The Principle of Maneuver in Cyber Operations

Scott D. Applegate
Volgenau School of Information Technology Engineering
George Mason University
Fairfax, Virginia
sapplega@gmu.edu

Abstract: The United States Military describes the concept of maneuver as the disposition of forces to conduct operations by securing positional advantages before and or during combat operations. This paper will briefly explore how the concept of maneuver in kinetic operations has evolved over time and how that concept relates to cyber operations and cyber warfare. It will attempt to define what constitutes the principle of maneuver within cyberspace as it relates to the traditional concept of maneuver in warfare and how the unique domain of cyberspace alters this concept. This paper will explore the characteristics of maneuver in cyberspace and the basic offensive and defensive forms of maneuver that have thus far emerged will be identified and analysed. The author will also briefly touch on the issue of sovereignty in cyberspace as it relates to cyber maneuver and attempt to identify how and when the concept of cyber maneuver might cross the line to violate a state's sovereignty. This paper will demonstrate that there is a valid concept of maneuver in cyberspace, and that the stealth and anonymity provided by the Internet allows for blatant acts which, in a kinetic operation, would most like result in open armed conflict.

Keywords: *Cyber Conflict, Cyber Maneuver, Cyber Operations, Cyber Warfare*

1. INTRODUCTION

Military Strategists have been writing on the principles and characteristics of warfare for more than two thousand years. Although the specific principles differ over time and in relation to particular strategists, the principle of maneuver has been an important concept and has been a determining factor in warfare since some of the earliest recorded battles. As technology has evolved and allowed for the expansion of warfare into new domains, so too has the concept of maneuver changed. The exploration of the seas created a new unique domain and introduced the concept of a global commons, bringing with it new challenges to overcome. Air and Space added a new dimension to the principle of maneuver and caused yet another shift in military strategy. During the last two decades, the introduction of computing systems and the Internet formed an interconnected, virtual environment that has led to the designation of a fifth warfighting domain known as Cyberspace. This new domain has its own set of unique characteristics and challenges and significantly overlaps operations in all four of the other warfighting domains.

The United States Military describes the concept of maneuver as the disposition of forces to conduct operations by securing positional advantages before and or during combat operations [1]. While this description has some applicability to operations in the domain of cyberspace, it is clear that this open, borderless, virtualized environment alters this principle significantly and an effort must be undertaken to understand and codify these changes.

While cyberspace is considered a warfighting domain, thus far it has manifested itself as more of a contested domain characterized by constant conflict between various competitor states, non-state actors and private entities. Battles rage across this domain continuously and although they have not risen to the level of a declared war, the outcome of some of these battles could have just as significant of an impact on the long term future of the states involved in these ongoing conflicts [2]. Critical computing resources are captured, industrial and military secrets are stolen, strategic plans and diplomatic negotiations are compromised and key government, private, military and infrastructure systems are infiltrated, all to gain a competitive advantage for the states initiating these attacks.

The methods and processes employed to attack and defend information resources in cyberspace constitute maneuver as they are undertaken to give one actor a competitive advantage over another. As various nation-states throughout the world have begun building cyber warfare programs and have actively begun conducting operations in cyberspace, it is important to understand what constitutes the principle of maneuver in cyberspace as it relates to the traditional concept of maneuver in warfare and how the unique characteristics of the cyberspace warfighting domain alter this concept.

2. MANEUVER AS A PRINCIPLE OF WAR

The principle of maneuver has evolved as a tenant of war over the course of several thousand years. Beginning in the earliest recorded battles, the concept of maneuver involved the movement of troops to positions of advantage to attempt to fix and destroy enemy forces. Early forms of engagement included maneuvers such as the single envelopment, the double envelopment and the penetration and were mostly tactical in nature. As technology evolved, commanders were able to leverage new forms of transportation to increase the speed and tempo of maneuver in battle. Additionally, advances in weapons technology introduced the concept of fires and altered the principle of maneuver. At this point the use of maneuver came to resemble more modern definitions of employing forces through movement in combination with fires but was still largely tactical in nature.

