

# Cyber Maneuver and Schemes of Maneuver

*Preliminary  
Concepts, Definitions,  
and Examples*

---

Dr. Patrick D. Allen

## **ABSTRACT**

**T**his article is intended to stimulate discussion among cyber warriors and others about an approach to cyber maneuvers at the operational level. Cyberspace is one domain in what is commonly called “Multi-Domain Operations,” while movement and maneuver is one of the warfighting functions in U.S. Army doctrine. This sets the context for a proposed approach to a concept for offensive and defensive cyber maneuver operations that starts with a goal or mission, and allows preparation of the commander’s intent via a scheme of maneuver. The scheme of maneuver includes a sequence of *categories of maneuver*, which in turn are accomplished by specific cyber (or non-cyber) maneuver actions or fires, thereby connecting the mission to the scheme and categories of maneuver, and then to specific actions and fires. Effectiveness of specific cyber actions and fires will change over time, but the categories of maneuver and their intent are much more enduring. Commanders using this approach do not need to be “techies” to define a cyber scheme of maneuver. So long as the commander has, or has been provided, sufficient understanding of operational-level tradeoffs and effects of offensive and defensive cyber maneuvers, the staff can provide the technical details.

## **PURPOSE**

Commanders currently provide an overarching intent to their operations orders. As cyberspace operations increase in frequency and importance, the commander’s intent should consistently include cyber operations as part of their scheme of maneuver. This article will hopefully stimulate discussion among United States cyber warriors and others and provide preliminary examples that enhance operational-level cyber maneuver doctrine by



**Dr. Patrick D. Allen (COL, Ret. USAR),** currently an Information Operations Specialist at the Johns Hopkins University Applied Physics Laboratory, has a B.S. in Physics, an M.S. and Ph.D. in Operations Research, and a Master's in Strategic Studies. A graduate of both Army War College and Air War College, over his 40-year career, Dr. Allen has supported various organizations within the U.S. Defense and Intelligence Communities on topics including cyber, analysis, research and development, and modeling and simulation, as well as consulted internationally for Canada, the United Kingdom, and Sweden. A former Visiting Fellow at Cranfield University, UK Defence Academy, and a former Director of the Military Operations Research Society, he holds one patent and is author of two books, *Information Operations Planning*, and *Cloud Computing 101: A Primer for Project Managers*, five book chapters, and many journal articles. Readers should feel free to contact the author directly.

describing *cyber maneuvers at the operational level*, and connecting high-level doctrine to the lower-level tactics, techniques, and procedures (TTPs).

This article also seeks to explain why commanders do not need to know the technical details of specific cyber actions to create a commander's intent that includes cyber operations. All they need to do is select a principle or *category of maneuver* that accommodates the commander's intent and operational concept, as reflected in the *scheme of maneuver*. The staff then selects specific cyber and non-cyber maneuver actions or fires to accomplish the intent of each category of maneuver, and discusses any emergent issues with the commander. This helps bridge the gap between operational knowledge and objectives, and cyber knowledge and objectives, which also leads to better integration of cyber effects into operations.

## CONTEXT SETTING

Commanders integrate warfighting functions into their operations. The U.S. Army defines six warfighting functions, which are suitable for the development of concepts for maneuver in cyberspace: "mission command, movement and maneuver, intelligence, fires, sustainment, and protection."<sup>[1]</sup> Maneuver, which is also one of nine principles of war,<sup>[2]</sup> is defined in Joint Publication (JP) 3-0 as "employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy."<sup>[3]</sup>

"Military doctrine aims at prescribing the manner in which an armed force will fight."<sup>[4]</sup> The U.S. Armed Forces are moving to multi-domain operations (MDO), which is doctrine that integrates the warfighting functions.

To summarize the main points of MDO, our adversaries are competing with the US short of conflict, using political, military, and economic means to separate the US from its partners. "The **central idea** in solving this problem is the *rapid and continuous integration of*

*all domains of warfare* to deter and prevail as we compete short of armed conflict.”<sup>[5]</sup> During conflict, our adversaries “will employ *multiple layers of stand-off* [attacks] in *all domains—land, sea, air, space and cyberspace*—to separate U.S. forces and our allies in time, space and function in order to defeat us... *The U.S. Army in Multi-Domain Operations 2028* concept proposes a series of solutions to solve the problem of *layered stand-off*.”<sup>[6]</sup> “*Multi-domain formations* possess the capacity, endurance and capability to access and employ capabilities across all domains to pose multiple and compounding dilemmas on the adversary.”<sup>[7]</sup> [Text as highlighted in the original; cyberspace defined in JP 3-12.<sup>[8]</sup>]

Cyber maneuver is one proposed component of MDO, and focuses on the warfighting function of maneuver within and through cyberspace. Offensive and defensive cyber maneuvers support multi-domain operations outside of cyber, and vice versa, as part of MDO doctrine integrating the warfighting functions during both competition and conflict. This article proposes mental models and terminology to help insert operational-level cyber maneuvers into MDO.

The US and its allies devote substantial time and effort identifying and fixing their network vulnerabilities, and identifying and exploiting vulnerabilities on adversary networks.<sup>[9]</sup> While these efforts are necessary, the shifting nature of conflict requires the US to be more proactive. For example, rather than simply finding adversary vulnerabilities, offensive cyber maneuvers can be leveraged to create such vulnerabilities, and also to cause adversaries to respond in ways that create new exploitable vulnerabilities. This article explains how this in turn can support the U.S. Cyber Command’s (USCYBERCOM) developing strategy that includes “persistent engagement” and “defend forward.”<sup>[10]</sup>

Similarly, waiting to detect adversary activities on our own networks is reactive. More proactive cyber defensive maneuvers will allow US cyber warriors to take actions on the network that expose and act against otherwise undetected adversaries.

