Sun Tzu and Cyber War

Kenneth Geers

Naval Criminal Investigative Service (NCIS)

Cooperative Cyber Defence Centre of Excellence (CCD COE)

Tallinn, Estonia

Abstract

Cyberspace is a new warfare domain. Computers and the information they contain are prizes to be won during any military conflict. But the intangible nature of cyberspace can make victory, defeat, and battle damage difficult to calculate. Military leaders today are looking for a way to understand and manage this new threat to national security. The most influential military treatise in history is Sun Tzu's *Art of War*: its recommendations are flexible and have been adapted to new circumstances for over 2,500 years. This article examines whether *Art of War* is flexible enough to encompass cyber warfare. It concludes that Sun Tzu provides a useful but far from perfect framework for the management of cyber war, and urges modern military strategists to consider the distinctive aspects of the cyber battlefield.

What is Cyber Warfare?

The Internet, in a technical sense, is merely a large collection of networked computers. Humans, however, have grown dependent on 'cyberspace': the flow of information and ideas that they receive from the Internet on a continual basis, and immediately incorporate into their lives. As our dependence upon the Internet grows, what hackers think of as their potential 'attack surface' expands. The governance of national security and international conflict is no different: political and military adversaries now routinely use and abuse computers in support of strategic and tactical objectives. In the early 1980s, Soviet thinkers referred to this as the Military Technological Revolution (MTR); fol-

孫子兵法

lowing the 1991 Gulf War, the Pentagon's Revolution in Military Affairs (RMA) was practically a household term (Mishra, 2003).

Cyber attacks first and foremost exploit the power and reach of the Internet: since the earliest days of the Web, Chechen rebels have demonstrated the power of Internet-enabled propaganda（Goble, 1999). Second, they exploit its vulnerability: in 2007, Syrian air defense was reportedly disabled by a cyber attack moments before the Israeli air force demolished an alleged Syrian nuclear reactor (Fulghum et al, 2007). Third, cyber attackers benefit from a degree of anonymity: during the 1999 war over Kosovo, unknown hackers tried to disrupt NATO military operations, and were able to claim minor victories (Geers, 2008). Fourth, even a nation-state can be targeted: in 2009, the whole of Kyrgyzstan was knocked offline during a time of political crisis (Keizer, 2009). This list could be lengthened to include cyber warfare's high return on investment, an attacker's plausible deniability, the immaturity of cyber defense as a discipline, the increased importance of non-state actors in the Internet era, and more.

Cyber attacks are best understood as an extraordinary means to a wide variety of ends: espionage, financial damage, and even the manipulation of national critical infrastructures. They can influence the course of conflict between governments, between citizens, and between government and civil society.

What is *Art of War*?

Modern military doctrine draws from a deep well of philosophy that spans political, economic, and scientific revolutions. The oldest and most profound treatise is Sun Tzu's *Military Strategy*, known as *Art of War* (孫子兵法). Much of our current understanding of military concepts such as grand strategy, center of gravity, decisive point, and commander's intent can be traced to this book (Van Riper, 2006).

According to Chinese tradition, *Art of War* was written by Sun Wu (now Tzu) in the 6th century B.C., and is one of China's *Seven Military Classics*. Some scholars argue that gaps in logic and anachronisms in the text point to multiple authors and they contend that *Art of War* is a compilation of different texts that were brought together over time. Nonetheless, the book has an internal consistency which implies it is the product of one school of military thought. *Art of War* was translated for the West by a French missionary in 1782, and may have had an influence on the battlefield victories of Napoleon, who was likely familiar with its contents (Sawyer, 1994).

Art of War has survived for 2,500 years because its advice is not only compelling, but concise, easy to understand, and flexible. Sun Tzu does not give military leaders a concrete plan of action, but a series of recommendations that can be adapted to new circumstances. Sun Tzu's concepts have been successfully applied to disciplines other than warfare, including sports, social relationships, and business (Sawyer, 1994).

