AIR WAR COLLEGE

AIR UNIVERSITY

PRINCIPLES OF WAR FOR CYBERSPACE

by

Steven E. Cahanin, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

15 January 2011

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Biography

Lieutenant Colonel Cahanin entered the Air Force in 1982 as an Airman Basic, Lackland AFB, Texas. While enlisted, he was an Avionics Technician on both analog and digital avionics on B-52H and B-1B aircraft. In 1987 he entered the Airman Education and Commissioning Program where he earned his degree in Meteorology and subsequent commission through Officer Training School at Lackland AFB, Medina Annex in 1990. In 1995 he completed a Master of Science in Upper Atmospheric Physics through an AFIT/CI assignment to Utah State University. Since commissioning, he has been a Fighter Wing Weather Officer, Flight Commander, Chief of Engineering, Detachment Commander, Program Element Monitor for the Defense Meteorological Satellite Program, Director of Weather Operations at the Tanker Airlift Control Center, a Squadron Director of Operations, a Squadron Commander for the 321st and 326th Basic Military Training Squadrons, and the Chief, Information Systems Division for Air Force Recruiting Service where he was responsible for the Air Force Recruiting Information Support System and IT support to 3 recruiting groups and 24 recruiting squadrons world-wide.

Introduction

As the United States Air Force develops doctrine, education, and organization for cyberspace, we need to consider the traditional principles of war and how/if they apply to cyberspace, and under what situations, so we can develop a conceptual foundation for effective cyberspace warfighting doctrine. Most importantly, we should understand the cyberspace domain requires a new and different way of thinking to develop the most useful doctrine, education, and organizational structures. We must avoid falling into the trap of merely rewording existing air and space doctrine by simply replacing "air" or "space" with "cyber."

There are generally two predominant traditions for principles of war—the western view of Clausewitz and the eastern view of Sun Tzu. Clausewitz's western Newtonian world conceptualizes war using mass, objective, and maneuver among other principles in a state-on-state kinetic war for a political objective. However, Sun Tzu's eastern world conceptualizes war focusing on the criticality of intelligence, deception to defeat the mind of the enemy, and knowing that *relationships between things* matter most in the strategy of war. It is essential to examine which tradition is the best guide for developing cyber strategy; or do we need a combination?

When developing principles of war for cyberspace, I assert we should look to Clausewitz for guidance when kinetic force-on-force effects seem to be required, but also look to Sun Tzu for guidance because intelligence, deception, and the relationship between things in cyberspace requires a different way of thinking; where force-on-force is often less effective toward achieving our objective than appropriate non-kinetic methods. Sun Tzu's principles of intelligence estimates, deception, and disposition are important guides for non-kinetic cyberspace operations. Interestingly, the interconnection and integration of networks occur as the mind of

the commander—including things such as intelligence fusion centers and cyber support. And what better way to attack this mind than gathering intelligence through and using deception in cyberspace?

U.S. military doctrine, education, and organizational structures are currently focused primarily in the Clausewitzian tradition of warfare. In fact, the Air Force no longer teaches Sun Tzu's principles of war in the Air War College strategy class.[1] Unfortunately, while Clausewitz may apply to certain aspects of cyber war, his principles sometimes fall short, and when that happens we need to think differently.

Western military thinking tends to see the world in a Newtonian structure with clear cut physical laws, but cyberspace is different; yes, it has physical laws of electricity and magnetism, but the actual *domain* can be far more—with virtual and cognitive aspects not present in the other domains. Therefore, cyberspace war theory and doctrine must consider *the relationship of things*, i.e. the network, and how people have chosen to structure and use the cyberspace domain. The U.S. military has not yet developed a theory of war for cyberspace. And although it has recently published its first cyberspace doctrine, AFDD 3-12 *Cyberspace Operations*, the Air Force appears to be continuing its focus on Clausewitzian thinking as it did with air and space doctrine.

So there are fundamental issues to examine and questions to answer as we develop cyberspace doctrine, education, and organizational structure. First, we have to master the domain at a conceptual level, i.e. how do we view war in a world where "everything" can be connected to "everything"? This requires understanding whether traditional principles of war may apply in this new domain, or are different principles the ones we should follow? Secondly, does cyberspace require a different approach in educating cyber warriors? The complexity of

[1] Reference AWC 2010-2011 Strategy course syllabus.

cyberspace may require a different way of thinking about how we currently educate cyberspace warriors. We need to begin to *think* differently about cyberspace, for if we do not, we will likely fall back on comfortable Clausewitzian western thought, even when it is not in our best interest.