## APPROACH

Technology by itself does not ensure victory in kinetic operations or in cyber conflict. *All conflict is primarily a battle of wits between opponents*—our minds against the minds of our adversaries. While technological advancements over an opponent are part of that competition of the minds, it is the continuous, ongoing operational application of *mental creativity and agility* over an opponent that leads to success in cyberspace.

Cyber maneuvers include the application of traditional military principles of maneuver to cyberspace and are also the actions that facilitate the achievement of maneuvering in cyberspace as described in JP 3-12. The following proposed definition of cyber maneuver will likely evolve over time based on feedback.

Cyber maneuvers are actions taken within and through cyberspace to achieve physical, technical, and cognitive positional and temporal advantages over an adversary.

Physical advantages include physical access to friendly and adversary cyber capabilities, including through a supply chain. Technical advantages include having better cyber capabilities and methods of employment than the adversary. Cognitive advantages include, but are not limited to, having better information about a situation than the adversary, such as surprise, deception, and apparent invincibility; the ability to manipulate adversary thoughts and actions; and undermining adversary confidence. Cyber maneuvers can also help achieve non-cyber effects, while non-cyber maneuvers can help achieve cyber effects.

Physical and technical *positional* advantages include access where and when desired, thus allowing for unhindered use of cyberspace to prevail over adversaries. Cognitive *positional* advantages include gaining dominance over the minds of the adversary with respect to their views of their options, chances for success, confidence in their situation, and overall will to continue the conflict. Cognitive positional advantage superior to the adversary in cyberspace can be enhanced by coordinating Information Operations with cyber maneuvers, as described below. International public opinion, especially that of US allies, should always be factored into whether, when, and how we achieve cognitive positional advantage, to include how and when the adversary is *made aware* of the threats or results of US actions.

Cyber maneuver is much more than identifying and controlling “cyber key terrain,” applying moving target defense technology, using decoys on a network, or performing lateral movement on an adversary’s network. These techniques can all contribute to specific cyber maneuvers, but cyber maneuver is larger than any of these examples.

## CONNECTING MISSION TO MANEUVERS

Military operations begin with a mission or goal. From the mission, commanders derive the “commander’s intent,” or prose description of sequential and parallel actions that will fulfill the mission. Thus, the commander’s intent describes a “scheme of maneuver” for how the various types or categories of cyber maneuver will unfold.

- ◆ ***Schemes of maneuver*** define which *categories of maneuver* will be applied and in which sequence to achieve a specified mission (e.g., achieving a set of desired results).
- ◆ ***Categories of maneuver*** define the purpose, intent, and general mechanism for applying cyber capabilities, are more enduring than cyber maneuver actions or cyber fires, and are an abstraction of specific cyber actions that allows easy insertion and operational flexibility into maneuver narratives. Categories of maneuver are key to defining “mission type” orders, and are distinguished from maneuver actions and cyber fires because they include an intent that can be mapped back up to the mission’s antecedent scheme of maneuver.
- ◆ ***Cyber maneuver*** actions achieve the intent of the category of maneuver they support. Maneuver actions are specific and less enduring than categories of maneuver because technology evolves, as do the countermeasures of cyberspace adversaries, who learn to

identify and counter specific maneuvers. (This article distinguishes “categories of maneuvers” from “maneuver actions” by using “maneuvers” to refer solely to the latter.)

- ◆ **Fires** may be cyber, physical, influence, or other actions designed to implement or facilitate cyber maneuvers. Note that physical actions and influence actions can support cyber maneuvers, just as cyber maneuvers can help achieve physical and influence actions. A specific fire may support multiple categories of maneuver, as described in the distributed denial of service (DDoS) example below.

Assembling these component definitions, the scheme of maneuver describes the commander’s intent, and is constructed from categories of cyber maneuvers sequenced (or parallel) to accomplish that mission. Cyber maneuver actions and fires are then selected to fulfill the intent of each category of maneuver that supports the scheme of maneuver. Maneuver actions and fires may be cyber, physical, or influence actions taken to support a category of maneuver, as shown in the Figure below.

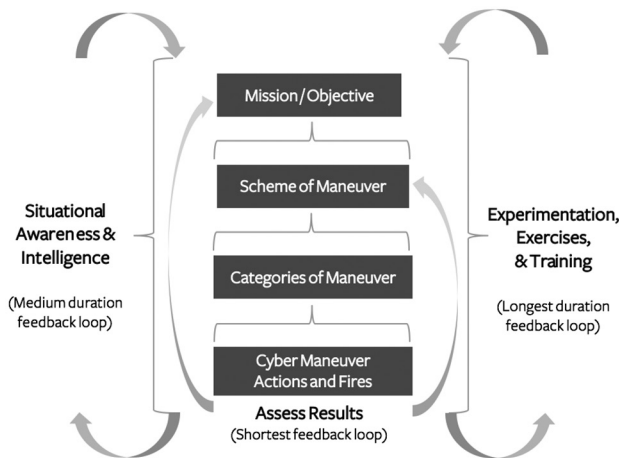


Figure 1: Components of Cyber Maneuver

As depicted above, the longest-duration feedback loop is the experimentation,<sup>[11]</sup> exercises, and training of the cyber maneuvers. The medium-duration feedback loop is driven by situational awareness and intelligence. The shortest feedback loop assesses the results of cyber maneuver actions and fires against the planned scheme of maneuver and/or the mission or objective. This Figure also highlights the dependence of cyber maneuver on sound situational awareness and intelligence, without which many maneuvers in cyberspace would be infeasible. Cyber actions are also useful in generating valuable intelligence or situational awareness to support other maneuvers.