There are thirteen chapters in *Art of War*; each is dedicated to a particular facet of warfare. This paper highlights at least one topical passage from each chapter, and will argue that Sun Tzu provides a workable but not a perfect framework for the management of cyber war.

Strategic Thinking

Art of War opens with a warning:

> The Art of War is of vital importance to the State. It is a matter of life and death, a road either to safety or to ruin. Hence it is a subject of inquiry which can on no account be neglected. *AoW: I. Laying Plans*[1]

At the strategic level, a leader must take the steps necessary to prevent political coercion by a foreign power and to prevent a surprise military attack. Regarding offensive military operations, *Art of War* states that they are justified only in response to a direct threat to the nation; economic considerations, for example, are insufficient (Sawyer, 1994).

Cyberspace is such a new arena of conflict that basic defense and attack strategies are still unclear. There have been no major wars (yet) between modern, cyber-capable adversaries. Further, cyber warfare tactics are highly technical by nature, often accessible only to subject matter experts. As with terrorism, hackers have found success in pure media hype. As with Weapons of Mass Destruction (WMD), it is challenging to retaliate against an asymmetric threat. Attack attribution is the most vexing question of all: if the attacker can remain anonymous, defense strategies appear doomed from the start. Finally, the sensitive nature of cyber warfare capabilities and methods has inhibited international discussion on the subject and greatly increased the amount of guesswork required by national security planners.

The grace period for uncertainty may be running out. Modern militaries, like the governments and economies they protect, are increasingly reliant on IT infrastructure. In 2010, the United States Air Force will procure more unmanned than manned aircraft for the first time (Orton, 2009). IT investment on

[1] All Sun Tzu quotes are from Sun Tzu, *Art of War* (1994) Project Gutenberg eBook, translated by Lionel Giles in 1910).

this scale necessarily means an increased mission dependence on IT. As adversaries look for their opponent's Achilles Heel, IT systems will be attractive targets. It is likely that the ground-fighting of future wars will be accompanied by a parallel, mostly invisible battle of wits between state-sponsored hackers over the IT infrastructure that is required to wage war at all.

Celebrated Red Team exercises, such as the U.S. Department of Defense's Eligible Receiver in 1997, suggest that cyber attacks are potentially powerful weapons. During the exercise, simulated North Korean hackers, using a variety of hacker and information warfare tactics including the transmission of fabricated military orders and news reports, "managed to infect the human command-and-control system with a paralyzing level of mistrust … as a result, nobody in the chain of command, from the president on down, could believe anything" (Adams, 2001).

Because cyber warfare is unconventional and asymmetric warfare, nations weak in conventional military power are also likely to invest in it as a way to offset conventional disadvantages. Good hacker software is easier to obtain than a tank or a rifle. Intelligence officials such as former CIA Director James Woolsey warn that even terrorist groups will possess cyber weapons of strategic significance in the next few years (Aitoro, 2009).

Some analysts argue persuasively that the threat from cyber warfare is overstated.[2] However, national security planners cannot afford to underestimate its potential. A general rule could be that as dependence on IT and the Internet grows, governments should make proportional investments in network security, incident response, technical training, and international collaboration.

In the near term, international security dialogue must update familiar vocabulary such as attack, defense, deterrence and escalation to encompass post-IT Revolution realities. The process that began nearly thirty years ago with MTR and RMA continues with the NATO Network Enabled Capability

[2] Two are Cambridge University Professor Ross Anderson and *Wired* Threat Level Editor Kevin Poulsen.

(NNEC), China's *Unrestricted Warfare*, and the creation of U.S. Cyber Command. However, the word cyber still does not appear in NATO's current Strategic Concept (1999), so there remains much work to do. A major challenge with IT technology is that it changes so quickly it is difficult to follow – let alone master – all of the latest developments.

From a historical perspective, it is tempting to think cyber warfare could have a positive impact on human conflict. For example, Sun Tzu advised military commanders to avoid unnecessary destruction of adversary infrastructure.