Assumptions

This analysis is grounded in three basic assumptions. First *cyberspace is a man-made domain* we must control for military operations to be successful across the other domains of land, sea, air, and space. Today, with few exceptions all other warfighting domains depend on cyberspace. This paper uses the DoD cyberspace definition in Joint Publication 1-02: "cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] However, these interconnections and capabilities bring with them the need to address the cognitive aspects of controlling and using the domain.

Secondly, *today's cyberspace targets can be penetrated or damaged by an attacker with enough determination and/or resources*. According to Dr. Kamal Jabbour, Air Force Senior Scientist for Information Assurance, current network defense policies and procedures have generally failed, and there are numerous examples of intrusions into our networks to provide sufficient support to this assumption.[3]

Finally, *cyberspace technology advancements will keep rapidly changing the domain*, requiring us to quickly adjust if we are to maintain freedom of action in cyberspace, both

[2] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (as amended 30 September 2010), 118.
[3] Dr. Kamal Jabbour, ST (SES), Air Force Senior Scientist for Information Assurance, "The Science and Technology of Cyber Warfare" (lecture, Army War College, Carlisle PA, 15 July 2010).

defensive and offensive.[4] New information technology is continually becoming available to the military, to the public, and to our opponents. Each new capability brings its own strengths and vulnerabilities. Software and hardware domain changes used to fix vulnerabilities can also create vulnerabilities. We must assume the cyberspace domain *will* continue to change and require flexible warfighting capabilities.

Cultures of Strategy and Cyberspace

To better understand the two schools of strategy we need to compare their cultures and ways of *thinking*. We can do this by contrasting western and eastern strategic thinking of Clausewitz versus Sun Tzu and the applicability to cyberspace.

Clausewitzian Cyberthink

Clausewitz's principles of war are based on a western Newtonian view of the world. Clausewitz states war is an act of force to compel our enemy to do our will, maximum use of force is required, the aim is to disarm the enemy, and the motive of war is the political objective.[5] Clausewitz additionally addresses the concepts of chance, luck, courage and intellect of the general; but eventually the bottom line is that war is a continuation of political intercourse carried on by what today we call kinetic force.

Interestingly, we can see Clausewitzian strategy in our western games. For example, chess is a power-based battle going after the king, poker requires bluffing and risk taking in a winner takes all battle, and American football in many ways resembles a battlefield that Clausewitz and American generals would be very familiar with. These are excellent examples of the very structured strategic environment which mirrors the Clausewitzian principles of war.

[4] Mike Lloyd, "The Silent Infiltrator," *Armed Forces Journal*, (June 2010).
[5] Carl von Clausewitz, On War, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75-81.

This way of thinking is ingrained in modern western military thought. The traditional western military way of thinking sees a pitched battle of winner takes all.

Clausewitz, however, had difficulties with irregular warfare because the western ways of warfare up to the nineteenth century did not experience this as a frequent occurrence.[6] Clausewitz viewed war in a world of state against state, with clear borders, to obtain a political objective, but in cyberspace this is not the case.[7] Cyberspace has no state borders. Ninety percent of the cyberspace structure is privately owned and a great number of world-wide internet hosts reside physically in the United States. [8] A cyber attacker could be located anywhere, whether state sponsored or not, and could even use cyberspace assets inside the U.S. to attack us—adding to the challenges of attribution.[9] But, none of this is to say that Clausewitz's principles are inappropriate when using kinetic force against an attacker's cyberspace assets such as network or computer facilities, *if attribution can be assigned*. In those cases using kinetic force to destroy the adversary's physical cyberspace assets may be appropriate, and be best guided by the traditional Clausewitzian principles of regular warfare, not cyber warfare.

Using solely Clausewitzian thinking, we could end up relegating operations in the cyberspace domain to facilitating network-centric operations in the other domains. This would put cyber assets in a supporting role to kinetic warfare—similar to the way airpower was first relegated to supporting land forces before it was discovered that air war had new aspects all its own. Today we're finding that cyberspace also has aspects all its own, ones that demand new ways of thinking. Sun Tzu's principles of war may help us with this new way of thinking and may often prove to be a better model for conflict/competition in cyberspace.