This construct avoids many problems encountered in the cyber maneuver literature, which tends to be either too abstract or too detailed. For example, “deter” is an objective, not a maneuver, while DDoS is an action that could support, e.g., three different categories of maneuver: “delay,” “distract,” or “spoiling attack.” An example of a “distract” intent occurred after the

series of large-scale Iranian DDoS attacks against US financial institutions. A later, much smaller, DDoS attack distracted financial institution defenders such that otherwise detectable fraudulent financial transactions actually succeeded.<sup>[12]</sup> An example of a spoiling attack is the alleged attack by USCYBERCOM against the Russian Internet Research Agency (IRA) in November 2018.<sup>[13]</sup> A single category of maneuver can include multiple cyber actions. Of these actions, any one at other times could be used for various categories of maneuver. Moreover, one category of maneuver can be used to help achieve the objectives of another category of maneuver, as described below (see section on Schemes of Maneuver).

## CATEGORIES OF MANEUVER WITH EXAMPLES

This article lists twenty-one categories of maneuver in cyberspace, which will likely evolve over time. The first eleven are similar to principles of kinetic operations; the next five are similar to psychological operations (PSYOP—now called Military Information Support Operation, or MISO) principles; the last five are common hacking and counter-hacking principles. Nearly all apply to offensive cyber operations (OCO), two apply exclusively to defensive cyber operations (DCO), and more than half apply to both.

### Similar to Kinetic Principles

- ◆ Ambush: Attract an adversary into a hidden “kill zone” (OCO, DCO)
- ◆ Herd: Push or Turn an adversary into a hidden “kill zone” (OCO, DCO)
- ◆ Stimulate a Response (DCO)
- ◆ Probe Adversary (OCO)
- ◆ Distract (OCO, DCO)
- ◆ Delay Adversary (OCO, DCO)
- ◆ Launch Spoiling Attack (OCO, DCO)
- ◆ Launch Supporting Attack (OCO)
- ◆ Counterattack (OCO, DCO)
- ◆ Counter Asymmetric Advantage (OCO, DCO)
- ◆ Leverage Deception (OCO, DCO)

### Similar to Psychological Operations (PSYOP) Principles

- ◆ Appear Invincible (OCO, DCO)
- ◆ Undermine Adversary Confidence (OCO, DCO)
- ◆ Create False Sense of Security (OCO)
- ◆ Leverage Shifting Allegiances (OCO, DCO)
- ◆ Employ Influence Messaging (OCO, DCO)

## Common Cyber Hacking and Counter-Hacking Principles

- ◆ Ensure Persistence (OCO)
- ◆ Vary Launch Points (OCO)
- ◆ Apply Social Engineering (OCO)
- ◆ Change the Terrain (or Manipulate the Network) (OCO, DCO)
- ◆ Leverage Perishability (DCO)

These categories can be used for offensive operations on adversary networks (Red space), defensive operations on friendly networks (Blue space), or in support of offensive or defensive operations in other networks not owned by us or the adversary (Gray space).<sup>[14],[15]</sup>

No single technique will work in all scenarios. No matter how successful a given technique, a countermeasure inevitably appears soon thereafter. The timing (simultaneous or sequential, and when) and flexibility of cyber maneuver schemes (if this does not work, do that instead) is what makes cyber maneuvers succeed. Similarly, no cyber maneuver technique *has* to work all the time. Sometimes, even using an unsuccessful technique can sow doubt in the minds of the target populace. For example, ineffectual Russian hacking attacks against voter registration systems in late 2018 caused substantial consternation in the US even though no Russian hacking attempt appears to have succeeded.<sup>[16]</sup>

This section provides examples of most of the twenty-one listed categories of maneuver. Again, individual maneuver actions and techniques will become more or less effective over time as cyber technologies evolve. *Categories of maneuver* and *principles of maneuver* are more enduring.

**Ambush** maneuvers seek to *lure* an adversary into an unforeseen “kill zone.”<sup>[17]</sup> For an offensive cyber example, our forces infect both a branch and a leaf node in an adversary network. The leaf node then announces it is infected, bringing forth the adversary’s network defenders, which access the infected leaf node via the branch node. Our forces infect the adversary responders’ toolkit, thereby converting the toolkit into an access vector and unwitting agent of future infection. This ambush example need not always work, but its existence may distract or cause hesitation by the adversary defender, which can be the ultimate goal of the maneuver.

**Herding** seeks to push or turn adversary actions in a direction more desirable to the US. For example, if the US infects the less active of two “hot swap” routers, and then DDoS the more active one, the result is to *push* or *turn* the adversaries into the kill zone of an already infected router. Herding can also be applied to DCO, attempting to force adversaries away from more lucrative targets on U.S. networks.

**Stimulating a response** can involve a network defender changing passwords for a network segment, and watching for a previously undetected adversary seek to regain lost access—one of many actions defender can take to expose or “out” as-yet-undetected adversaries.