The 1700s and 1800s saw the rise of operational maneuver as Napoleon's Grand Army swept through Europe in 1805 [3]. While Napoleon recognized and utilized operational maneuver, it was not until the battles of the American Civil War that it truly became institutionalized as a formal part of doctrine [4]. During World War Two, the German's use of Blitzkrieg ushered in another evolutionary step in maneuver shifting from attrition to maneuver warfare. Prior to World War II, maneuver focused almost exclusively on destroying or defeating the enemy and sought to engage the enemy in decisive battles. By attacking though Belgium and avoiding the strength of the French army, German armored formations were able to drive deep into the enemy rear to achieve strategic success. "The effects of the lightening deep penetrations created a state of paralysis on the French military command forcing the capitulation of France itself" [5]. The development of Blitzkrieg by the Germans and similar developments in other militaries led to the concept of maneuver warfare which focused on incapacitating the enemy through shock and disruption rather than through attrition warfare.

During the 1970s and 80s, Colonel John Boyd developed theories which described maneuver in terms of competitive decision cycles. According to Boyd, "Victory in competitive decision cycles requires one side to understand what is happening and act faster than the other" [6]. Boyd's theories again revolutionized the principle of maneuver as they focused on creating the ability to make appropriate decisions faster than an opponent rather than on kinetic movement and fires. Maneuver in Boyd's terms could be described as "to operate inside an adversary's observation-orientation-decision-action (OODA) loops or get inside his mind-time-space to penetrate an adversary's moral-mental-physical being in order to isolate him from his allies, pull him apart and destroy his will to resist" [7]. Boyd was a key designer of the strategy the United States used to decisively defeat Iraq in the first Gulf War, the asymmetric success of which shocked many other states and led to what was called a Revolution in Military Affairs.

Modern definitions of maneuver owe a great deal to Boyd and many other military theorists and are an amalgamation of the experience of generations of military

strategists. This discussion has very briefly described how the principle of maneuver has evolved and has necessarily skipped many important theorist and contributing theories in favor of brevity. Entire books could be written on how these theories have evolved over time but that is outside the scope of this paper. For purposes of this discussion, it is important to understand that "the essence of maneuver is taking action to generate and exploit some form of advantage over the enemy" [8]. Distilled down to its most basic form, maneuver can be simply defined as movement towards an objective. With this understanding in mind, it is appropriate to attempt to understand how the principle of maneuver applies to the domain of cyberspace and how the unique characteristics of this domain alter this concept.

3. CYBER MANEUVER

Cyber Maneuver is the application of force to capture, disrupt, deny, degrade, destroy or manipulate computing and information resources in order to achieve a position of advantage in respect to competitors. Maneuver in the traditional warfighting domains primarily involves the movement of military forces and application of fires, however, in cyberspace, there is obviously no movement of forces in the kinetic sense since it is a virtualized environment. Instead, maneuver in cyberspace involves the application of force to specific points of attack or defense. This force is the special purpose code written to accomplish the attacker's or defender's objectives and is implemented at the time and virtual location of their choosing. In a very real sense, forces do not move in cyberspace, the point(s) of attack are moved [9]. This makes observation and detection very difficult, especially in relation to the source of attacks.

Cyber maneuver is used to influence human and machine behavior. In a certain sense that is a redundant statement since the purpose of influencing machine behavior is ultimately to influence human behavior. Cyber maneuver leverages positioning in the cyberspace domain to disrupt, deny degrade, destroy or manipulate computing and information resources. It is used to apply force, deny operation of or gain access to key information stores or strategically valuable systems.

Another key factor in considering maneuver in cyberspace is that thus far, there has not been any open, state-on-state, cyber wars. There is, however, a constant state of conflict between states, surrogates or proxies, non-state actors and private entities and a great deal of evidence exists pointing to state involvement in much of this ongoing conflict. It is therefore advantageous to consider not just enemy states, but other adversaries and competitors when describing maneuver in cyber operations. International laws are still relatively immature in regard to cyber warfare, and so long as that remains the case, it is very likely that states will leverage this ambiguity to take actions in cyberspace that would be unacceptable in the physical world.

In defining cyber maneuver, it is important to understand the characteristics that make maneuver in cyberspace unique and to try to identify the major forms of both offensive and defensive maneuver that have thus far emerged in this domain. It should be noted that this effort is not meant to be exhaustive or all-inclusive. This is merely a starting point to try to quantify the trends that are emerging in this relatively new warfighting domain and to provide a basis for others to continue to refine doctrine in relation to cyberspace operations.

A. Characteristics of Cyber Maneuver

Cyberspace is a unique environment comprised of physical, informational and cognitive elements that blend together to create the virtual domain across which cyber operations occur. The principle of maneuver, when applied to operations in cyberspace, has distinct characteristics when compared to maneuver associated with the other warfighting domains of air, land, sea and space.