---

[6] Ibid., 479-483.
[7] Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: The MIT Press, 2001), 15.
[8] Rebecca Grant, *Rise of Cyberwar*, A Mitchell Institute Special Report (Mitchell Institute Press, 2008), 13.
[9] Martin C. Libicki, Cyberdeterrence and Cyberwar, (Santa Monica, CA: RAND, 2009), 41-52.

Sun Tzu Cyberthink

Sun Tzu said, "For one to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[10] Only if one understands this way of thinking can they fully appreciate Sun Tzu, otherwise his writings may appear overly simplistic to the western reader. A proper reading of Sun Tzu requires an understanding of Chinese culture and the word *shi*, which can mean many things including, "reality may be perceived as a particular deployment or arrangement of things to be relied on and worked to ones advantage."[11] To Sun Tzu, this concept was very clear, but to modern western military thinkers it might not be so obvious. Sun Tzu's principles of war are grounded in the concepts that all warfare is based on deception, that the general must attack the mind of the enemy, and kinetic weapons are only to be used when there is no alternative.[12] These concepts may be perfect for cyberspace, where an opponent can win without kinetic fighting.

Using our game analogy, Sun Tzu's way of thinking is akin to the oldest board game on Earth, *go*, which has its origins in China over 4,000 years ago.[13] Most certainly Sun Tzu was aware of this game in his time, and it is still played among children and adults in China today. *Go* is a simple two player game on a 19x19 line matrix board with white and black "stones," with each opponent placing one stone at a time. Each stone has no more value or power than the others, unlike chess pieces or poker cards. As the stones interact with each other they represent the "yin and yang penetrating each other's territory as the flow of water."[14] This game

[10] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith, (London: Oxford University Press, 1963), 77.
[11] Francios Jullien, *The Propensity of Things: Toward a History of Efficacy in China* (New York, NY: Zone Books, 1995, 15.
[12] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith, (London: Oxford University Press, 1963), 40-41.
[13] David Lai, Learning From the Stones: A Go Approach to Mastering China's Strategic Concepts, Strategic Studies Institute (Carlisle, PA: U.S. Army War College Press), May 2004), 2.
[14] Ibid., 7.

demonstrates the use of *shi* in a Sun Tzu like strategy, as the relationship of all the stones on the board is used to place the opponent at a disadvantage—the basis of a successful strategy in *go*.

As is often the case in war, in *go* it is difficult or impossible to win everything. The objective is to secure more territory than your opponent, and the rules of the game are such that overly aggressive actions often lead to disaster.[15] Sun Tzu understood these principles well. His principles of intelligence, deception, and the relationship between things can all be applied for success in *go*.

Clausewitzian principles of mass and maneuver are seen in western games of chess, poker, and football—and often in war. But cyberspace frequently resembles the fluid and relational aspects of *go*—needing a view of strategy more akin to Sun Tzu. We need to *think* differently about cyberspace to determine which principles of war to apply and when.

Yin and Yang in Cyberspace

We can use the idea of yin and yang to conceptualize the flow between applying the principles of Sun Tzu and Clausewitz in cyberspace. According to the Taoist philosophy, yin and yang are interdependent, cannot exist without each other, and everything can be described as either yin or yang. [16] We know there is interdependence between kinetic and non-kinetic warfare. Sun Tzu therefore could be looked at as the yin (i.e. non-kinetic) in cyberspace while Clausewitz as the yang (i.e. kinetic)—both dependent on each other, unable to exist without each other. The challenge as we develop cyberspace doctrine is to determine the appropriate use for both Sun Tzu and Clausewitz, and resist the temptation to revert to straight western thinking.

[15] Ibid., 12.
[16] *New World Encyclopedia*, s.v. "Yin and Yang" http://www.newworldencyclopedia.org/entry/Yin_and_yang.

We need both Sun Tzu and Clausewitz to work as the yin and yang to understand how to fight and win in this new domain.

Cyber Yin

Cyberspace doctrine best uses Sun Tzu's principles of war in the non-kinetic cyberwar environment—particularly intelligence and deception, and how the disposition of things matters. We must start, however, by understanding how different cultures might *think* about the cyberspace domain. How would they operate and fight in it? Countries have different doctrines based on different cultures. For example, Chinese and US cultural differences are significant, and understanding those differences is critical. According to the Geert Hofstede™ Cultural Dimensions Model, the Chinese culture has a very low individualism in addition to a very high long term outlook.[17] How might this knowledge help us in cyberspace? We must consider these cultural differences when examining how Sun Tzu might move us forward in using cyberspace.