**Probing an adversary** is the offensive version of stimulating a response. The results of probing actions can provide valuable information about how an adversary defender will likely react, which can significantly contribute to achieving reflexive control<sup>[18]</sup> over the defender.

**Distract** and **delay** are two categories of maneuver that encompass many specific maneuver actions. As mentioned above, for example, a DDoS attack can help achieve a delay, a distraction, or a spoiling attack. Decoys can also distract or delay adversaries.

“A **spoiling attack** is a tactical maneuver that can cripple a hostile attack at the very outset, while the enemy is assembling for an attack.”<sup>[19]</sup> A spoiling attack seeks to disrupt adversary momentum or preparations, which buys time, gains initiative, or disrupts adversary effectiveness.

As a cyber example, USCYBERCOM allegedly performed a form of spoiling attack against Russian influence operations days before for the 2018 elections by launching attacks against the Russian Internet Research Agency (IRA) that, according to one source, “basically took the IRA offline...They shut them down...”<sup>[20]</sup>

Cyber **supporting attacks** are designed to achieve an effect outside of cyberspace, e.g., taking down an adversary’s electric power grid. Cyber warriors often operate in and through cyberspace to affect physical systems and adversary minds. Similarly, physical actions outside of cyberspace can support cyberspace maneuvers.

In the kinetic world, **counterattacks** typically are launched when the adversary is reaching its culminating point, i.e., when the attacker has extended itself geographically and expended its resources, such as ammunition, fuel, human energy and other combat resources.<sup>[21],[22]</sup> The counterattack seeks to time its attack to coincide with the adversary’s most vulnerable moment, roll back any gains, and perhaps destroy its forces, and otherwise create and exploit follow-on opportunities. Identifying an adversary’s culminating point in cyberspace is quite challenging. For example, bots do not get tired or run out of energy. One can “hack back” at a remote intruder, or send infected files as part of the stolen materials being exfiltrated by an adversary, but timing these actions is independent of any identifiable culminating point. Counterattack is one of our proposed categories of cyber maneuver, yet its meaning is quite different from the kinetic principle of the same name. Joint Cyberspace Operations doctrine for Defensive Cyberspace Operations-Response Actions already includes the cyber counterattack maneuver.<sup>[23]</sup>

In **countering an asymmetric advantage**, history is replete with examples of one side having an advantage (e.g., in range or firepower), yet the other side invariably adopted tactics and/or maneuvers that countered those advantages. The side with limited range and/or maneuverability chooses to fight in close-in terrain, such as urban areas (like Stalingrad in World War II), forests (like Teutoburg Forest in 9 A.D.), or mountainous terrain (like Afghanistan throughout history). Countermeasures in cyberspace follow the martial arts technique of leveraging an adversary’s strength against it. For example, botnets are large and difficult to identify and



eradicate. Rather than trying to reduce the size of a botnet, render it unmanageably large, or at least so large as to make its command and control channels obvious. One potentially useful technique is to place a copy of the botnet malware on 100,000 nodes in a virtual private cloud with Internet access we control. The bots all duly report back to their C2 network, potentially swamping the C2 nodes. At the very least, the C2 node locations can be identified by the huge traffic generated by 100,000 simultaneously reporting new bots. Once the C2 nodes are exposed or overwhelmed, all nodes in the cloud can be shut down by our side, which owns them, thereby barring adversary access to a new 100,000-node botnet.

Cyberspace offers myriad ways to **leverage deception**, such as deploying decoy assets (e.g., hosts, routers, or servers), decoy users, decoy credentials, decoy traffic, and decoy content. Many commercial deception-for-cyber-defense tools are now available. For example, multi-fidelity decoy assets can effectively keep adversary intruders guessing as to what is real. Having very low-fidelity decoy nodes on the network may cause intruders to think they know what decoys look like. Learning the decoy was actually a higher-fidelity decoy should give adversaries pause. Repeats with increasingly high-fidelity decoys can cause the adversary to wonder whether a real network asset is actually authentic.

Projecting **invincibility** can seriously degrade adversary morale. In some cases, the adversary is truly helpless, such as when the Operation DESERT STORM (ODS) Coalition had air superiority over Iraqi ground forces and could bomb them at will.<sup>[24]</sup> In other cases, the invincibility may merely be an illusion. The following cyberspace example dates from when “Anonymous,” in its heyday, would announce that on a certain date in the following week, nothing could be done to stop the hacking of a given target. The author is not sure if the following is what Anonymous did, but it is likely that Anonymous would have already hacked the target and planted several back doors. They could also have already downloaded materials unique to the target to prove the target was hacked, even if the target disconnected itself from the Internet. Sure enough, whenever Anonymous declared a target would be hacked, it was. Whether Anonymous really could hack any target or had already hacked the target was irrelevant, as either way, *it gave the impression of invincibility*.

Similar cyber maneuvers can be performed against our adversaries. After our forces hack a target, they let that target know it will be hacked at a specified future time, creating a “horns of a dilemma”<sup>[25]</sup> for the target. Either the adversary shuts off all outside connections, constituting a self-denial-of-service, or it maintains normal operations with increased vigilance, and risks proof of vulnerability to penetration, as forewarned.

