conduct offensive cyber operations in advance of conventional ground forces to hide a massed formation entering a zone of combat until such time as a response would be technically or practically infeasible by a target party. Such activities could involve the spoofing of aerial or satellite reconnaissance in real-time, the manipulation of land, sea, or air radar systems. While the obfuscation of massed forces might be desirable in some situations, the minimization of those forces for the purposes of eliciting an attack might be an objective in another. By portraying limited air power, an adversary might be inclined to overwhelm invading forces with its own airpower only to be greeted by a much larger force.

Similarly, by leveraging local ICT infrastructure land forces could leverage real-time intelligence to track the ingress and egress of enemy combatants into an area of operations. Such a system could provide a heads up display based on network location data through GPS and triangulated cellular networks the position, within approximately 10 feet, of all persons in possession of mobile devices. These devices could help blue forces distinguish between combatants and civilians and help to determine repeat combatants in irregular warfare situations. Providing field commanders with a heads up display illustrating the massing or dispersal of individuals based on readily available location data, provided by existing mobile networks could facilitate more efficient combined arms maneuvers and minimize potential collateral damage. This use of mobile technology to facilitate situational awareness and identify potential hostile parties has been utilized in other countries most notably in mass public disturbances.[23]

Combining a heads up informationalized environment with large-scale data analytics could provide evidence of specific devices being present in multiple potential combatant incidents and therefore enhance targeted intelligence by indicating threat is present. Moreover, sustained penetration of local ICT infrastructures combined with big data analysis and pattern recognition might provide clues to who is and is not resident to an area of operations. Such data could possibly reduce the impact of embedded military units in areas of operations by providing more accurate, timely and efficient targets so as to minimize generalized searches and patrols.

Combined virtual-physical standalone or enabling actions from cyber to conventional military forces are



still in their infancy. As weapon systems advance and become more automated they are likely to increase in vulnerability thus opening up new ways to engage in combined virtual-physical maneuvers. It is not inconceivable that one day in the not too distant future a tank, such as Russia's new T14 Armata might find itself unable to use its manpower saving automated systems as the result of a determined state or sub-state adversary's rigorous work at finding digital vulnerabilities. Particularly as the battlefield becomes increasingly digitized across land, sea, air and space, the ability to step inside of an adversary's OODA loop and selectively pick apart the efficiencies gained through networked warfare could provide the crucial time needed for other non-cyber forces to accomplish their mission.

## **Conclusion**

Maneuver in cyberspace as in conventional domains has historical parallels. The creation of United States Cyber Command and the various service cyber commands has increased the importance of cyber operations for offense, defense and intelligence. Such operations are gaining traction as an essential component in the maintenance of national security. Yet, because cyberspace is a man-made domain that is both virtual and physical the specific TTPs are different. It is reasonable and possible to apply the unique characteristics of cyberspace within established practices for maneuver warfare with a bit of creative out-of-the-box thinking. The above discussion on maneuver in cyberspace necessitates continued study to best understand how to create synergies for stand alone virtual, virtual-physical standalone and virtual-physical support operations. A cyber maneuver framework that includes deception, intelligence (for offense and defense), movement, execution provides many of the realistic concepts already employed by cyber teams for both offensive and defensive cyber maneuvers. As a community from the operators to policy-makers and everyone in between, there is a need for a robust discussion on what cyber is, how it works, and where it should be accurately fits within military operations. These discussions are happening, but the pace of the world is moving quickly. Just this summer the Department of Defense released its revised cyber strategy. In this strategy the Department lays out five strategic goals.

These goals are:

- Build and maintain ready forces and capabilities to conduct cyberspace operations
- Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions
- Be prepared to defend the U.S. Homeland and U.S. vital Interests from disruptive or destructive cyber attacks of significant consequence.
- Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.
- Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Understanding maneuver in the domain facilitates nearly all of these strategies at some level. More importantly it shifts the discussion from abstract and broad goals to specific uses of cyber and examines how cyber can facilitate concrete objectives. The above framework is just a first step and is meant to be in line with broader DoD cyber strategy and serve as a concept piece. The above is a concept for how virtual and virtual-physical maneuvers in cyberspace can and might look as more and more U.S. Cyber Defense infrastructure becomes more active involved. This framework should be expanded upon the further the debate on what constitutes maneuvers in cyberspace and how they can facilitate both within and cross-domain maneuvers.

*Special thanks to Col. Thomas Cook, Maj. Kent Solheim, Maj. James Finocchiaro, Cpt. Seth Loertsche, Cpt. Eric Waage, Cpt. Brent Chapman, Dr. David Gioe and the research support of the Army Cyber Institute.*

*The views expressed are those of the author and do not reflect the official policy or position of West Point, the Department of the Army, the Department of Defense, or the US Government.*

## End Notes

[1] Demchak, Chris. “Cybered Conflict, Cyber Power and Security Resilience as Strategy” in Reveron, Derek S. 2012. *Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World*. Washington: Georgetown university press.

