



Sun Tzu and the Art of Cyberwar

Roy Wilson

Sun Tzu is widely recognized as the premier military strategist in the history of the world. His book “The Art of War” was written approximately 2,500 years ago in China but its strategic and tactical information remains widely recognized as valid for modern warfighters. It has influenced the strategic and tactical thinking of military leaders such as America’s Gen. Douglas MacArthur, China’s Mao Zedong and Vietnam’s Gen. Vo Nguyen Giap.

Modern warfare historically has been conducted in four domains; land, sea, air and space. In 2016, NATO accepted the cyber domain as a fifth domain for warfare. The decision is aligned with the U.S. military strategy that already recognized cyberspace as a warfare domain. In 2009 the U.S. Government established the United States Cyber

Wilson is an Acquisition Cybersecurity professor at the Defense Acquisition University’s Mid-Atlantic campus in California, Maryland. He is a retired U.S. Air Force (USAF) officer with more than 35 years of experience in aviation systems engineering for the USAF and U.S. Navy.



Command (USCYBERCOM) to fulfill tasks related to cyber conflicts. Examining Sun Tzu's "The Art of War" in light of the new cyberwarfare domain reveals some very interesting and highly applicable strategies and tactics. "The Art of War" is laid out in 13 chapters with the following chapter titles.


Laying Plans
Waging War
Attack by Stratagem
Tactical Dispositions
Energy
Weak Points and Strong
Maneuvering
Variation in Tactics
The Army on the March

Terrain
The Nine Situations
The Attack by Fire
The Use of Spies

Strategies from each of these 13 chapters are herein examined from the cyberwarfare domain perspective. The Sun Tzu quote is provided in *italics* in bulleted items, followed by a short analysis of cyberwarfare domain applicability. In the interest of space, the number of strategies examined are limited to a few from each chapter in "The Art of War."

Chapter 1. Laying Plans

■ *The art of war is of vital importance to the state. It is equally true today that the art of cyberwar is of vital*



**Use the conquered foe to augment
one's own strength.**

**Sun Tzu apparently understood the
concept of a botnet 2,500 years ago.**

importance to the state. Defending our national infrastructure and commerce systems is not just vital, but critical to maintaining our citizen's safety. The ability to conduct offensive cyber operations as a means of degrading our enemy's war-fighting capability is of equal importance.

■ *Hold out baits to entice the enemy.* Sun Tzu apparently understood the concept of a honeypot 2,500 years ago. A honeypot entices the enemy into a cyber arena where the defender has the initiative.

■ *Attack him where he is unprepared.* An unsecured network is the "low hanging fruit" for a cyber warrior.

Chapter 2. Waging War

■ *Use the conquered foe to augment one's own strength.* Sun Tzu apparently understood the concept of a botnet 2,500 years ago.

■ *There is no instance of a country having benefited from prolonged warfare.* This is an interesting observation and equally true in the cyberwarfare domain. As a cyberwar progresses, it would be wearing on the population to have disruptions in commerce, health care and compromises to personal privacy that would be likely targets in the cyber domain.

Chapter 3. Attack by Stratagem

■ *The skillful leader subdues the enemy's troops without any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field.* Warfare in the cyber domain could potentially result in overthrow of the enemy without any physical combat in the other four warfare domains.

■ *We may know that there are five essentials for victory:*

- *He will win who knows when to fight and when not to fight.*
- *He will win who knows how to handle both superior and inferior forces.*
- *He will win whose army is animated by the same spirit throughout all its ranks.*
- *He will win who, prepared himself, waits to take the enemy unprepared.*
- *He will win who has military capacity and is not interfered with by the sovereign.*

An argument can be made that each of these essentials apply to the cyber domain. Choosing the cyber battlespace time and location, understanding strengths and weaknesses of our cyber forces and the enemy cyber forces, having the initiative, and free rein from civilian authorities are keys to success.

■ *If you know the enemy and know yourself, you need not fear the result of a hundred battles.* Winning in the cyber domain depends on knowing your cyberwarfare capabilities and those of the enemy.

Chapter 4. Tactical Dispositions

■ *To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.* Cybersecurity needs to be engineered into our systems, both military and civilian. Cybersecurity applies to both networks as well as platforms and control systems. Weakness in enemy systems need to be exploited vulnerabilities in cyberwarfare.

■ *To lift an autumn hair is no sign of great strength; to see the sun and moon is no sign of sharp sight; to hear the noise of thunder is no sign of a quick ear.* In our cyberwarfare domain, we need to be more than "script kiddies" on defense and offense.

■ *The skillful fighter puts himself into a position which makes defeat impossible, and does not miss the moment for defeating the enemy.* In cybersecurity, our systems need to be resilient that they cannot be defeated. Our cybersecurity defensive observe, orient, decide and act (OODA) loop must react to and defeat any cyberattack.

Chapter 5. Energy

■ *The impact of your army may be like a grindstone dashed against an egg—this is effected by the science of weak points and strong.* Analysis of software or hardware weaknesses, vulnerabilities, pivot points and attack surface will support the identification of weak points and strong points.