> In the practical *Art of War*, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to recapture an army entire than to destroy it, to capture a regiment, a detachment or a company entire than to destroy them. *AoW: III. Attack by Stratagem*

If cyber attacks play a lead role in future wars, and the nature of the fight is largely over IT infrastructure, it is conceivable that international conflicts will be shorter and cost fewer lives. A cyber-only victory could facilitate economic recovery and post-war diplomacy. Such an achievement would please Sun Tzu, who argued that the best leaders can attain victory before combat is even necessary (Sawyer, 1994).

> Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting. *AoW: III. Attack by Stratagem*

But there is no guarantee that the increased use of cyber warfare will lead to less human suffering during international conflicts. If national critical infrastructures such as water or electricity are damaged for any period of time, what caused the outage will make little difference to those affected. Military leaders are specifically worried that cyber attacks could have unforeseen 'cascading' effects that would inadvertently lead to civilian casualties, violate the Geneva Convention and bring war crimes charges (Graham, 1999). The anonymous nature of cyber attacks also leads to the disturbing possibility of unknown and therefore undeterred hackers targeting critical infrastructures during a time of peace for purely terrorist purposes.

Cultivating Success

Due to the remarkable achievements of cyber crime and cyber espionage[3] – as well as plenty of media hype – cyber warfare will be viewed by military commanders as both a threat and an opportunity. But the most eloquent passages from *Art of War* relate to building a solid defense, and this is where a cyber commander must begin.

> The *Art of War* teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable. *AoW: VIII. Variation in Tactics*

Sun Tzu advises commanders not to rely on the good intentions of others, or to count on best-case scenarios (Sawyer, 1994). In cyberspace, this is sound advice: computers are attacked from the moment they connect to the Internet (Skoudis, 2006). Cyber attackers currently have numerous advantages

[3] Many examples could be cited here, such as ("Espionage Report…" 2007; Cody, 2007).

over defenders, including worldwide connectivity, vulnerable network infrastructure, poor attacker attribution, and the ability to choose their time and place of attack.

Defenders are not without resources. They own what should be the most powerful asset in the battle – home-field advantage – and they must begin to use it more wisely. Defenders have indigenous 'super-user' rights throughout the network, and they can change hardware and software configurations at will. They can build redundancy into their operations and implement out-of-band cross-checking of important information. Such tactics are essential because cyber attack methods evolve so quickly that static, predictable defenses are doomed to fail. A primary goal should be to create a unique environment that an attacker has never seen before. This will require imagination, creativity, and the use of deception.

> Hence that general is skillful in attack whose opponent does not know what to defend; and he is skillful in defense whose opponent does not know what to attack. *AoW: VI. Weak Points and Strong*

Adversary cyber reconnaissance should be made as difficult as possible. Adversaries must have to work hard for their intelligence, and they should doubt that the information they were able to steal is accurate. Attackers should be forced to lose time, wander into digital traps, and betray information regarding their identity and intentions.

> Thus one who is skillful at keeping the enemy on the move maintains deceitful appearances, according to which the enemy will act. He sacrifices something, that the enemy may snatch at it. By holding out baits, he keeps him on the march; then with a body of picked men he lies in wait for him. *AoW: V. Energy*

As in athletics, cyber warfare tactics are often related to leverage. In an effort to gain the upper hand, both attackers and defenders attempt to dive deeper than their opponent into files, applications, operating systems, compilers, and hardware. Strategic attacks even target future technologies at their source: the research and development networks of software companies or personnel working in the defense industry.

> The general who is skilled in defense hides in the most secret recesses of the earth… *AoW: IV. Tactical Dispositions*

In fact, professional hacker tools and tactics are stealthy enough that a wise system administrator should presume some level of system breach at all times. Defenses should be designed on the assumption that there is always a digital spy somewhere in the camp.

One of the first challenges in cyber warfare is simply to know if you are under attack. Therefore, a good short-term cyber defense goal is to improve an organization's ability to collect, evaluate, and transmit digital evidence.