[2] Department of Defense. 2010. “Joint Publication 3-0 Joint Operations.” *Reading*, no. October: 1–34. [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf).

[3] Department of Defense. 2013. *Joint Publication 3-12: Cyberspace Operations*. [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_12R.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf) . p. viii.

[4] For Terms associated with cyberspace operations please see: Department of Defense. 2013. *Joint Publication 3-12: Cyberspace Operations*. [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_12R.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf).

[5] Waage, Erick. 2015. “Phreaker, Maker, Hacker, Ranger: One Vision for Cyber Support to Corps and Below in 2025.” *Small Wars Journal*.

[6] “Joint Publication 3-0 Joint Operations.” pp. 27-28.

[7] Waage. “Phreaker, Maker, Hacker, Ranger”

[8] Memmot, Mark. 2014. “Sniper Attack On Calif. Power Station Raises Terrorism Fears?: The Two-Way?: NPR.” *The Wall Street Journal*. <http://www.npr.org/sections/thetwo-way/2014/02/05/272015606/sniper-attack-on-calif-power-station-raises-terrorism-fears>.

[9] Lin, Herbert. “Operational Considerations in Cyber Attack and Cyber Exploitation” in Reveron, Derek S. 2012. *Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World*. Washington: Georgetown university press.

[10] A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one—and often thousands—of unique IP addresses.

[11] Department of Defense. 2013. *Joint Publication 3-12: Cyberspace Operations*. P. I-4.

[12] A honeypot is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

[13] Marsh, Doug. 2007. “The Battle of Marathon: The Stunning Victory and Its Contribution to the Rise of Athens.” *Studia Antiqua* 5 (2): p. 36.

[14] Zaloga, Steve, and Ron. Volstad. 1989. *The Red Army of the Great Patriotic War, 1941-45*. London; New York: Osprey: p. 43.

[15] Clark, D. J., and K. a. Konrad. 2007. "Asymmetric Conflict: Weakest Link against Best Shot." *Journal of Conflict Resolution* 51 (3): 457–69.

[16] Citation Brantly *Journal of Intelligence and National Security*

[17] Macintyre, Ben. 2012. *Double Cross?: The True Story of the D-Day Spies*. New York: Crown.

[18] Weinraub, Bernard. 2003. "Threats and Responses - Articles of Capitulation - Iraqis Told, 'Sign Here' To Surrender -- As Lee Did." *New York Times*.  
<http://www.nytimes.com/2003/03/20/world/threats-responses-articles-capitulation-iraqis-told-sign-here-surrender-lee-did.html>.

[19] Clarke, Richard A, and Robert K Knake. 2010. *Cyber War?: The next Threat to National Security and What to Do about It*. New York: Ecco.

[20] Hollis, David. 2011. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, no. August 2008. <http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>

[21] Waage. "Phreaker, Maker, Hacker, Ranger"

[22] Wong, W. Eric, Vidroha Debroy, Adithya Surampudi, Hyeonjeong Kim, and Michael F. Siok. 2010. "Recent Catastrophic Accidents: Investigating How Software Was Responsible." *SSIRI 2010 - 4th IEEE International Conference on Secure Software Integration and Reliability Improvement*, p. 15.

[23] Brantly, Aaron. 2014. "You Were Identified as a Participant in a Mass Disturbance." *NDI Tech Blog*. <https://www.nditech.org/blog/2014/01/you-were-identified-participant-mass-disturbance>.

## About the Author



### Aaron F. Brantly

Aaron F. Brantly, Ph.D. is Assistant Professor of International Relations and Cyber in the Department of Social Sciences, Cyber Policy Fellow, Army Cyber Institute and Cyber Fellow, Combating Terrorism Center at the United States Military Academy.

Available online at : <http://smallwarsjournal.com/jrnl/art/strategic-cyber-maneuver>

Links:

- {1} <http://smallwarsjournal.com/author/aaron-f-brantly>
- {2} [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf)
- {3} [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_12R.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf)
- {4} <http://www.npr.org/sections/thetwo-way/2014/02/05/272015606/sniper-attack-on-calif-power-station-raises-terrorism-fears>
- {5} <http://www.nytimes.com/2003/03/20/world/threats-responses-articles-capitulation-iraqis-told-sign-here-surrender-lee-did.html>
- {6} <http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>
- {7} <https://www.nditech.org/blog/2014/01/you-were-identified-participant-mass-disturbance>

Copyright © 2016, Small Wars Foundation.



Select uses allowed by Creative Commons BY-NC-SA 3.0 license per our [Terms of Use](#).  
Please help us support the [Small Wars Community](#).