The Taiwanese offer us insight into the Chinese perspective, as they are much more capable of identifying a Sun Tzu approach than a western analyst.[18] Taiwanese analysis says the Chinese are developing cyberspace operations and a network in the context of Sun Tzu—thinking of deception, psychological warfare, and the use of strategy as opposed to use of force.[19] For example, they are developing over a long timeline a network warfare capability where Chinese civilians would participate alongside the military as "network combatants."[20] In the event they get this doctrine correct, they could force us into a kinetic response or no response at all depending on our willingness to escalate. Once we understand that cyberspace requires a

[17] Geert Hofstede™ Cultural Dimensions Model, s.v. "Geert Hofstede," http://www.geert-hofstede.com/hofstede_dimensions.php?culture1=95&culture2=18.
[18] Timothy L. Thomas, Taiwan Examines Chinese Information Warfare, *High Frontier* 5, no. 3 (May 2009): 26-35.
[19] Ibid., 26-35.
[20] Ibid., 26-35.

different way of thinking, we can examine Sun Tzu's principles of intelligence and deception, and how the disposition of things matters in cyberspace.

Intelligence and deception are critical principles of war for cyberspace, and should be integrated into cyberspace doctrine and operations. Examples abound on how state and non-state actors are using these principles. An intelligence gathering example occurred with the probing of the U.S. military networks caused by the insertion of a thumb drive into a military laptop in the Middle East.[21] This thumb drive inserted a code that "spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead."[22] A cyberspace deception operation example is the 2006 Israeli/Hezbollah War, where Hezbollah used deception with great success.[23] A freelance photographer, siding with Hezbollah, took pictures after an Israeli attack and modified them using Photoshop to show more damage than was done. Approximately 920 of his doctored photos made their way onto the Reuters database and were used by global news services before he was caught and fired.[24] It is easy to see You Tube and other cyberspace capabilities can be used as a "Tet Offensive" where the opponent loses public support even though they may be winning a kinetic war. Therefore, intelligence and deception must be primary principles of war in cyberspace.

The concept of the *disposition of things* is also critical to cyberspace. This idea takes us back to the concept of *shi*, and the *potential born of disposition*. The potential born of disposition means the "general must aim to exploit, to his own advantage and to maximum effect, whatever conditions he encounters."[25] This means the disposition of things within the

[21] Ellen Nakashima, "Defense Official Discloses Cyberattack: Foreign agencies code on flash drive spread to Central Command," *Washington Post*, 25 August 2010.
[22] Ibid.
[23] Timothy L. Thomas, "Hezbollah, Israel, and Cyber PSYOP", IO Sphere (Winter 2007).
[24] Ibid.
[25] Francios Jullien, *The Propensity of Things: Toward a History of Efficacy in China* (New York, NY: Zone Books, 1995, 27.

cyberspace domain matters both in physical design and management. The physical design and use of cyberspace in our warfighting can give us either high or low efficacy, and how we use the cyberspace domain matters. The Chinese thinking during the Warring States period, between the fifth and third centuries B.C., was that war unfolding could be logically predicted and therefore managed, hence their strategic thought was they could *manage reality*[26]—something that is curiously interesting for cyberspace. Reality is in the eyes of the beholder, and can be *managed* in cyberspace as we see above with deception operations, but also by *changing the domain* as discussed next.

Changing the domain means our adversaries could set up a cyberspace domain (since it is man-made) completely different to what western states understand and/or prefer, and gain a significant potential advantage born of the *disposition of things* in cyberspace. This leads us to the concept of "cyber terrain." The Chinese among others have figured this out and are changing the cyber terrain to make access significantly more difficult.[27] For example, the Chinese have developed a more secure operating system completely unlike the western world in the hope they could change the cyber terrain and make it impenetrable to United States military or intelligence—and they have been doing this since 2001.[28] We, however, depend on the current cyber terrain in the United States and our enemies know this terrain very well. They navigate our cyber terrain with ease by taking advantage of foreign ownership of software and hardware technologies and our supply chain.[29]

---

[26] Ibid., 25.
[27] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency*, (Washington, DC: CSIS Report, December 2008), 26.
[28] Bill Gertz, "China Blocks U.S. From Cyber Warfare," *Washington Times*, 12 May 2009, http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/.
[29] AFDD 3-12, *Cyberspace Operations*, 15 July 2010, 4-5.