1) Speed

One of the most obvious characteristics of maneuver is cyberspace is the speed at which it can occur. Actions in cyberspace can be virtually instantaneous, happening at machine speeds. The speed at which actions can take place in cyberspace makes it incredibly difficult for one actor to react and adjust to a successful attack or to the modification of a defensive formation. By the time a successful attack is detected and mitigation undertaken, it is likely that either data has already been compromised or worse, hostile actions have already been completed to the detriment of the defending unit. If a modification is made to an element's defense in the midst of an attack, it is unlikely the attacker will be able to modify the attack quickly enough to continue successfully without being detected. In cyber operations, speed favors the side which has gained the initiative and successful maneuver allows an attacker or defender to get inside their adversaries' decision cycles and move more rapidly than they can react. Speed is a double edged sword in cyberspace. Actions happen at machine speeds, but reactions tend to happen at human speeds since reactions usually require some form of analysis and the involvement of a decision maker.

2) Operational Reach

Maneuver in cyberspace has almost unlimited operational reach. "Operational reach is the distance over which military power can be concentrated and employed decisively" [10]. In kinetic operations, operational reach is limited by terrain and distance, but since distance is virtually meaningless in cyberspace, reach in cyber operations tends to be limited by the scale of maneuver and the ability of an element to shield its actions from enemy observation, detection and reaction.

3) Access and Control

Maneuver in cyberspace requires access to friendly, neutral and enemy systems and one of the main goals of maneuver in cyberspace is to gain access to these systems in order to facilitate follow-on operations such as exploitation of data, disruption of systems or to gain leverage. Gaining control of systems is synonymous with building forward bases in a kinetic operation. It allows an attacker to move the point of attack forward to systems that are not attributable to the initiating state and potentially escalates an attacker's privilege level relative to the ultimate target system or network.

4) Dynamic Evolution

The technology upon which cyberspace is based is constantly evolving. Recent years have seen rise to heavy use of web based applications, cloud computing, smart phones, and converging technologies. This ongoing evolution leads to constant changes in tactics, techniques and procedures used by both attackers and defenders in cyberspace. Methods that work today may not work tomorrow due to new and unforeseen technological advances. Unlike kinetic conflicts the battlefield terrain can shift presenting very little room for planning. Surveillance of the targets and defences can offer an advantage.

5) Stealth & Limited Attribution

Stealth and limited attribution have become the hallmarks of most attacks in cyberspace. Cyberspace is dominated by non-state, bad actors and sophisticated state actors that use the advantage of anonymity to mask their actions, making them unattributed [11]. Even large scale, overt attacks such as distributed denial of service (DDoS) attacks are most often difficult to attribute to a specific actor or state.

Every action that takes place in cyberspace is observable at some level. That being said, most actions are not observed in a meaningful way. This may be due limited sensor coverage, limited analysis capability or a number of other factors and it is these factors that assist attackers in hiding their attacks. Additionally, the ability to leapfrog from compromised system to compromised system makes attribution very difficult, especially when the systems in question are geographically dispersed in different international jurisdictions.

6) Rapid Concentration

In cyber space, attacks can rapidly build from a single source system to thousands or even tens of thousands of systems with little or no warning to the target system.

In kinetic operations, it is very difficult for an attacker to generate this type of mass with little or no warning, especially in the modern era of satellite imagery, radar, etc. In cyberspace, attackers can make use of botnets and crowd-sourcing to rapidly generate distributed mass effects that are especially effective in attacks like distributed denial of service attacks. This type of massing can also be used to hide more subtle attacks, distracting defenders who are attempting to restore services from these massed attacks while attackers conduct more covert penetration attacks.

7) Non-serial and Distributed

Maneuver in cyberspace allows attackers and defenders to simultaneously conduct actions across multiple systems at multiple levels of warfare. For defenders, this can mean hardening multiple systems simultaneously when new threats are discovered, killing multiple access points during attacks, collecting and correlating data from multiple sensors in parallel or other defensive actions. For attackers, this can mean simultaneously attacking numerous targets at multiple locations in parallel rather than engaging in serial attacks. "Serial attack is the old fashioned ebb and flow of battle. It is a linear concept where two adversaries engage in a series of attacks and counter attacks. In parallel attack, the point of attack is against multiple targets and the effects are non-linear" [12]. These non-linear effects can create serious dilemmas for defending units who often have limited resources to defend large numbers of systems. This is especially true when attackers focus their attacks at multiple levels generating tactical, operational and strategic effects simultaneously.