**Undermining adversary confidence** shakes the adversary’s confidence in its resources. During ODS, coalition forces would come up on the Iraqi military radio nets and announce coalition presence on the Iraqi nets, thereby proving it was literally operating within the Iraqi communications space.<sup>[26]</sup> These on-net announcements had a devastating effect on Iraqi morale, with lost confidence in the confidentiality, integrity, and even availability of working communications.

A similar set of cyber maneuvers can be performed, for example, by leaving messages on adversary computer screens, confirming your access to its network, along with five changes you made to that network, with each change flagged with a calling card, each confirming one of your five actions. If in reality, you made only four changes, imagine the untold consternation to the adversary, who devotes untold time trying to find and fix the phantom fifth change!

Conversely, **creating a false sense of security** gives the adversary wholly unfounded confidence in its network. For example, if we stop sending messages on adversary networks that had undermined its confidence, at the same time it took *unsuccessful* steps to end our intrusions, and it mistakenly believed its actions stopped our messages, with our forces still on its network, that adversary would have a false sense of security about its network. Note that the use of maneuvers to cause the adversary to lose confidence in its resources, followed by a false sense of security maneuver, is a good combination to employ as a pair within a scheme of maneuver. Similarly, once our forces are on the adversary's network, our forces could pretend that they have not gotten in by making obvious access attempts designed to be readily blocked.

**Shifting allegiances** can be leveraged at the individual, group, and national levels. In addition to causing someone to switch sides, shifting allegiances can also mean that someone or some group “shifts into neutral” for a short period of time.<sup>[27]</sup> For example, when the CIA had paid the local tribes a substantial amount of money to keep Osama bin Laden trapped in Tora Bora, bin Laden then paid the tribesmen even more money to let him pass through their lines. As a result, bin Laden escaped from Tora Bora because the Afghani tribesmen hired by the CIA “shifted into neutral” long enough for him to escape.<sup>[28]</sup>

Shifting allegiances have always been a problem historically. From individuals opening castle gates to large scale defections before or even during a key battle, empires have been lost or gained because of a timely shift in allegiance. In cyberspace, this may be as simple as “just put this thumb drive into a computer,” or a longer-term campaign of convincing someone to switch sides. An example of shifting into neutral in cyberspace would be to ignore an alert or to fail to check certain logs until a specified time has passed.

Cyber maneuvers can support, and be supported by, non-cyber activities, such as **employing influence messages**. One type of influence message aimed at cyber adversaries is to misattribute a cyber action intentionally to stimulate an adversary response in Blue or Gray spaces. These misattribution messages are more likely to work against civilian criminal hackers than nation-state hackers; however, criminal hackers are often hired by nation-states to do their hacking, so this method may succeed. Messages may also be sent directly to Red space recipients informing them their identities and actions are known. USCYBERCOM allegedly sent such messages to the Russian IRA to attempt to dissuade them from further activities.<sup>[29]</sup>

**Ensuring persistence, varying launch points, and applying social engineering** are also standard hacking techniques and will not be further elaborated upon here.

**Changing the terrain** by manipulating the network works on both the defense and offense. Researchers have been working on various forms of moving target defenses for years with some success in changing memory address spaces. An alternative to just rotating IP addresses is to rotate Media Access Control (MAC) addresses, and changing the Organizationally Unique Identifiers (OUI), which are the first three octets of the universally administered address the manufacturer assigns to each device. These changes can be achieved by running a PowerShell script. The goal is to frustrate and complicate adversary reconnaissance and target identification – machines self-identifying as Dell laptops might roll their OUIs and suddenly appear on an adversary’s sensors as iPhones, vulnerable IoT webcams, or Cisco firewall appliances. Note for example Operation ShadowHammer (the ASUS hack) targeted fixed MAC addresses.<sup>[30]</sup>

An offensive version of rotating MAC addresses and OUIs on an adversary’s network can be part of a “moving target attack.” While every adversary machine can still function, no communication between endpoints can occur for about 30-45 minutes until the Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) catch up and IP/MAC mapping concludes. Repeated application of this attack can keep the adversary endpoints isolated from each other for longer periods. Nothing is destroyed, making this an attractive permitted maneuver during Red Team engagements or during pre-conflict as it will likely meet rules of engagement (ROE).

The defender can also **leverage perishability** by increasing the rate of network changes. Access can be lost through normal system changes or upgrades, as well as by defender actions. Cyber techniques are perishable because evolving countermeasures and workarounds neutralize or reduce original use efficacy. “The technology upon which cyberspace is based is constantly evolving... This ongoing evolution leads to constant changes in tactics and procedures used by both attackers and defenders in cyberspace.”<sup>[31]</sup> “This capability to maneuver and provide operational reach may be lost at any time if the configuration of the relevant cyberspace nodes is modified.”<sup>[32]</sup>

Note that most of the maneuver actions listed in this article have yet to be laboratory tested. The article focuses primarily on the upper part of the stack illustrated above: How to connect goals to the scheme of maneuver, and to the categories of maneuver supporting the scheme of maneuver. The primary purpose of listing the component maneuver actions is to give examples, which should not be considered vetted maneuver actions.

JP 3-12, *Cyberspace Operations*, lists two main categories of cyberspace attack actions: manipulate and deny. Deny includes degrade (reduce capability to a specified level of operation), disrupt (100 percent denial for a specified period), and destroy. “Manipulate” includes changing information or information systems in Red or Gray spaces “using deception, decoying, conditioning, spoofing, falsification and other similar techniques.”<sup>[33]</sup> The Table below shows that most categories of maneuver presented in this article belong to the “manipulate”

## CYBER MANEUVER AND SCHEMES OF MANEUVER

category. Only a few (spoiling attack, supporting attack, counterattack, leveraging shifting allegiances, and changing the terrain) support both “manipulate” and the three denial categories.