Sun Tzu writes about the five different kinds of terrain (entrapping, indecisive, constricted, precipitous, and distant) and the ability to use these terrains to his advantage.[30] I believe we can use this concept in cyberspace. Sun Tzu warns the commander about how to act in these different environments. Since our operations are connected across many cyber terrains (.com, .org, .edu, .mil, .smil, etc.), cyberspace warriors need to understand the differences of each just like a land warrior understands different terrains. A potential way to defend cyberspace is to *change the cyber terrain* to make it difficult or impossible for enemies to operate the way they need to.

Imagine if we could change the *physical* characteristics of air so our adversaries could not use existing aircraft. This is a far-fetched example for the air, but not for cyberspace. The action of changing the cyber terrain could negate the ability to operate within it. If the Chinese succeed at this, they could force us to revert to Clausewitzian kinetic options which may not be the best choice for our political objectives and may leave us with no good choices. Even so, there are times where Clausewitz may be the better or the only choice.

Cyber Yang

Cyberspace doctrine best uses Clausewitzian principles of war when kinetic warfare is involved. AFDD 3-12, *Cyberspace Operations*, is an excellent start toward developing this doctrine, but it is solely from the Airman's and Clausewitzian perspective. AFDD 3-12 states, "Just as air operations grew from its initial use as an adjunct to surface operations, space and cyberspace have likewise grown from their original manifestations as supporting capabilities into warfighting arenas in their own right."[31] Additionally, AFDD 3-12 uses the tenets of airpower

[30] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith, (London: Oxford University Press, 1963), 124-129.
[31] AFDD 3-12, *Cyberspace Operations*, 15 July 2010, 14.

and principles of joint operations and directly relates these to cyberspace.[32] All services are developing cyberspace doctrine and some may challenge AFDD 3-12 doctrinal claims, especially airman centric views. Furthermore, cyberwar will likely be fought *jointly* across all warfighting domains.

A strategic level cyberwar is likely to spill over into other domains and therefore require Clausewitzian kinetic operations against cyberspace assets. Rarely indeed is war fought in a single domain—all domains are interdependent, and therefore the new doctrine is bound to be heavy with cyberspace in a supporting role to kinetic war—just like airpower sometimes plays a supporting role. However, actions and challenges *centered* in cyberspace are different, and we need to open our minds to new ways to fight in the cyberspace domain just as early airpower theorists did for the air domain.

We need to consider that cyberwar may develop characteristics of traditional strategic coercion and deterrence against the United States. Some cyberspace theorists argue a strategic cyberwar can be fought solely in the cyber domain and coerce an enemy without violence.[33] However, others believe the coercive effect using strategic cyberwar solely in cyberspace are speculative at best since the attack would likely not cause enough damage to force a target state to concede defeat, and coercing non-state actors using cyber attack is practically impossible today due to the challenges with attribution.[34] Regardless, when considering coercion and deterrence or the need for it, currently there is no incentive for state actors to threaten strategic cyberwar against the United States since the major countries capable of launching such an attack

[32] Ibid., 16-19.
[33] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, (New York, NY: Frank Cass), 205-208.
[34] Martin C. Libicki, Cyberdeterrence and Cyberwar, (Santa Monica, CA: RAND, 2009), 137.

need the cyber domain to remain functioning for their own uses, and thus would be hurt too.[35] Since war tends to spill across domains, there is little reason to believe that future strategic war will contain itself to the cyberspace domain; therefore, Clausewitzian principles of war would then apply in combination with Sun Tzu's.

Clausewitzian kinetic principles of war in cyberspace doctrine must then account for the impacts of kinetically destroying cyberspace infrastructure. Adversary cyberspace assets, wherever they may be, could be very useful. For example, the Joint Force Commander might require a communications node, bridge, building, etc. be targeted, but what would be the impacts to cyberwar operations? Is there a critical need for that bridge because a fiber optic cable runs through it, a cable needed to communicate cessation of hostilities of for use in the recovery stage later? Would this destruction impact critical cyber operations? Who will advocate for the protection of these targets when necessary? Does this mean we need a Joint Force Cyber Component Commander? The initial Air Force cyberspace operations doctrine suggests this role should be assigned to the Joint Force Air Component Commander[36], but is that the best solution? Target deconfliction for cyberspace is critical where we may destroy a key infrastructure piece whose cyber importance is not obvious to a land, sea, or air component commander, not like a bridge or airfield they know we may need—so we need to get this correct.