B. Basic Forms of Offensive Cyber Maneuver

Cyber Maneuver most differs from its kinetic counterparts in offensive operations. While the goal of maneuver, to secure positional advantages in respect to an enemy or competitor state, remains relatively consistent with kinetic maneuver, the means to do so is vastly different given that maneuver is conducted at machine speeds inside a virtual construct.

1) Exploitive Maneuver

Exploitive Maneuver is the process of capturing information resources in order to gain a strategic, operational or tactical competitive advantage. It is modern day espionage at its finest, but it is the use of this information in follow-on operations that makes it a valid and dangerous form of cyber maneuver. In this new warfighting domain, information is analogous to terrain and the capture of key information resources can lead to decisive results across the political, economic, financial or military spectrums. Unlike terrain on a kinetic battlefield, once captured, information resources cannot be retaken to regain an advantage. On the kinetic battlefield, a key piece of terrain captured by the enemy can potentially be counter-attacked and the advantage of holding that terrain regained for future operations. This is not true in the information environment when dealing with

sensitive data or information stores. Once critical information resources are exposed, the originating state often loses a significant competitive advantage and the gaining state utilizes these resources for its own purposes.

Over the course of the last decade, various nation-states have recognized the competitive advantage they can gain by harvesting the intellectual property and state secrets of competitor nations. Chief among these has been China which has been conducting large scale cyber operations to capture information resources. "China has made industrial espionage an integral part of its economic policy, stealing company secrets to help it leapfrog over U.S. and other foreign competitors to further its goal of becoming the world's largest economy" [13]. Additionally, there is some anecdotal evidence that suggests that China has used captured information resources to give it distinct advantages when engaging in diplomatic or corporate negotiations. A recent investigation in Canada linked Chinese hackers to intrusions at several law firms and government offices in an apparent effort to gain a strategic advantage in ongoing deal negotiations. "The investigation linked the intrusions to a Chinese effort to scuttle the takeover of Potash Corp. of Saskatchewan Inc. by BHP Billiton Ltd. as part of the global competition for natural resources" [14].

While espionage is certainly not new, cyberspace has enabled the capture and exploitation of information on an unprecedented scale. Given that information is analogous to terrain in cyberspace, it stands to reason that the processes involved in attacking and defending it must represent a key form of maneuver in cyber operations.

2) Positional Maneuver

Positional Maneuver is the process of capturing or compromising key physical or logical nodes in the information environment which can then be leveraged during follow-on operations. These nodes could be viewed as centers of gravity in the information environment and gaining logical control of these nodes will give the attacker key advantages and leverage during the escalation of conflict, especially in the case of war or other combat operations. "Leverage is used to impose a force's will on the enemy, increase the enemy's dilemma, and maintain the initiative" [15]. The logical nodes in question could be Supervisory Control and Data Acquisition (SCADA) systems, enemy command and control systems, systems designed to provide a common operational picture during combat operations or any other key system whose compromise at a key moment in battle could give the initiating force a decisive advantage.

A prime example of this kind of positional maneuvering could be intuited from the 2007 Israeli attack on a suspected nuclear reactor at Dayr az-Zawr, Syria. Israeli strike aircraft managed to fly into Syria without alerting Syrian air defense systems to carry out this raid. This was apparently accomplished through a combination of both electronic and cyber-attacks which caused all of Syria's air defense radar

systems to go offline for the duration of the raid [16]. Before the kinetic operation could be undertaken, the Israelis had to know that they could disrupt the systems in question. This implies that the Israelis had already gained the necessary level of access into these systems and had pre-positioned themselves to carry out this attack. They had to be confident they could disrupt these critical systems at the time of their choosing to ensure the success of the raid. The use of positional maneuver prior to the initiation of actual kinetic combat operations set them up for success and illustrates the potential decisive nature of this form of cyber maneuver, especially at the tactical and operational levels of war.

3) Infleuncing Maneuver

Influencing Maneuver is the process of using cyber operations to get inside an enemy's decision cycle or even to force that decision cycle though direct or indirect actions. This is a broad form of maneuver intended to gain and maintain information superiority and dominance and to maintain freedom of maneuver in cyberspace. Influencing maneuver is often used in conjunction with other forms of offensive maneuver. Influencing maneuver can be used in direct or indirect operations. A direct example of influencing maneuver could include actions such as compromising command and control systems and manipulating data subtly in order to degrade the confidence a commander has in his systems to slow down his decision cycles. Indirect actions might include feeding compromised and manipulated data to the media to force a desirable reaction from an enemy. Influencing maneuver falls heavily in the spectrum of traditional information operations but makes use of cyber maneuver to accomplish its objectives.