Table 1: Mapping the 21 Categories of Maneuver to JP 3-12 Attack Categories

Categories of Maneuver	Degrade	Disrupt	Destroy	Manipulate
Ambush: Attract to a “kill zone”				✔
Herd: Push to a “kill zone”				✔
Stimulate a Response				
Probe Adversary				
Distract				✔
Leverage Deception				✔
Delay Adversary				✔
Counter Asymmetric Advantage				✔
Launch Spoiling Attack	✔	✔	✔	✔
Launch Supporting Attack	✔	✔	✔	✔
Counterattack	✔	✔	✔	✔
Appear Invincible				✔
Undermine Adversary Confidence				✔
Create False Sense of Security				✔
Leverage Shifting Allegiances	✔	✔	✔	✔
Employ Influence Messaging				✔
Ensure Persistence				
Leverage Perishability				
Vary Launch Points				
Apply Social Engineering				✔
Change the Terrain	✔	✔	✔	✔

### COMMANDER’S INTENT AND SCHEMES OF MANEUVER

The commander’s intent is a clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander’s desired results without further orders, even when the operation does not unfold as planned.<sup>[34]</sup>

The scheme of maneuver is “the central expression of the commander’s concept for operations that governs the development of supporting plans or annexes of how arrayed forces will

accomplish the mission.”<sup>[35]</sup> In the preceding Figure, the commander’s intent is represented within the scheme of maneuver, which includes a sequence of categories of maneuver like the ones described above. For example, if the mission is to use non-kinetic means to deter a nation from invading a neighboring US ally country, the scheme of maneuvers might be:

Employ cyber *probing*, *ambushes*, and *herding* to ensure persistent access to the adversary network. By [specified date], launch actions to *undermine adversary confidence* in its network resources, followed by a *change the terrain* to preclude its network connectivity until [specified date]. If by this [specified date] the adversary has been deterred from invading the neighboring country, execute *create a false sense of security* on its network. If the adversary starts preparing again to invade its neighbor, execute *appearance of invincibility* maneuvers to deter their resumption of preparations.

Note that this scheme of cyber maneuver consists of a specified sequence of eight categories of maneuver (listed in italics). Which specific cyber maneuver actions and fires will be selected by the commander’s staff is less important than *articulating the intent* described by the sequence of maneuver elements of the scheme of cyber maneuver. Moreover, if the intent of each category of maneuver has been approved, then the specific maneuver actions eventually selected to accomplish that intent are more likely to be approved as well.

Creating a common lexicon is important to identify clearly both the similarities and the differences among traditional military kinetic and PSYOP doctrines and cyber operations. “We should recognize when these constructs do not fit cyber and use simple, clear language to communicate.”<sup>[36]</sup> “As the military continually seeks to adapt its approach to maneuvering intelligently in the cyberspace domain, it must also do the same with its practice of training cyberspace maneuver leaders.”<sup>[37]</sup>

Cyber schemes of maneuvers not only should have their own synchronization matrix to coordinate and deconflict cyber elements of the operation; cyber maneuvers should also be included in the overall mission synchronization matrix across the whole force,<sup>[38]</sup> to preclude not only mission fratricide (such as cutting electrical power before broadcasting a TV message to the populace), but also fratricide among cyber maneuver elements.

A second sample cyber scheme of maneuver focuses on exposing and neutralizing adversary activity on a friendly network that will soon be used in a critical operation, the intent being to get the adversary off our networks for a specified time period—not forever.

Increase monitoring on the network and then *stimulate a response* by changing all authentication passwords simultaneously. Watch for adversary attempts to regain access. *Leverage deception* to allow the adversary to regain access onto decoy assets to *delay adversary* regaining access and identify adversary TTPs. Simultaneously execute *delay adversary* maneuvers in identified adversary hop points and listening posts operating out of Gray space and Red space. This will increase the time the adversary needs to regain access and help identify new hop points and listening posts being used as alternative, faster routes.

A third sample cyber scheme of maneuver focuses on protecting another nation from adversary actions and eventually exposing the adversary actions on that country's networks.

Identify adversary-compromised resources operating on another nation's networks. *Undermine adversary confidence* in its footholds on the network by feeding it false information and malware. Change the terrain by using SatCom box technology to relay more obviously the communications from the adversary to its listening posts such that the targeted nation can more easily identify the source of the adversary activities. Covertly assist the targeted nation in exposing the adversary presence on its network. In addition, *create a false sense of security* in the adversary for its implants that have not yet been exposed. When the adversary claims to have no further presence on the targeted nation's network, expose to the host nation via *influence messaging* these previously unexposed (but detected by us) adversary implants.

There are many negative effects for the adversary, such as its exposed presence (especially repeated exposed presence post-denial, which is politically damaging). Second, the adversary loses access to key networks in the targeted nation. Third, it likely will be more cautious about compromising other networks in the targeted nation for fear of a similar outcome.

Note: one category of maneuver can support another category of maneuver. For example, defensively modifying the MAC addresses is listed under the maneuver category "change the terrain," but changing the terrain can also be used to enable a deception for a defense maneuver, or a herding maneuver. The scheme of maneuver can describe these planned interactions between categories of maneuvers, to ensure the sequence of desired maneuver effects is achieved.

Overall, the mission or goal defines the objective. Then the commander's intent defines the scheme of maneuver at the level of the categories of maneuvers. The identified categories of maneuver are fleshed out by the staff with specific maneuver actions that meet the criteria to accomplish the scheme of maneuver and thereby accomplish the mission.

A key advantage of this framework is that commanders need not know all technical details of specific maneuver actions. So long as operational-level effects and tradeoffs are understood, the commander selects a category of maneuver tailored to his/her intent, and incorporates it as a component of the overall scheme of maneuver, then the gap between operational knowledge and objectives, and cyber knowledge and objectives, can be effectively bridged. This in turn should lead to better integration of cyber effects into overall operations.

## NEXT STEPS

This section suggests some follow-on steps not covered in this article, and thus seeks to stimulate discussion that further fleshes out the optimal integration of the cyber domain into the overall operation and, in particular, the categories of maneuver. For example, one important

related topic not covered is how best to extend this analysis to integration of cyber actions with radio spectrum and electronic warfare capabilities within the schemes of maneuver.

Another goal is to institutionalize a lexicon for cyber maneuvers for military personnel who are more familiar with kinetic and PSYOP concepts. This in turn, should help facilitate multi-domain operations across both the physical and cyberspace domains, to include electronic warfare, and influence operations in both competition and conflict. While a shared culture of understanding of terminology does not yet exist for our cyber warriors, this article hopefully will stimulate rigorous discussion and thought as to how best we can solidify and clarify doctrine and terminology to strengthen a shared culture. This article gives an early snapshot glimpse of evolving thought on the topic at the Johns Hopkins University Applied Physics Laboratory (JHU/APL). The proposed definitions, maneuver actions, and benefits are all works in progress.

Addressing DoD's implementation of doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) issues is beyond the scope of this article.<sup>[39]</sup>


This article does not address one important consideration of conflict in cyberspace, which is being able to detect and identify adversary cyber maneuvers, and recommend counter-maneuvers designed to thwart or even exploit adversary maneuvers. The focus instead is first to facilitate agreement on formulating cyber maneuver actions, cyber maneuver categories, and schemes of maneuver. Establishing at least a preliminary set of clear definitions should prove valuable in tackling efforts to detect and counter adversary uses of cyber maneuvers.

Another important factor not addressed in this article is the need for good situational awareness (SA) and intelligence support to accomplish cyber maneuvers. The author assumes that intelligence dominates obtaining information about adversary capabilities in Red and Gray spaces, while SA dominates obtaining information about our cyber capabilities in Blue and Gray spaces. Intelligence can also be obtained directly from cyber maneuvers, such as probing actions to identify adversary responses.<sup>[40]</sup> Moreover, this paper does not address the important tradeoff issues associated with intelligence loss and gain that the staff must consider when using certain cyber capabilities. The commander obviously requires clear staff feedback whenever a potential scheme of maneuver cannot or should not be accomplished by the existing suite of available cyber actions. In addition, experiments will help determine how well these maneuvers work in a simulated environment with human opponents, as well as quantify the benefits of cyber maneuvers.

## SUMMARY

This article grapples with the analysis and lexicon of commanders charged with integrating cyber domain operations into other much longer established domains of the battlefield. The article presents an approach to offensive and defensive cyber maneuvers at the operational level that starts with a goal or mission, and allows preparation of the commander's intent via a scheme of maneuver. The scheme of maneuver includes a sequence of *categories of maneuver*,

which in turn are accomplished by specific cyber (or non-cyber) maneuver actions or fires. This approach connects the mission to the scheme of maneuver, to categories of maneuver, and then to specific actions and fires. The categories of maneuver and their intent are much more enduring than specific cyber maneuvers or fires, which will evolve over time. Using this approach, commanders do not require technical expertise in order to define and execute a cyber scheme of maneuver. So long as the commander has, or has been provided, sufficient understanding of the operational-level tradeoffs and effects of offensive and defensive cyber maneuvers, the staff will provide the technical details.

This article has briefly described twenty-one categories of maneuvers, illustrated with a sample maneuver action for each, and presented three sample schemes of maneuvers. This is just the beginning. The author anticipates and welcomes additional cyber maneuvers, categories of maneuvers, and sample schemes of maneuver. Readers should feel free to contact the author directly. 

## DISCLAIMER

The views expressed here are those of the author and do not reflect the official policy or position of the Johns Hopkins University Applied Physics Laboratory.

## ACKNOWLEDGMENTS

While Dr. Patrick Allen (COL Ret., USAR) was the initiator and primary author of this article, many Johns Hopkins University Applied Physics Laboratory (JHU/APL) staff and consultants contributed ideas, references, comments and reviews throughout the writing process. Since there were 35 other contributors and reviewers, they are listed here in alphabetical order: Natalie Anderson, Mika Ayenson, Alex Barut, Dave Bondura, Calvert “Triiip” Bowen, Bob Butler, Jamie Castle, Welton Chang, James Curbo, Matt Dinmore, Pete Dinsmore, Bud Halla, Bryon Hartzog, Kristine Henry, Mike Hostetter, Jessi Hupka, David Lachut, Alex Lee, Sue Lee, Stephen Lidard, Paul Markakis, Jennifer McKneely, Dan Meidenbauer, Rob Nichols, J. R. Parsons, Jody Patilla, Aaron Pendergrass, Doan-Trang Pham, John Quigg, Rob Schrier, Tamim Shookoor, Karl Siil, Kath Straub, Katherine Watko, and Keith Wichmann.