Recommendations

This analysis leads me to two recommendations. First, we must develop doctrine using a Clausewitz and Sun Tzu combination for cyberspace kinetic and non-kinetic effects, sort of

[35] Carolyn Duffy Marsan, "How Close is 3.0?," Network World 24, no. 33 (August 2007): 4.
[36] AFDD 3-12, *Cyberspace Operations*, 15 July 2010, 28.

"ClauseTzu" principles of war. Secondly, due to the complex and ever changing nature of the cyberspace domain, we must pursue a rigorous cyber warrior education program.

ClauseTzu Cyberspace Doctrine

We must develop cyberspace doctrine using a combination of Sun Tzu principles of war for non-kinetic actions, and Clausewitz principles of war for kinetic actions. AFDD 3-12 is a good start on translating applicable Clausewitzian principles of war using cyberspace primarily in a supporting role. However, as I've shown, Sun Tzu's principles of war are often essential in cyberspace. It is not too late to develop cyberspace doctrine integrating those eastern principles of war. AFDD 3-12 is the first piece of cyberspace doctrine, and it has generally fallen back on reliance on traditional western thinking.

We must ensure cyberspace doctrine accounts for cyberspace's unique aspects, taking care to not simply borrow wholesale from the other domains and just replace "air" or "space" with "cyber." We therefore should integrate Sun Tzu's principles of intelligence, deception, and the disposition of things into cyberspace doctrine as this is exactly how war is being fought in cyberspace today, by default.

Cyberspace doctrine must include guidance to execute operations across the entire cyberspace domain. This includes how to interact with cyber terrain outside the military networks, since military operations are dependent on the *entire* cyberspace domain. This will require a Joint Force Cyber Component Commander to ensure cyber operations are integrated in warfighting—paying particular attention to target deconfliction (both between cyber targets and between cyber and kinetic targets) and legal issues. Obviously, there are legal aspects that must be considered and changed for the military to fight effectively in all cyber terrains, which affects

implementation of needed changes. Unfortunately, legal considerations/recommendations are beyond the scope of this paper.

As air doctrine had to develop separately from land doctrine, cyberspace doctrine must develop separately from air doctrine. Cyberspace war has already begun and it is being fought through deception, intelligence, and the disposition of things across the changing "cyber terrain." We would do well to integrate the best combination of principles into our cyberspace doctrine.

Cyberspace Education

This analysis has highlighted cyberspace complexity and continual change, and therefore calls for enhanced *education* in addition to training. This education would address understanding complex cyber theory and how to operate, fight, and win in cyberspace. While we are developing cyberspace doctrine we must accompany it with a concerted effort to better educate cyberspace warriors. Today we *train* most Air Force communications personnel in operating, maintaining, and monitoring the cyberspace domain. This needs to be taken to the next level through *educating* cyberspace warfighters, because education is different from training.

An analogy of *education* versus *training* for employing power in cyberspace is the comparison of a pilot and an aircraft mechanic. The pilot knows how to use the aircraft in the domain for warfighting, while the mechanic ensures the aircraft is available. Regarding cyberspace, we are currently spending most of our effort training network mechanics and neglecting the *education* of our cyber warriors.

Cyberspace requires a robust *education* for our cyber warriors. Cyberspace is extremely technically challenging, and it is continually physically changing (infrastructure, linkages and virtual spaces) much more rapidly and extensively than the other warfighting domains. This

education requires a high up-front investment that will provide a long-term benefit.[37] Education means acquiring the theoretical knowledge, ability to deal with uncertain futures, in addition to problem solving skills necessary for operating in the cyberspace domain.[38] We should,

- Create a cadre of cyber warrior officers similar to rated pilots and space operators
- Educate them in computer engineering, intelligence, and deception
- Educate them in "ClauseTzu" cyberspace doctrine

Employing cyberspace power will require highly educated cyber warriors who fully understand cyberspace and its strategic aspects and are able to continually adapt as the domain inevitably changes.