C. Basic Forms of Defensive Cyber Maneuver

To date, defensive maneuver in cyberspace generally resembles its kinetic counterparts. Perimeter defences, intrusion detection, and defense-in-depth is almost identical in concept whether executed in a kinetic defense or in the virtual world of cyberspace and the Deceptive Defense is somewhat akin to an ambush, luring in an attacker although for somewhat different purposes. The Moving Target Defense is unique to the cyberspace and relies on technical mechanisms that do not have a true analogy in the physical world.

Cyber defense is often seen as being much more difficult than offensive operations due to what is perceived as an asymmetric advantage on the side of the attacker. While that is largely true, the proper use of defensive maneuver can offset that advantage and allow defenders to regain the initiative. "Cyber defense seeks to anticipate and avoid threats, detect and defeat threats, survive and recover from attacks. In an analogy to the OODA loop, cyber defense seeks to operate inside the OODA loop of the threat" [17].

1) Perimeter Defense & Defense in Depth

Line Defense is the Maginot Line of cyberspace and like this historic example; it is highly susceptible to maneuver. The line defense is used by many organizations who spend resources protecting the perimeter of their network with firewalls, intrusion detection systems and other defensive measures but leave the interior of their networks relatively undefended. Defense in depth is mitigation strategy that attempts to mitigate the vulnerabilities of the line defense by hardening the interior of the network and individual systems as well. While defense in depth is a more effective strategy than a line defense, both these defensive formations suffer from the fact that they are fixed targets with relatively static defenses which an enemy can spend time and resources probing for vulnerabilities with little or no threat of retaliation.

2) Moving Target Defense

The Moving Target Defense, unlike the line defense discussed above, does not attempt to create impenetrable defensive rings to prevent attacks and protect resources. Instead, this form of defensive maneuver uses technical mechanisms to constantly shift certain aspects of targeted systems to make it much more difficult for an attacker to be able to identify, target and successfully attack a target. A Moving Target Defense attempts to "create, evaluate and deploy mechanisms and strategies that are diverse, continually shift, and change over time to increase complexity and costs for attacker, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency" [18]. Typically, Moving Target Defenses use one of three methods, Address Space Randomization, Instruction Set Randomization and Data Randomization, to attempt to thwart attacks although other forms of system diversification are currently being researched.

During the 2008 cyber-attacks against Georgia, the Georgian government demonstrated a rudimentary form of the Moving Target Defense by relocating its primary sites on servers in several other allied countries. "The Georgian government took an unorthodox step and sought cyberrefuge in the U.S., Poland and Estonia. Within the U.S., Georgia located its cybercapabilities on servers at Tulip Systems (TSHost) in Atlanta, Ga., and at Google in California. When Estonia experienced a cyberattack in 2007, it essentially defended in place; Georgia, on the other hand, maneuvered" [19]. By employing defensive maneuver, Georgia was able to maintain key government services in the face of a massive denial of service attack which was largely successful against its original Defense-in-Depth strategy.

3) Deceptive Defense

Deceptive maneuver is the cyberspace analogy to an ambush. Deceptive maneuver uses processes to lure an attacker in to committing actions which will reveal their methodology or assist the defender in attribution. An excellent example of this is the use of honeypots, purposely vulnerable systems designed to appeal to an attacker as an attractive target. The use of these types of systems can allow a defender to regain the initiative by stalling an attack, giving the defender time to gather information on the attack methodology and then adjusting other defensive systems to account for the attacker's tactics, techniques and procedures.

4) Counter Attack

The counter attack is another form of defensive maneuver and has a direct kinetic counterpart. While the concept of a counter attack is relatively straight forward, the execution of a counter attack in cyberspace is complicated by the difficulty of attribution and the fact that many attacks originate from compromised, third party systems. Taking these issues into account, counter attacks may prove necessary to restore critical operations even at the cost of disabling or damaging a compromised third party system. In situations where attribution has been established, the use of a counter attack can allow a defender to stall an attack and regain the initiative. Consider a situation in which the command and control server for a botnet has been identified. Conducting a counter attack against such a system could disrupt a distributed attack and allow the defender to restore operations.