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. *AoW: III. Attack by Stratagem*

In the late 1990's, Moonlight Maze, the "largest cyber-intelligence investigation ever," uncovered wide-ranging attacks targeting U.S. technical research, government contracts, encryption techniques, and war-planning data. Despite years of effort, law enforcement was able to find "disturbingly few clues" to

help determine attribution.[4] And because cyber warfare is a new phenomenon that changes so quickly, it is difficult even for law enforcement officers to be sure they are operating within the constraints of the law.

A long-term national objective should be the creation of a Distant Early Warning Line for cyber war. National security threats such as propaganda, espionage, and attacks on critical infrastructure have not changed, but they are now Internet-enabled. Adversaries have a new delivery mechanism that can increase the speed, diffusion, and even the power of an attack.

> Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. *AoW: XIII. The Use of Spies*

Because IT security is a highly technical discipline, a broader organizational support structure must be built around it. To understand the capabilities and intentions of potential adversaries, such an effort must incorporate the analysis of both cyber and non-cyber data points. Geopolitical knowledge is critical. Whenever international tension is high, cyber defenders must now take their posts. In today's Middle East, it is safe to assume that cyber attacks will always accompany the conflict on the ground: in 2006, as fighting broke out between Israel and Gaza, pro-Palestinian hackers denied service to around 700 Israeli Internet domains (Stoil and Goldstein, 2006).

Information collection and evaluation was so important to Sun Tzu that the entire final chapter of *Art of War* is devoted to espionage. Spies are called the "sovereign's most precious faculty" and espionage a "divine manipulation of the threads." The cost of spying, when compared to combat operations, is said to be so low that it is the "height of inhumanity" to ignore it; such a com-

[4] Russian telephone numbers were eventually associated with the hacks, but the U.S. was unable to gain further attribution (Adams, 2001).

mander is "no leader of men, no present help to his sovereign, no master of victory."[5]

In the wars of the future, brains will beat brawn with increasing frequency. Following the IT Revolution, the need for investment in human capital has risen dramatically. However, cyber defense is still an immature discipline, and it is difficult to retain personnel with highly marketable training. To gain a long-term competitive advantage, a nation must invest in science and technology as a national priority (Rarick, 1996).

Objective Calculations

Sun Tzu warns that a commander must exhaustively and dispassionately analyze all available information. Offensive operations in particular should wait until a decisive victory is expected. If objective calculations yield an unfavorable result, the inferior party must assume a defensive posture until circumstances have changed in its favor (Sawyer, 1994).

> Now the general who wins a battle makes many calculations in his temple ere the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose. *AoW: I. Laying Plans*

In any conflict, there are prevailing environmental and situational factors over which the combatants have little control. *Art of War* lists over three dozen such factors to evaluate, including offense/defense, ortho-

[5] Sun Tzu, *Art of War*: XIII. The Use of Spies.

dox/unorthodox, rested/exhausted, dry/wet, and confident/afraid (Sawyer, 1994). Most of these will have direct or indirect parallels in cyberspace.

In cyberspace, reliable calculations are extremely difficult to perform. First and foremost, cyber attackers possess enough advantages over defenders that there is an enormous gap in Return-on-Investment (RoI) between them. The cost of conducting a cyber attack is cheap, and there is little penalty for failure. Network reconnaissance can be conducted, without fear of retaliation, until a suitable vulnerability is found. Once an adversary system is compromised and exploited, there are often immediate rewards. By comparison, cyber defense is expensive, challenging, and there is no tangible RoI.

Another aspect of cyberspace that makes calculation difficult is its constantly changing nature. The Internet is a purely artificial construct that is modified continually from across the globe. Cyber reconnaissance and intelligence collection are of reliable valuable to a military commander only for a short period of time. The geography of cyberspace changes without warning; software updates and network reconfiguration create an environment where insurmountable obstacles and golden opportunities can appear and disappear as if by magic. The terrestrial equivalent could only be a catastrophic event such as an earthquake or an unexpected snowstorm.