Conclusion

Fighting the next major war will certainly involve asymmetric attacks in cyberspace on the United States since that is currently an Achilles heel—as we are finding in current uses of cyberspace, especially the internet, by our non-state enemies as well as opponent states. We must understand the *threat* of cyber war. Non-state actors or individuals can attack a nation in cyberspace due to the low cost of entry as well as the attribution challenges. State actors will continue to pursue asymmetric advantages using cyberspace in future conflicts through intelligence gathering and deception operations as well as physical cyberspace attacks. We need to prepare for both defense and attack in cyberspace.

We can defend and possibly mend this weakness through understanding that cyberspace is *different*. Our potential adversaries know this. This requires new ways of thinking about war. We should understand the concept of *shi* and that the disposition of things in cyberspace matters.

[37] Dr. Kama Jabbour, ST (SES), Air Force Senior Scientist for Information Assurance, "The Science and Technology of Cyber Warfare" (lecture, Army War College, Carlisle PA, 15 July 2010).
[38] Ibid.

The principles of war outlined in Sun Tzu's *Art of War* can provide us guidance in situations where traditional Clausewitzian principles don't apply, or at least not as well.

Finally, we must *educate* a cadre of cyber warriors and organize/prepare them to fight effectively in cyberspace. These will be our warriors in the cyber domain just as our pilots are in the air. In the air domain, early airpower advocates like Billy Mitchell ensured airpower was not relegated to a support role—because he understood the air domain was different and it added new and unique roles and capabilities that had to be mastered and leveraged for us to fight effectively. Where is cyberspace's Billy Mitchell? Until he or she arrives, we might ask ourselves, "What would Sun Tzu do?"

Bibliography

Air Force Doctrine Document (AFDD) 3-12. *Cyberspace Operations*, 15 July 2010.

Air War College Academic Year 2010-2011 Strategy Course syllabus.

Geert Hofstede™ "Cultural Dimensions", http://www.geert-hofstede.com/hofstede_dimensions.php (accessed 13 Nov 2010).

Gertz, Bill. "China blocks U.S. from cyber warfare." *The Washington Times*, 12 May 2009.

Grant, Rebecca. *Rise of Cyber War*. A Mitchell Institute Special Report. Arlington, VA: Mitchell Institute, November 2008.

Griffith, Samuel (Translator). Sun Tzu: The Art of War. London: Oxford University Press, 1963.

Howard, Michael and Paret, Peter (Translators). Carl Von Clausewitz: On War. Princeton.: Princeton University Press, 1976.

Jabbour, Dr. Kamal, ST (SES), Air Force Senior Scientist for Information Assurance. Address. Combined/Joint Force Land Component Commanders Course, Army War College, Carlisle, PA, 15 July 2010.

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (as amended through 30 September 2010).

Jullien, Francios. The Propensity of Things: Toward a History of Efficacy in China, New York: Zone Books, 1995

Lai, David. Learning From the Stones: A *Go* Approach to Mastering China's Strategic Concept, *Shi*. Strategic Studies Institute, U.S. Army War College, 2004.

Libicki, Martin C. Cyberdeterrence and Cyberwar. Rand Corporation, 2009.

Lonsdale, David J. The Nature of War in the Information Age: Clausewitzian Future. New York: Frank Cass, 2004.

Lloyd, Mike. "The Silent Infiltrator," Armed Forces Journal, (June 2010).

Marsan, Carolyn Duffy. "How Close is World War 3.0?" Network World 24, no. 33 (August 2007): 1-5.

Nakashima, Ellen. "Defense Official Discloses Cyberattack: Foreign agency's code on flash drive spread to Central Command." *Washington Post*, 25 August 2010.

New World Encyclopedia. "Yin and Yang" http://www.newworldencyclopedia.org/entry/Yin_and_yang (accessed 6 November 2010).

Rattray, Gregory J. Strategic Warfare in Cyberspace. Cambridge: The MIT Press, 2001.

Thomas, Timothy L. "Hezbollah, Israel, and Cyber PSYOP." *IO Sphere* (Winter 2007): 30-35.

Thomas, Timothy L. "Taiwan Examines Chinese Information Warfare." *High Frontier* 5, no. 3 (May 2009): 26-35.

Securing Cyberspace for the 44th Presidency. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, DC: CSIS, December 2008.