4. SOVEREIGNTY ISSUES AND CYBER MANEUVER

Sovereignty can be defined as a state exercising authority and control over a given area or geographic region. In relation to sovereignty, cyberspace is informally considered a global commons, similar to the sea and air domains, in that it is considered to be outside the geographic jurisdiction of any particular state and is an internationally shared resource utilized for trade, communications and other uses. Cyberspace is also described as a borderless domain, but that is not an entirely accurate statement and there are a number of different means that states can and do use to justify sovereign control of portions of this domain.

A. Efforts to Define Borders in Cyberspace

A number of states such as China have begun filtering content at the logical borders of their portion of cyberspace and in doing so have created de facto borders by exercising control and authority over these virtual regions. Additionally, a number of states including the United States are currently exploring policies on how to define national borders in cyberspace [20]. This makes sense in both political and military contexts since it is currently difficult to cry foul for virtual

incursions when there is no formal policy defining what the United States considers to be its sovereign territory in this domain. However, individual states defining sovereignty in cyberspace have limited utility without international agreements acknowledging the right to sovereignty in this domain. Both the United States and Russia have publically declared that they reserve the right to respond to cyber-attacks using all means at their disposal to include traditional kinetic options. This implies that the current state of this issue is based more on right-by-might than any form of international consensus.

One difficulty in defining borders in cyberspace is that the physical geography of cyberspace does not even remotely match the logical geography. Every router, switch and device upon which the domain of cyberspace exists is physically located within a state. One could use this as an argument to use state borders as a map of cyber borders. In this model, all systems residing inside the United States and its territories would be considered to be with the sovereign control of the United States and attacks on these systems would represent a violation of that sovereignty and a hostile act. While this may seem like a simple and straight forward way to deal with this issue, it would leave many US systems unprotected when you consider the logical borders of US systems in cyberspace. "The United States Military operates a global, logical domain (Dot MIL) that spans over 88 countries in over 3,500 locations. This logical domain interconnects with more than 20,000 leased circuits and supports over 2.8 million users" [21]. Clearly the United States would consider an attack by a competitor state against its military systems, even those residing outside the United States, to be a hostile act. Therefore, simply relying on physical boundaries does not fully address the issue. However, the complexity involved in trying to establish logical borders is insurmountable. "There is no clear-cut way to establish a permanent or even semi-permanent cyberspace boundary using the logical boundary approach. The demarcation point would be in a constant state of fluctuation" [22]. Even with the current ambiguity over sovereignty in cyberspace, there are forms of cyber maneuver that could still be considered hostile acts and violations of sovereignty.

B. Violating Sovereignty in Cyberspace

Viewed in its current state, cyberspace resembles a vast frontier with millions of small enclaves, many of which are surrounded by defensive perimeters. While the Internet is sometimes described as borderless, this is more of a legal distinction involving "jurisdictional uncertainty and transcendence of international borders" [23]. In reality, the electronic perimeters of various enclaves do provide a version of borders that, in reference to maneuver, could have significant importance. It would be easy for a state to claim a violation of its sovereignty based on a cyber-attack on these enclaves, especially when these enclaves represent government or military organizations. The state in question has a vested interest in protecting these enclaves, and is exercising control and authority over them.

Consider a state which exercises positional maneuver to put a Remote Access Tool (RAT) into another state's SCADA systems, especially systems associated with critical infrastructure. While this action has not technically damaged these systems, the presence of this tool suggests a future intent to make illicit use of it in what might be a very damaging attack. This could be construed as a precursor to a first strike. Additionally consider if a state like Iran used exploitive maneuver to capture information on nuclear weapons technology from Israel or the United States. Such maneuver could easily trigger a kinetic response given the public policy these states have against allowing Iran to gain nuclear weapons. While the above examples are both fictitious, both illustrate how actions in this domain could be seen as violations of a state's sovereignty.

Another serious consideration in regards to sovereignty and cyber maneuver is the concept of neutral states. In kinetic operations, a state must generally get permission from another state if its maneuver will cross that state's physical borders. How does this translate to the cyberspace domain when virtually any action between states will involve crossing national, international, state and non-state boundaries on both the physical and logical levels? Additionally, maneuver and attacks often involve the use of third party, neutral systems to mask attribution and provide the initiating state plausible deniability for the actions it initiates. Translating this to an example in the physical world, imagine what the United States' response would be if Canada somehow managed to fire missiles at Mexico from Texas. Yet events like this happen constantly in the cyberspace domain and rely on stealth and limited attribution to avoid political recriminations.