Art of War describes six types of battlefield terrain, ranging from "accessible," that can be freely traversed by both sides, to "narrow passes," which must either be strongly garrisoned or avoided altogether (unless the adversary has failed to fortify them).[6] Although they will change over time, cyber equivalents for each *Art of War* terrain type are easily found in Internet, intranet, firewall, etc.

> The natural formation of the country is the soldier's best ally; but a power of estimating the adversary, of controlling the forces of victory, and of shrewdly calculating difficulties, dan-

[6] Sun Tzu, *Art of War*: X. Terrain.

gers and distances, constitutes the test of a great general. *AoW: X. Terrain*

Cyberspace possesses characteristics that the *Art of War* framework does not encompass. For example, in cyberspace the terrestrial distance between adversaries can be completely irrelevant. If 'connectivity' exists between two computers, attacks can be launched at any time, from anywhere in the world, and they can strike their targets instantly. There is no easily defined 'front line': civilian and military zones on the Internet often share the same space, and military networks typically rely on civilian infrastructure to operate. With such amazing access to an adversary, never before in history has superior logic – not physical size or strength – more often determined the victor in conflict.

Similar to cyber geography, cyber weapons also have unreliable characteristics. Some attacks that hackers expect to succeed fail, and vice versa. Exploits may work on one, but not another, apparently similar target. Exploits that work in one instance may never work again. Thus, it can be impossible to know if a planned cyber attack will succeed until the moment it is launched. Cyber weapons should be considered single-use weapons, because defenders can reverse-engineer them to defend their networks or try to use them for their own offensive purposes. These limitations make meticulous pre-operational cyber attack planning and timing critical (Parks and Duggan, 2001; Lewis, 2002).

Last but not least, one of the major challenges confronting any military commander is to keep track of the location and constitution of adversary forces. However, cyber defenses such as passive network monitoring devices can be nearly impossible to find.

If in the neighborhood of your camp there should be any hilly country, ponds surrounded by aquatic grass, hollow basins

> filled with reeds, or woods with thick undergrowth, they must be carefully routed out and searched; for these are places where men in ambush or insidious spies are likely to be lurking. *AoW: IX. The Army on the March*

Cyber commanders are wise to assume, especially if they are conducting an offensive operation on adversary terrain, that the defenses and traps they can see are more powerful than they appear, and that there are some defenses in place that they will never find. Adversary sensors could even lie on the open Internet, such as on a commercial Internet Service Provider (ISP), outside of the cyber terrain that the adversary immediately controls.

Time to Fight

Once the decision to go to war has been made (or forced), Sun Tzu offers plenty of battlefield advice to a military commander. *Art of War* operations emphasize speed, surprise, economy of force, and asymmetry. These characteristics happen to be synonymous with cyber warfare.

> Rapidity is the essence of war: take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots. *AoW: XI. The Nine Situations*

> If you set a fully equipped army in march in order to snatch an advantage, the chances are that you will be too late. On the other hand, to detach a flying column for the purpose involves the sacrifice of its baggage and stores. *AoW: VII. Maneuvering*

The potential role of computer network operations in military conflict has been compared to strategic bombing, submarine warfare, special opera-

tions forces, and assassins (Parks and Duggan, 2001).The goal of such unorthodox, asymmetric attacks is to inflict painful damage on an adversary from a safe distance or from close quarters with the element of surprise.

> By discovering the enemy's dispositions and remaining invisible ourselves, we can keep our forces concentrated, while the enemy's must be divided…Hence there will be a whole pitted against separate parts of a whole, which means that we shall be many to the enemy's few. *AoW: VI. Weak Points and Strong*

In theory, a cyber attack can accomplish the same objectives as a special forces raid, with the added benefit of no human casualties on either side. If cyber attacks were to achieve that level of success, they could come to redefine elegance in warfare.