■ *Energy may be likened to the bending of a crossbow; decision, to the releasing of a trigger.* A Trojan implanted in a system has potential energy that is released when the trigger command conditions are satisfied.

■ *Energy amid the turmoil and tumult of battle, there may be seeming disorder and yet no real disorder at all.* Disorder and chaos may be the intended desire of a cyberattack on a nation's infrastructure. However, the perceived disorder and chaos is a result of the orderly commands executed by a cyber attacker—and, hence, no disorder at all.

Chapter 6. Weak Points and Strong

■ *The clever combatant imposes his will on the enemy, but does not allow the enemy's will to be imposed on him.* Warfare in the cyber domain requires both an offensive and defensive capability.

■ *A 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.* A cyberattack surface can provide multiple entry points into a system that the attacker can use to enter and then pivot to critical subsystems. Keeping knowledge of our weaknesses from our enemy will reduce the likelihood of a successful attack.

■ *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.* This cuts to the heart of cyberwarfare principles. A successful advanced persistent threat (APT) is subtly and secretly entered into the target system or a Trojan is likewise introduced. From that point on the system is owned ("Pwned") by us, and its fate is in our hands.

■ *Do not repeat the tactics which have gained you one victory, but let your methods be regulated by the infinite variety of circumstances.* Our offensive tactics in the cyber domain must continually evolve. What worked in one engagement will very probably not work in the next unless we stay inside of the defenders OODA loop. Conversely, our cyber defenses must be threat agnostic and behavioral based. Beat the abnormal behavior and you've defeated the threat regardless of the tactics evolution. This also is associated with Sun Tzu's following precept:

■ *He who can modify his tactics in relation to his opponent and thereby succeed in winning, may be called a heaven-born captain.*

Chapter 7. Maneuvering

■ *Let your plans be dark and impenetrable as night, and when you move, fall like a thunderbolt.* Maneuver in the cyber domain must be kept secret and when the trigger is pulled, the cyberattack must be designed to effectively accomplish the mission.

■ *Ponder and deliberate before you make a move.* This is equally true and maybe more so in the cyber domain. Cyberattacks may result in retaliatory attacks that the aggressor is unprepared to respond to or may even lead to traditional warfare in the other domains.

Chapter 8. Variation in Tactics

■ *In the wise leader's plans, considerations of advantage and of disadvantage will be blended together.* Strategic and tactical trade

space in the cyber domain needs to be understood prior to any engagement. We will always hold some advantages but will also have a disadvantage somewhere.

■ *Reduce the hostile chiefs by inflicting damage on them; and make trouble for them, and keep them constantly engaged; hold out specious allurements, and make them rush to any given point.* Modern cyberattacks that take down Internet connectivity, disable communications, or disrupt power generation systems would be very appealing to Sun Tzu.

■ *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.* In the cyber domain of warfare, it is inevitable that we will be attacked. In fact, both our civilian and military information technology (IT) systems have been and are being subject to cyberattacks. This is the rationale behind the new System Survivability Key Performance Parameter that says in part that all new systems need to be designed to survive in a cyber contested environment. We need to design our systems to deter, detect and recover from any cyberattack.

Chapter 9. The Army on the March

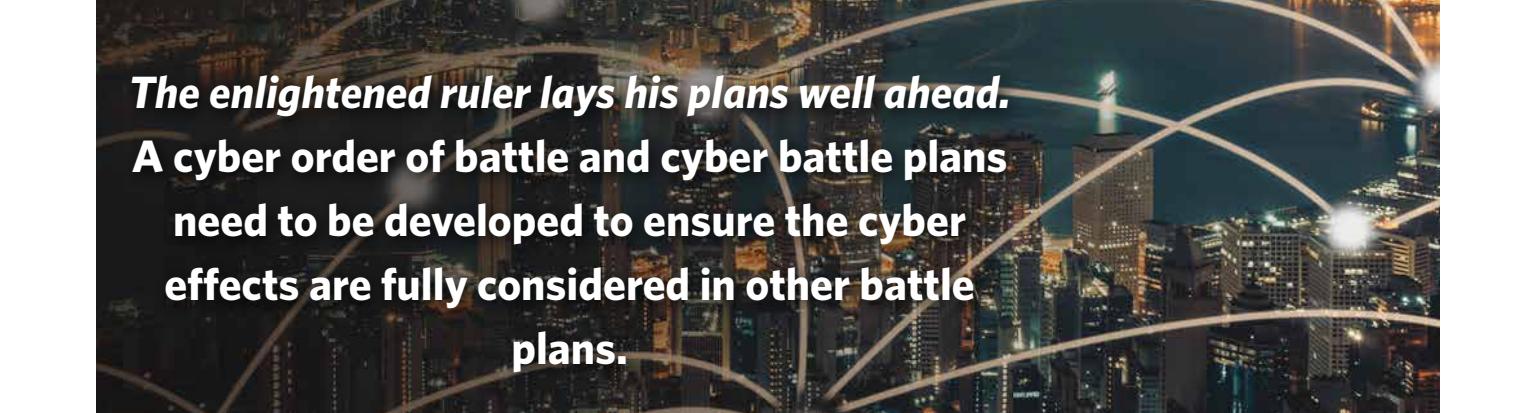
■ *Pass quickly over mountains, and keep in the neighborhood of valleys.* Concealing one's activities to avoid discovery by the enemy is a central tenet of any good cyberattack. Being able to enter a system undetected and move laterally within a system to reach the objective is essential to success.