As more states begin to explore the idea of sovereignty in cyberspace, its relevance to cyber maneuver will continue to grow in importance. However, until some consensus is reached in the international community as to whether there exists a right to sovereignty in cyberspace and on what basis borders will be defined; this will remain an area of ambiguity that can be exploited in cyber operations.

5. Analysis and Conclusions

The principle of maneuver remains an important warfighting principle in cyberspace, but there are significant differences that must be taken into account when defining this concept. Information is the currency of warfare in cyberspace. Maneuver is used in cyberspace to position and apply force to attack or defend information resources much as kinetic maneuver makes use of key terrain in the physical world. Unlike terrain however, the capture of information resources can have a much more lasting impact at all levels of engagement since once exposed, the value of information depends on its usefulness to both the attacker and defender. This value can represent a short term gain such as exposure of tactical plans, or could have an impact that spans years such as the exposure of highly classified technologies.

Like its kinetic counterpart, cyber maneuver is used to give an actor a position of advantage over its enemies. Unlike kinetic maneuver, it is also highly applicable to adversaries and competitor states, even if those states are political allies. Cyber operations have not been limited to enemy states battling each other. Allied states with competing economic and political agendas are undoubted using these tools to secure competitive advantages. Proper use of cyber maneuver allows a force to maintain freedom of action in the cyberspace domain and can lead to competitive advantages in economic, political and military strategies.

Initiative is vitally important to cyber maneuver since actions are far quicker than reactions in this domain. Losing the initiative in cyberspace can leave a force paralyzed as it tries to apply human analysis and decisions to actions that are happening at machine speeds. Unlimited operational reach combined with non-linear effect compound this issue and add to the complexity faced by decision makers when reacting to enemy maneuvers.

Sovereignty issues will play an important role in cyber maneuver as various states and the international community try to come to some consensus on whether the concept of borders are applicable to cyberspace and if so, how to define them. Current difficulties in determining attribution for attacks combined with legal ambiguity make it advantageous for attackers to operate outside their parent state's sovereign systems. Attackers have a vested interest in dispersing attack sources; however, this could potentially present some significant issues since it involves launching attacks from systems belonging to enemy, neutral, or even allied third parties. So long as the current status quo remains, this type of attack pattern will probably remain prevalent and cyber maneuver will take this into account. Should attribution become easier due to technology changes, or should the international community come to terms with sovereignty issues in cyberspace, this could lead to significant changes in how maneuver is conducted in cyberspace, especially in regard to use of third party systems as jump off points for attacks.

One of the most dominant characteristics of maneuver in cyberspace is the fact that blatantly hostile acts are often accomplished with little or no recrimination against the initiator due to anonymity and the difficult of attribution. In many cases, similar acts in the physical world would be easily considered acts of war. Consider the Stuxnet virus which is thought to have disabled or damaged approximately 1000 centrifuges at the Natanz Nuclear Facility in Iran [24]. Outside of accusations in the media, Iran has done little in the way of retribution for this attack. Had this attack been carried out kinetically, it is very likely that it would have resulted in retaliation against the initiating state although what form that retaliation would have taken remains open to debate.

As states around the world are building and developing cyber warfare programs, understanding how the principles of war apply to this new warfighting domain becomes increasingly important since it is these principles that strategists and

theorists use to develop strategy and doctrine. Maneuver has a critical role in this doctrine since maneuver is an integral tool that supports and enables other warfighting functions and principles. Maneuver is used to build mass, bypass strength, exploit vulnerability, gain and maintain the initiative and exploit success to achieve a state's tactical, operational and strategic objectives. While maneuver in cyberspace is uniquely different than its kinetic counterparts, its objective remains the same, to gain a position of advantage over a competitor and to leverage that position for decisive success. It is therefore important to continue to study and define the evolving principle of maneuver in cyberspace to ensure the success of operations in this new warfighting domain.

ACKNOWLEDGEMENTS

The author would like to gratefully acknowledge the efforts of Dr. Angelos Stavrou of George Mason University and Major André Abadie of the United States Army who assisted in the editorial review of this paper.

REFERENCES

[1] Joint Publication 3-0: Joint Operations, JP 3-0. Joint Chiefs of Staff, United States Department of Defense, Washington D.C., 2011, p. III-27.