A cyber attack is best understood not as an end in itself, but as an extraordinary means to accomplish almost any objective. Cyber propaganda can reach the entire world in seconds via online news media; cyber espionage can be used to steal even nuclear weapons technology (Gerth and Risen, 1999); a successful cyber attack on an electrical grid could bring down myriad other infrastructures that have no other source of power (Divis, 2005); and in 2008 and 2009 hackers were even able to force entire nation-states offline. (Keizer, 2008; Keizer, 2009). A good analogy from *Art of War* is in the way Sun Tzu describes the military use of fire.

> There are five ways of attacking with fire. The first is to burn soldiers in their camp; the second is to burn stores; the third is to burn baggage trains; the fourth is to burn arsenals and magazines; the fifth is to hurl dropping fire amongst the enemy. *AoW: XII. The Attack by Fire*

Sun Tzu did not know that baggage trains would one day need functioning computers and uncompromised computer code to deliver their supplies on time.

Specific tactical advice from *Art of War* provides a clear example. As in the Syrian air defense attack cited above, Sun Tzu instructs military commanders to accomplish something for which digital denial-of-service (DoS) appears ideal: to sever communications between adversary military forces.

> Those who were called skillful leaders of old knew how to drive a wedge between the enemy's front and rear; to prevent co-operation between his large and small divisions; to hinder the good troops from rescuing the bad, the officers from rallying their men. *AoW: XI. The Nine Situations*

If modern military forces use the Internet as their primary means of communication, what happens when the Internet is down? Thus it is likely that cyber attacks will play their most critical role when launched in concert with a conventional military (or terrorist) attack.

Sun Tzu warns that surprise attacks may come when a defender's level of alert is lowest:

> Now a soldier's spirit is keenest in the morning; by noonday it has begun to flag; and in the evening, his mind is bent only on returning to camp. A clever general, therefore, avoids an army when its spirit is keen, but attacks it when it is sluggish and inclined to return. This is the art of studying moods. *AoW: VII. Maneuvering*

Cyber criminals already operate according to this rule. They know the work schedules of network security personnel, and often launch attacks in the evening, on weekends or on holidays, when their adversaries are at home.

If an invasion is successful, Sun Tzu advises military commanders to survive as much as possible on the adversary's own resources.

> Hence a wise general makes a point of foraging on the enemy. One cartload of the enemy's provisions is equivalent to twenty of one's own, and likewise a single picul of his provender is equivalent to twenty from one's own store. *AoW: II. Waging War*

In this sense, *Art of War* and cyber warfare correspond perfectly. In computer hacking, attackers typically steal the credentials and privileges of an authorized user, after which they effectively become an insider, in the adversary's (virtual) uniform. At that point, inflicting further damage on the network – and thus on the people using that network and their mission – through DoS or espionage is far easier. Such attacks could include poisoned pen correspondence and/or critical data modification. Even if the compromise is discovered and contained, adversary leadership may lose its trust in the computer network, and cease to use it voluntarily.

Finally, cyber warfare is no different from other military disciplines in that the success of an attack will depend on keeping its mission details a secret.

> O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence we can hold the enemy's fate in our hands. *AoW: VI. Weak Points and Strong*

In military jargon, this is called operational security (OPSEC). However, the characteristics that make cyber warfare possible – the ubiquity and intercon-

nected nature of the Internet – ironically make good OPSEC more difficult than ever to achieve. Open source intelligence (OSINT) and computer hacking can benefit cyber defense as much as cyber offense.

The Ideal Commander

Decision-making in a national security context carries significant responsibilities because lives are often at stake. Thus, on a personal level, *Art of War* leadership requirements are high.

> The Commander stands for the virtues of wisdom, sincerity, benevolence, courage and strictness. *AoW: I. Laying Plans*

Good leaders not only exploit flawed plans but flawed adversaries (Parks and Duggan, 2001). Discipline and self-control are encouraged; emotion and personal desire are discouraged.[7] Sun Tzu states that to avoid a superior adversary is not cowardice, but wisdom (Sawyer, 1994), and due to the painstaking nature of objective calculations, patience is a virtue.

> Thus it is that in war the victorious strategist only seeks battle after the victory has been won, whereas he who is destined to defeat first fights and afterwards looks for victory. *AoW: IV. Tactical Dispositions*

Commanding a cyber corps will require a healthy mix of these admirable qualities. As a battleground, cyberspace offers political and military leaders almost limitless possibilities for success – and failure. Behind its façade of global connectivity and influence, the Internet has a complicated and vulnerable architecture that is an ideal environment in which to conduct asymmetric

[7] Sun Tzu, *Art of War*: VIII. Variation in Tactics.

and often anonymous military operations. Imagination and creativity are required skill sets. Cyber warfare also involves an enormous amount of uncertainty: even knowing *whether* one is under attack can be an immense challenge. And the high tempo of Internet operations may lead to a high burn-out rate throughout the ranks.

A cyber commander must have a minimum level of subject matter expertise in IT. The core concepts of computing, networking, and data security should be thoroughly understood before employing them in support of a national security agenda. Any leader must be able to articulate the mission so that everyone in the organization understands and believes in it (Rarick, 1996); a further challenge in cyber warfare will be communicating with highly technical personalities who have vastly different personal needs than the soldiers of a traditional military element.

In all future wars, military leadership will have the challenge of coordinating and deconflicting the cyber and non-cyber elements of a battle plan. Sun Tzu gives high praise for a great tactician:

> Having collected an army and concentrated his forces, he must blend and harmonize the different elements thereof before pitching his camp. After that, comes tactical maneuvering, than which there is nothing more difficult. The difficulty of tactical maneuvering consists in turning the devious into the direct, and misfortune into gain. *AoW: VII. Maneuvering*

As circumstances change throughout the course of a conflict, both tactics and strategy must be reevaluated and modified to fit the new environment (Rarick, 1996).

> He who can modify his tactics in relation to his opponent and thereby succeed in winning, may be called a heaven-born captain. *AoW: VI. Weak Points and Strong*

The dynamic nature of the Internet and the speed of computer network operations guarantee that traditional military challenges such as seizing the initiative and maintaining momentum will require faster decision cycles than a traditional chain-of-command can manage. A cyber commander must have the ability and the trust of his or her superiors to act quickly, creatively, and decisively.

Art of Cyber War: Elements of a New Framework

Art of War is the most influential military treatise in human history. The book has survived over 2,500 years in part because its guidance is highly flexible: strategists and tacticians have adapted *Art of War* to new circumstances across many scientific revolutions, and Sun Tzu's insight has never lost much of its resonance.

This paper argues that in the future, cyber warfare practitioners should also use *Art of War* as an essential guide to military strategy. However, cyberspace possesses many characteristics that are unlike anything Sun Tzu could have imagined in ancient China. There are at least ten distinctive aspects of the cyber battlefield.

1. The Internet is an artificial environment that can be shaped in part according to national security requirements.
2. The rapid proliferation of Internet technologies, including hacker tools and tactics, makes it impossible for any organization to be familiar with all of them.

3. The physical proximity of adversaries loses much of its relevance as cyber attacks are launched without regard to terrestrial geography.
4. Frequent software updates and network reconfiguration change Internet geography unpredictably and without warning.
5. In a reversal of our historical understanding of warfare, the asymmetric nature of cyber attacks strongly favors the attacker.
6. Cyber attacks are more flexible than any weapon the world has seen: they can be used for propaganda, espionage, and the destruction of critical infrastructure.
7. Cyber attacks can be conducted with such a high degree of anonymity that defense strategies such as deterrence and retaliation are not credible.
8. It is possible that a lengthy and costly cyber war could take place without anyone but the direct participants knowing about it (Libicki, 2009).
9. The intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking.
10. There are few moral inhibitions to cyber warfare because it relates primarily to the use and exploitation of information in the form of computer code and data packets; so far, there is little perceived human suffering.

None of these characteristics of cyberspace or cyber conflict fits easily into Sun Tzu's paradigm. As national security thinkers and military strategists begin to write concepts, strategies, and doctrine for cyber warfare with the *Art of War* model in mind, they should be aware of these differences.

References

Adams, J. (2001). Virtual Defense. Foreign Affairs, 80(3), 98-112.

Aitoro J. R. (2009, Oct 2). Terrorists nearing ability to launch big cyberattacks against U.S. Nextgov. Retrieved November 24 2010 from nextgov Web site: http://www.nextgov.com.

Cody, E. (2007, Sep 13) Chinese Official Accuses Nations of Hacking. Washington Post. Retrieved November 24 2010 from Washington Post Web site: http://www.washingtonpost.com.

Divis, D. A. (2005, Mar 9) Protection not in place for electric WMD. UPI. Retrieved November 24 2010 from UPI Web site: www.upi.com.

Espionage Report: Merkel's China Visit Marred by Hacking Allegations. (2007, Aug 27). Spiegel. Retrieved November 24 2010 from Spiegel Web site: www.spiegel.com.

Fulghum, D. A., Wall, R., & Butler, A. (2007). Cyber-Combat's First Shot. Aviation Week & Space Technology 167(21), 28.

Geers, K. (2008, Aug 27) Cyberspace and the Changing Nature of Warfare. SC Magazine. Retrieved November 24 2010 from SC Magazine Web site: www.scmagazineus.com.

Gerth, J. and Risen, J. (1999, May 2). 1998 Report Told of Lab Breaches and China Threat. The New York Times. Retrieved November 24 2010 from New York Times Web site: www.nytimes.com

Goble, P. (1999, Oct 9) Russia: Analysis from Washington: a Real Battle on the Virtual Front. Radio Free Europe/Radio Liberty. Retrieved November 24 2010 from Radio Free Europe/Radio Liberty Web site: www.rferl.org.

Graham, B. (1999, Nov 8). Military Grappling with Guidelines for Cyber Warfare; Questions Prevented Use on Yugoslavia. The Washington Post. Retrieved November 24 2010 from Washington Post Web site: www.washingtonpost.com.

Keizer, G. (2009, Jan 28). Russian ‘cyber militia’ knocks Kyrgyzstan offline. Computerworld. Retrieved November 24 2010 from Computerworld Web site: www.computerworld.com.

Keizer, G. (2008, Aug 11). Cyber Attacks Knock out Georgia’s Internet Presence. Computerworld. Retrieved November 24 2010 from Computerworld Web site: www.computerworld.com.

Lewis, J. A. (2002, December). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies (CSIS). Retrieved November 24 2010 from CSIS Web site: www.csis.org.

Libicki, M. C. (2009). Sub Rosa Cyber War. In C. Czossek & K. Geers (Eds.), The Virtual Battlefield: Perspectives on Cyber Warfare (pp. 53-65). Amsterdam, Netherlands: IOS Press.

Mishra, S. (2003). Network Centric Warfare in the Context of ‘Operation Iraqi Freedom.’ Strategic Analysis, 27(4), 546-547.

Orton, M. (2009, Jan 14). Air Force remains committed to unmanned aircraft systems. U.S. Air Force. Retrieved November 24 2010 from U.S. Air Force Web site: www.af.mil.

Parks, R. C. & Duggan, D. P. (2001). Principles of Cyber-warfare. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.

Rarick, C. A. (1996). Ancient Chinese advice for modern business strategists. S.A.M. Advanced Management Journal, 61(1), 42.

Sawyer, R. D. (1994). Sun Tzu: Art of War. Oxford: Westview Press.

Skoudis, E. (2006). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. New Jersey: Prentice Hall.

Stoil, R. A. & Goldstein, J. (2006, Jun 28). One if by land, two if by modem. The Jerusalem Post. Retrieved November 24 2010 from Jerusalem Post Web site: www.jpost.com.

Van Riper, P. K. (2006). Planning for and Applying Military Force: an Examination of Terms. U.S. Army War College: Strategic Studies Institute.