■ *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.* This saying of Sun Tzu speaks to the design and architecture of our IT systems. We need to employ software assurance practices in design/implementation and security architectures that give our adversary no place to hide malware.

Chapter 10. Terrain

■ *With regard to ground of this nature [accessible], be before the enemy in occupying the raised and sunny spots, and carefully guard your line of supplies.* Several studies have shown that our cyber supply lines are very vulnerable. Department of Defense Instruction (DoDI) 5200.44, Trusted Systems and Networks, lays out some countermeasures to address the supply chain concern. It is essential that the military Services develop supply chain risk countermeasures and document them in classified appendices in program acquisition documentation such as the Life Cycle Support Plan and the Program Protection Plan.

■ *If you know the enemy and know yourself, your victory will not stand in doubt.* The first phase in the anatomy of a cyberattack is reconnaissance. The importance of good reconnaissance was made abundantly clear in the StuxNet virus attack on the Iranian nuclear fuel enrichment facility. Specific hardware in



The enlightened ruler lays his plans well ahead.

A cyber order of battle and cyber battle plans need to be developed to ensure the cyber effects are fully considered in other battle plans.

the facility was subject to the attack and that could not have been accomplished if necessary intelligence wasn't gathered well during the reconnaissance phase.

Chapter 11. The Nine Situations

■ *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.* Skillful leaders in the cyber domain will drive a cyber wedge between the enemy's front and rear; to prevent co-operation between divisions. DoDI 8510.01, Cybersecurity, recognizes the importance of information communication on the modern battlefield and structures the DoD cybersecurity around protection of the information. Our modern systems are ever more reliant on participation in the DoD Information Network (DODIN) for success on the battlefield. In fact, it has been stated, the "If you are not on the net, you are a target."

■ *Rapidity is the essence of war: take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots.* Our successful cyberattack will enter via unguarded or weakly guarded spots. Conversely, we need to examine the cyberattack surface for our systems to ensure we leave no entry point unguarded. The unguarded spot is where the adversary will launch their exploit.

■ *The skillful tactician may be likened to the shuai-jan. Now the shuai-jan is a snake that is found in the Ch'ang Mountains. Strike at its head, and you will be attacked by its tail; strike at its tail, and you will be attacked by its head; strike at its middle, and you will be attacked by head and tail both.* Our cyber defensive countermeasures must be modeled after the shuai-jan. Behavioral monitoring tools that provide for active countermeasures need to be developed to ensure system resiliency in the face of a cyberattack. Cyber domain defense tactics are still in their infancy relative to the other domains of warfare. "The Art of War" had a significant influence on the works of U.S. Air Force Col. John Boyd (1927-1997), arguably the best military strategist to work in the field since Sun Tzu. Boyd advanced tactics in the domain of air warfare following World War II, and cyber warriors need to do the same in their warfighting domain before a major conflict in the cyber domain breaks out.

■ *Forestall your opponent by seizing what he holds dear.* Likewise in the cyber domain! For our systems, we need to conduct a Cyber Failure Modes Effects and Criticality Analysis (Cyber

FMECA) to determine what is critical and crucial to defend from cyberattack. In risk management terminology, these must-define areas are those that score the high mark of 5 on the consequence (or impact) axis of the risk matrix. In an aviation system, this may be the flight control algorithms, or in a defense business system this may be the personal identification information of active-duty Service members.

Chapter 12. The Attack by Fire

■ *The enlightened ruler lays his plans well ahead.* A cyber order of battle and cyber battle plans need to be developed to ensure the cyber effects are fully considered in other battle plans. Likewise, we need to expect cyberattack plans to have been developed by our adversaries and build cyber effects into our campaign models.

■ *No ruler should put troops into the field merely to gratify his own spleen; no general should fight a battle simply out of pique.* Warfare in the cyber domain must be carefully considered. Hasty action in the cyber domain may result in retaliatory action in either the cyber or any of the other four warfare domains. An act of war is an act of war.

Chapter 13. The Use of Spies

■ *What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge.* The cyber domain throughout history has been an essential element in gathering intelligence. Cryptographic algorithms, such as the Julian cypher, have been in use for centuries providing information protection. Likewise, the breaking of cryptographic algorithms to discover information has been a key to decisive victories. As proof, I refer the reader to the victory secured by U.S. forces at the battle of Midway only 6 months after the devastating Japanese attack on the U.S. Navy at Pearl Harbor in World War II.

■ *Be subtle! Be subtle! And use your spies for every kind of business.* The best advanced persistent threat is subtle and undetected in execution of its mission. Our adversaries do not limit their cyber espionage to the business of the DoD. They infiltrate the defense industrial base, civilian institutions of higher learning, financial institutions, and infrastructure (hospitals, power generation and water systems to name a few such targets). &

The author can be contacted at roy.wilson@dau.mil.