Brainstorming sessions were held at JHU/APL that included veterans and currently serving military reservists (from cyber, kinetic, PSYOP, and intelligence communities), staff member SMEs involved in both defensive and offensive cyber technology and operations, and staff knowledgeable in influence and Gray Zone operations. This article seeks to synthesize all preceding sources, and help discuss and the future of cyber maneuver.



## NOTES

1. Army Doctrine Publication No. 3 *Operations*, ADP 3-0, para. 46.
2. “Objective, offensive, mass, maneuver, economy of force, unity of command, security, surprise, and simplicity.” Joint Publication 3-0, *Joint Operations*, January 17, 2017, incorporating change 1, October 22, 2018. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_0chl.pdf?ver=2018-11-27-160457-910](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0chl.pdf?ver=2018-11-27-160457-910)
3. JP 3-0, Ibid.
4. John Whiteclay Chambers II, *The Oxford Companion to American Military History*, Oxford University Press, <https://www.oxfordreference.com/view/10.1093/acref/9780195071986.001.0001/acref-9780195071986?b-tog=chap&hide=true&jumpTo=Do&page=14&pageSize=20&skipEditions=true&sort=titlesort&source=%2F10.1093%-2Facref%2F9780195071986.001.0001%2Facref-9780195071986>
5. TRADOC PAM 525-3-1 “The U.S. Army in Multi-Domain Operations 2028,” December 6, 2018, Preface.
6. TRADOC PAM 525-3-1, Ibid.
7. TRADOC PAM 525-3-1, Ibid.
8. Joint Publication 3-12 *Cyberspace Operations* defines cyberspace as “a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”
9. Aaron F. Brantly, “Strategic Cyber Maneuver,” *Small Wars Journal*, October 17, 2015.
10. Paul Nakasone, “An Interview with Paul M. Nakasone,” *Joint Forces Quarterly*, Issue 92, 1st Quarter 2019.
11. Robert R. Hoffman, *Cyber Defense Review*, Vol. 4, No. 1, Spring 2019.
12. Steven Musil, “Cybercrooks use DDoS attacks to mask theft of banks’ millions,” *CNet.com*, August 21, 2013.
13. Ellen Nakashima, “U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms,” *The Washington Post*, February 27, 2019.
14. Kamal Jabbour, “The Science and Technology of Cyber Operations,” *High Frontier*, (May 2009), 11.
15. Joint Publication 3-12 *Cyberspace Operations*, June 8, 2018, I-4.
16. Justin Lynch, “The voting day crisis election officials fear,” *the Fifth Domain*, 23 October 2018.
17. While FM 3-0 *Operations* defines an ambush as “an attack by fire or other destructive means from concealed positions on a moving or temporarily halted enemy,” we modified the definition of ambush for increased applicability to cyberspace.
18. According to Tim Thomas, “Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.” Timothy Thomas, “Russia’s Reflexive Control Theory and the Military,” *Journal of Slavic Military Studies*, 2004 17: 237–256.
19. FM 3-0, Ibid., Glossary.
20. Ellen Nakashima, Ibid.
21. Joint DoD Dictionary, “The point at which a force no longer has the capability to continue its form of operations, offense or defense.”
22. Joint Information Operations Planning Handbook, January 2012, I-31 to I-32.
23. JP 3-12, II-4.
24. Al Zdon, “Persian Gulf War Ten Years Later: Winning the war by convincing the enemy to go home,” [http://www.iwar.org.uk/psyops/resources/gulf-war/13th\\_psyops.htm](http://www.iwar.org.uk/psyops/resources/gulf-war/13th_psyops.htm).
25. The phrase “horns of a dilemma” describes placing the adversary in a position of two options, where both options cause the adversary to lose something significant. B.H. Liddell Hart, *Strategy*, Praeger, New York, 1954, p. 152.
26. Zdon, Ibid.
27. Patrick Allen, “Training and Planning for Shifting Allegiances,” *Royal Uniform Services Institute (RUSI) Journal*, October 2008.
28. Philip Smucker, ‘How bin Laden got away: a day-by-day account of how Osama bin Laden eluded the world’s most powerful military machine,’ *The Christian Science Monitor*, 4 March 2002.
29. Ellen Nakashima, Ibid.

**NOTES**

30. Catalin Cimpanu, “Researchers publish list of MAC addresses targeted in ASUS hack,” Zero Day, *ZDNet.com*, 29 March 2019.
31. Scott Applegate, “The Principle of Maneuver in Cyber Operations,” Conference Paper, June 2012; <https://www.researchgate.net/publication/236020494>
32. JP 3-12, II-12.
33. JP 3-12 IV-6.
34. JP 3-0, GL-7.
35. Joint DoD Dictionary.
36. Rob Schrier, “Demonstrating Value and Use of Language—Normalizing Cyber as a Warfighting Domain,” *The Cyber Defense Review*, Summer 2017, 19.
37. Andrew Schoka, *Ibid.*
38. Brett T. Williams, “The Joint Force Commander’s Guide to Cyberspace Operations,” *Joint Force Quarterly*, Issue 73, 2nd Quarter 2014.
39. *DoD Dictionary*. (Corresponding terms for civilian agencies are people, framework, processes, and pillars.)
40. JP 3-12, IV-1, IV-2.