[2] J. Markoff, "Before the Bunfire, Cyberattacks," The New York Times, Aug. 12, 2008; http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[3] J.N. Wasson, "Innovator or Imitator: Napoleon's Operational Concepts and the Legacies of Bourcet and Guibert," SAMS Monograph, School of Advanced Military Studies, Command and General Staff College, Fort Leavenworth, KS, 1998.

[4] M.J. Lyons, "Napoleon, 'Stonewall' Jackson, and Operational Art," Desaxx – Military History – Military Art – National Security, Sep. 7, 2010, http://desaxx.blogspot.com/2010/09/napoleon-stonewall-jackson-and.html.

[5] F. Zachar, "Strategic Maneuver: Defined for the Future Army," SAMS Monograph, School of Advanced Military Studies, Command and General Staff College, Fort Leavenworth, KS, 2000; http://cgsc.cdmhost.com/cdm/singleitem/collection/p4013coll3/id/576/rec/8.

[6] L. Wells II., "Maneuver in the Global Commons – The Cyber Dimension," SIGNAL Magazine, Dec. 2010; http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2472&zoneid=306.

[7] J.R. Boyd, "Patterns of Conflict," Project on Government Oversight, Defense and National Interest – John Boyd Compendium, 1986; http://dnipogo.org/john-r-boyd/.

[8] Marine Corps Doctrinal Publication 1-0: Marine Corps Operations, MCDP 1-0, Department of the Navy Headquarters, United States Marine Corps, Washington D.C., p. 6-3.

[9] R.C. Parks & D.P. Duggan, “Principles of Cyber Warfare,” IEEE Security & Privacy, vol. 9, no. 5, p. 31, Sep./Oct. 2011.
[10] Joint Publication 3-0: Joint Operations, JP 3-0. Joint Chiefs of Staff, United States Department of Defense, Washington D.C., 2011, p. III-28.
[11] J.R. Schilling, “Defining Our National Cyberspace Boundaries,” Masters Thesis, National War College, Washington D.C., 2010.
[12] P.K. Singh, “Maneuver in Cyberspace,” MMS Thesis, Command and Staff College, Marine Corps University, Quantico, VA.
[13] M. Riley & J Walcott, “China-Based Hacking of 760 Companies Shows Cyber Cold War,” Bloomberg, Dec. 14, 2011; http://mobile.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war?category=%2Fnews%2Findustries%2F.
[14] M. Riley & S. Pearson, “China-Based Hackers Target Law Firms to Get Secret Deal Data,” Bloomberg, Jan. 31, 2012; http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.
[15] Overview of Operational Art, Joint Electronic Library, Defense Technical Information Center, Joint Doctrine Reference Materials, [Online] Available: www.dtic.mil/doctrine/jrm/opart.doc.
[16] D.A. Fulghum & R. Wall, “U.S. Electronic Surveillance Monitored Israeli Attack on Syria,” Aviation Week, Nov. 14, 2007; http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=defense&id=news/ISRA112107.xml&headline=U.S.%20Electronic%20Surveillance%20Monitored%20Israeli%20Attack%20On%20Syria.
[17] K.T. Jabbour, “50 Cyber Questions Every Airman Can Answer,” Wright Patterson Air Force Base Public Affairs, Wright Patterson Air Force Base, Ohio, 2008; http://www.au.af.mil/au/awc/awcgate/afrl/50_cyber_questions.pdf.http://www.au.af.mil/au/awc/awcgate/afrl/50_cyber_questions.pdf.
[18] S. Jajodia, A.K. Ghosh, V. Swarup, C. Wang & X.S. Wang, Eds. New York, Springer Science + Business Media, 2011.
[19] S.W. Korns, “Botnets outmaneuvered,” Armed Forces Journal, Jan. 2009; http://www.armedforcesjournal.com/2009/01/3801084/.
[20] J.R. Schilling, “Defining Our National Cyberspace Boundaries,” Masters Thesis, National War College, Washington D.C., 2010.
[21] J.R. Schilling, “Defining Our National Cyberspace Boundaries,” Masters Thesis, National War College, Washington D.C., 2010.
[22] J.R. Schilling, “Defining Our National Cyberspace Boundaries,” Masters Thesis, National War College, Washington D.C., 2010.
[23] K.T. Jabbour, “50 Cyber Questions Every Airman Can Answer,” Wright Patterson Air Force Base Public Affairs, Wright Patterson Air Force Base, Ohio, 2008.
[24] D. Albright, P. Brannan & C. Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” Institute for Science and

International Security, Washington, D.C., Dec. 22, 2010; http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf.