The Calculus of Cyber Warfare as Influenced by the Subtle Art of Military Theory

David R. Shaw
dshaw@cyberba.net

Jeff Carr
jeff@suitsandspooks.com

Tom Muehleisen
tmuehleisen@cyberba.net

University of Washington
Center for Information Assurance and Cybersecurity
Bothell, WA

Abstract - Ever since The "History of the Peloponnesian War as written by Thucydides, an Athenian historian who also happened to serve as an Athenian general during the war, we have intellectually feasted upon progressive war theories throughout the ages. Conventional war is generally considered a three-dimensional endeavor. With the advent of cyber warfare, we add a fourth dimension of silent, asymmetric proportions, normally conducted by nation-states waged against one another. This war is currently being fought on a global scale endangering the security of many States and organizations. We face a vicious cyber offense with no rules of engagement and defend with a cyber defense system that labors valiantly under layers of rules, regulations, and oversight that is legacy from decades back, slow to progress to match the speed and efficiency of the cyber threat.

The authors of this paper seek to address the cyber threat from a military perspective, adapting time proven strategic military theory and theorists concepts of conventional warfare to principles of cyber warfare.

General Terms

Military Theory, Cybersecurity

Keywords

Military, Cyber, Cybersecurity, Cyberwar

1 INTRODUCTION

Recent headlines such as *"The New Handbook for Cyberwar is Being Written by Russia"* [1], *"How China is preparing for cyberwar"* [2], and *"Cyber nationalism and the new world order"* [3] puts a bright light on the global shift from threats of a conventional war somewhere remote to the "civilized" nations to a hyper threat of a technology war targeted directly at our Nation State, and has elevated to the probability of ONE affecting all in its path. The governments in North America and Europe have been working furiously to armor their high value systems with a focus on cybersecurity that is totally unprecedented.

By applying military theories and styles to cybersecurity and risk management frameworks for government agencies, we are making it infinitely more difficult for the threat actors to achieve success in their attacks. However, the private sector remains almost completely vulnerable to loss during a cyber war or similar level of attack which will literally cripple our national economy when hit with a massive attack. The global financial depression of 2008 provides us with an insight to this claim as to consequences.

The cyber risk management emphasis in the private sector has been largely through the Information Sharing and Analysis Centers (ISACS) coalescing the larger members of the commercial businesses. Certain sectors of the nation's private sector, including the public utilities, and other NGO's, are levered into compliance of antiquated regulations and processes by audit and regulatory oversight. Likewise, most commercial businesses who have structured risk management and incident

response plans are not testing them regularly and therefore leave the data protection and response from incursions to their technology managers, or ignore the risk.

The problem is mammoth and the ability to thwart the threat against the private sector critical infrastructure is well beyond the scope of any government or similar sized entity to solve externally. Therefore, the problem must be solved from within the confines of the individual businesses with totally unconventional means.

We are therefore advocating adapting principles of military style attributes and well established military theories to businesses that will harmonize their protection of critical data and resources, maintain cybersecurity pace with the threat actors and threat vectors enveloping virtually every sector of our technology. This adaptation may also armor against devastating losses that are causing over 60% of the business attacked to fail within 6 month of the attack.

This paper advances that the calculus of cyber warfare can be likened to the theoretical military style frameworks devised, tested and embedded in conventional warfare. President George W. Bush stated: "Cyberspace is the nervous system—the control system of our country" [4], Cyber aggression upon our national interests, including our manufacturing and service industries, and critical infrastructures can and should be considered as an act of war. Thus, we have adopted principles and theories of warfare to the framework of cyber warfare, which is in its adolescent stage of growth and dynamics.

2 APPLICABLE MILITARY THEORIES

2.1 Past and Present: Clausewitz and Luttwak

Carl Philipp Gottfried (or Gottlieb) von Clausewitz was a Prussian general and military theorist who stressed the "moral" (meaning, in modern terms, psychological) and political aspects of war. His most notable work, Vom Kriege (*On War*), was unfinished at his death. Clausewitz was a realist in many different senses and, while in some respects a romantic, also drew heavily on the rationalist ideas of the European Enlightenment. He stressed the dialectical interaction of

diverse factors, noting how unexpected developments unfolding under the "fog of war" (i.e., in the face of incomplete, dubious, and often completely erroneous information and high levels of fear, doubt, and excitement) call for rapid decisions by alert commanders [5].

Drawing from the theoretical treatments in his book *On War*, one is challenged from the onset of Book 1 to draw multiple direct parallels to cyber warfare from his theories, assertions and aphorisms. However, Clausewitz has provided us with some grist for our comparative mill. My favorite is the following equation (Figure 1) that is paraphrased or adapted as The Calculus of Cyber Warfare, phrased as:

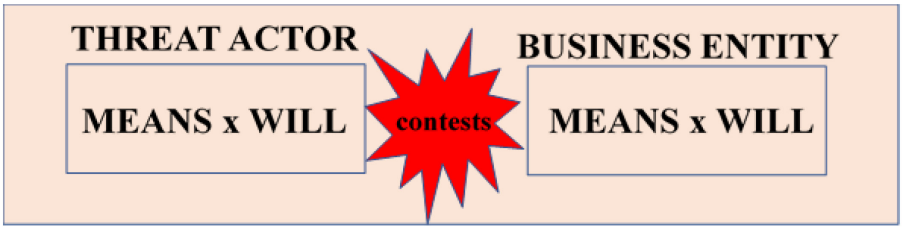

Figure 1: The Total Power to Wage Cyber War (of two opponents)

As directed to cyber warfare, the "means" relates directly to the skills, tools, access, funding, and all that the threat actor can possibly bring against a target or targets which is described by Clausewitz as the maximum exertion of strength. The "will" factors in the intangibles or non-material force multipliers such as mobilizing moral forces which often are fungible with national politics for nation-state threat actors. An additional factor are the rules of engagement which are often obviated by the threat actor(s) which gives them an additional advantage over a constrained cyber defense system / process.

The defender must employ at least equal resources and amass will throughout the organization to fend off any and all attacks by the threat actors, regardless of their skill levels. The objective is for the targeted business (face it, we are all targeted), to identify its key high value assets and build a defense in depth to make it infinitely

difficult for threat actors to penetrate. Lastly, there needs to be an enterprise wide understanding of the threats and defense postures to Harmonize the risk management leadership / command structure from top to bottom with a firm understanding of their respective roles, responsibilities and relationships (3 R's) regarding cybersecurity. This goes to both Means and Will to "get it right" every time.

The following image (Figure 2) is a sample of cybersecurity defense in depth demonstrating means and a certain degree of will by virtue of the type of defense.

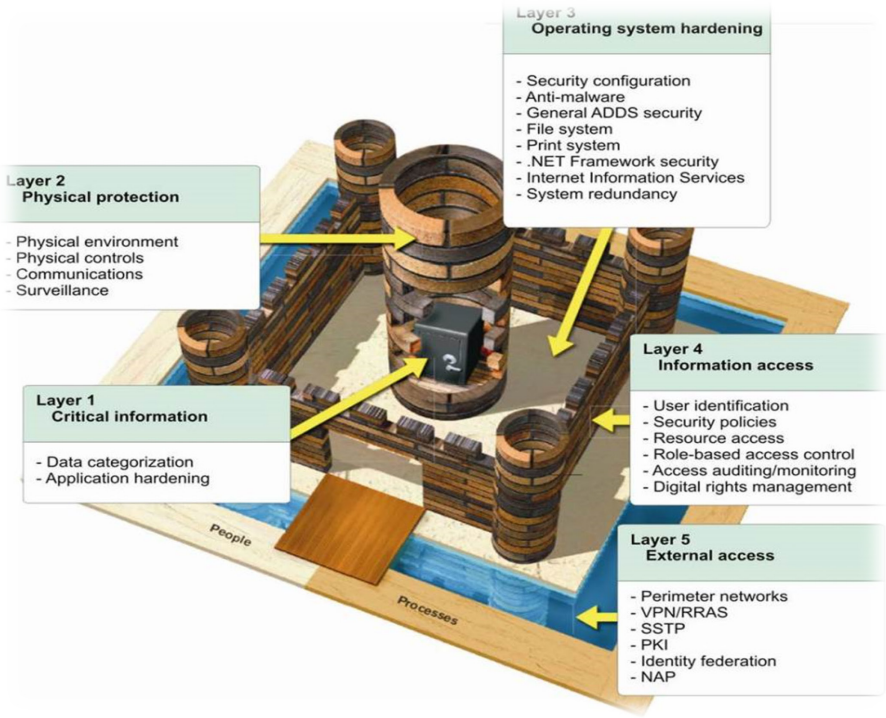

Figure 2: Castle Defense System – Defense in Depth [6]

The "C-Suite" must identify the high value units (HVUs) in the entity to be protected. Then Clausewitz's theory of Means x Will is invoked as outlined above to protect the HVUs) as the Iron Calculus of Cyber Warfare.

Edward Luttwak is both a celebrated author ("Coup D'Etat: A Practical Handbook", "Strategy: The Logic of War and Peace") and a consultant to modern-day governments on the application of strategy in warfare [7]. This article references his book "Strategy: The Logic of War and Peace" from the perspective of defending against attacks in cyberspace where the principals of "least expectation" and "deception" certainly apply.

"Least expectation", according to Luttwak, is the practice of understanding what an adversary expects you to do, and then doing the opposite. This is contradictory to the logic of peacetime when, if you wish to travel from point A to point B, you take the most direct route, using the best roads at a time of day that has the least amount of traffic. However, when you have an adversary whose mission is to intercept and engage you, you'll want to travel on the worst roads, in the middle of the night with no moon, and in heavy rain. Luttwak's entire first chapter is dedicated to this contrary logic where "a bad road can be considered good precisely because it is bad" [8].

One of the emerging strategies in network defense is the use of deception, which has come a long way from the use of honey pots. Gartner predicts that by 2018, 10 percent of enterprises will be using a form of this technology from one of a handful of cybersecurity startups focused on delivering new deception tools and techniques [9].

Deception as a network defense strategy presumes that the defender can fool the attacker in believing that a server or the nodes on a server are an authentic part of the network and contain valuable data of interest to the attacker when in fact the server traps the attacker in a contained zone on the network where his actions can be studied safely for as long as the illusion can be sustained.

Unfortunately, there are two big obstacles to a successful deception defense. One is that you need to know what the attacker is interested in so that you can create an enticing trap. The other is that you need to dedicate resources to creating a compelling illusion that will be believable to an experienced attacker. Those resources pull from the overall Security Operations Centre (SOC) budget, usually limited to begin with.

"More commonly, the use of (passive) dummies and (active) decoys of any kind, from fake tanks and guns or complete unites, to flying or navigating decoys that simulate specific aircraft or submarines, are much cheaper than the real thing but still absorb resources that would otherwise increase the strength on hand." [10]

A third consideration in evaluating deception as a strategy, according to Luttwak, is that "deception deceives when there is a predisposition to deception" [11]. In network warfare, deception is the adversary's bread and butter. The use of a spear phishing attack to fool the intended victim into opening a poisoned document or visiting a website that serves malware is the most common way that organizations find themselves breached.

When a SOC is fighting an adversary who understands the tactics of deception so thoroughly, its own deception strategy will require substantial thought and planning in order for it to work. Even if it is successful in stopping the first attack, it will need to be revised in order to stop the second, and so on.

The hard truth is that, in time, a dedicated adversary with sufficient resources will gain access to the victim's network. For that reason, the best approach is not to waste resources on keeping adversaries out, but instead focus those resources on keeping the organization's crown jewels from leaving.

2.2 The OODA Loop

Decision process is a critical feature in defending against cyber-attacks. The OODA loop was developed by a fighter pilot tactician and is a formalized decision making procedure that is applied to any situation where a practiced decision-making

process is necessary in a threat situation. It is especially important when the decisions have to be made quickly, as in a threat situation. The development of a rapid, agile decision making process is essential for cyber threats and can provide huge tactical advantages. Most entities when confronted with cyber threats / attacks take a "chess player role" where they make a move and wait for the threat actor to make a counter-move. To establish an effective defense posture against cyber threats, decisive moves should be as rapid as possible to keep the threat off balance and keep the initiative on side of the defender.

O-O-D-A stands for Observe-Orient-Decide-Act. It is a "loop" because it is repeated until the situation is over or the objective is satisfied (in some instances, the process is continuous and may never be satisfied). The objective is to work through the loop faster than a threat actor to gain or maintain a tactical advantage. In an ideal situation, a threat should be dealt with before the threat actor has even realized he is in a confrontational situation and entered his own OODA loop; this is a defense-in-depth situation. If in a reactive posture and the threat actor has initiated the attack, the objective is to "get inside" his loop to gain an effective advantage followed by a continued exercise of the process to fortify the advantage.

This looping concept referred to the ability possessed by fighter pilots that allowed them to succeed in combat via a rapid and agile decision process. The OODA Loop is now used as a standard framework or methodology by military, federal and commercial entities as a basis for rapid and continuous assessment and decision making. The premise of the model is that decision-making is the result of rational behavior in which problems are viewed as a cycle of Observation, Orientation (situational awareness), Decision Making, and Action. Boyd diagramed the OODA loop as shown in Figure 3 below:

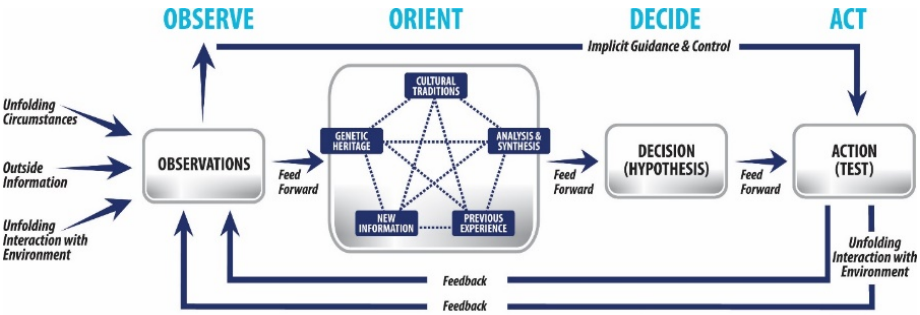

Figure 3: Standard OODA Loop Functional Diagram

An entity (whether an individual or an organization) that can process this cycle more quickly than an opponent can "get inside" the opponent's decision cycle and gain the advantage. The essential components of the OODA Loop as depicted in the above figure are:

- **Observation**: Scan the whole environment and gather information from it.
- **Orientation**: Use the information to form a mental image of the circumstances. That is, synthesize the data into information. As more information is received, one may "deconstruct" old images and then "create" new images. Note that different people require different levels of details to perceive an event. It is often implied that the reason people cannot make good decisions is that people are bad decisions makers — much akin to saying that the reason some people cannot drive is that they are bad drivers. However, most bad decisions result from the fact that a person will often fail to place the information that is available into its proper context. Orientation emphasizes the context in which events occur, so that it may facilitate decisions and actions. That is, orientation helps to turn information into knowledge, and knowledge, not information, is the real predictor of making good decisions.
- **Decision**: Consider options and select a subsequent course of action or actions.

- **Action**: Carry out the conceived decision. Once the result of the action is observed, the entire cycle starts over. Note that in combat (or competing against the competition), you want to cycle through the four steps faster and better than the enemy, hence, it is a loop.

The Loop doesn't mean that individuals or organizations have to observe, orient, decide, and act, in the order as shown in the diagram above. Rather, picture the loop as an interactive feedback web with orientation at the core, as shown in the diagram below. Orientation is how a situation is interpreted, based on culture, experience, new information, analysis, synthesis, and heritage.

The Loop is a set of interacting loops that are kept in continuous operation thus the decision process is agile, capable of rapid assessment, and can encompass multiple perspectives as discussed below.

It has been generally stated that nation-states operation like biological organisms composed of discrete systems. These systems include leadership, organic essentials, infrastructure, population, and the military. A Hungarian immigrant, Brigadier General Huba Wass de Czege (pronounced VOSH de tsay-guh) (born August 13, 1941) is the son of Count Albert Wass de Szentegyed et Czege. Wass de Czege retired from the United States Army as a General Officer with a reputation as a highly innovative thinker. He is the founder and first director of the School of Advanced Military Studies at the United States Army Command and General Staff College [12]. He stated that Positive Ends is the possibility of taking advantage of a new security environment to create conditions for long-term peace.

The adaptation of this theory goes to enveloping a new strategic risk management framework, policy and process with advanced tools to create a longer-term threat avoidance and protect organizational HVUs and E-Systems. Cyber-attacks generally may appear to be chaotic and are asymmetric, requiring a highly dynamic tool(s) and processes to assess and visualize them. Whether successful or unsuccessful, such attacks can be devastating and have the capability to create havoc in what has become our fundamental infrastructure for communication and

commerce. From simple email, to social networks, from e-business to critical intelligence gathering, nearly every aspect of modern operations rely on systems potentially exposed to cyber threats. Identifying potential vulnerabilities, performing risk analysis, and subsequently building cyber defense systems in depth are essential steps to protect high value E-Systems.

Key attributes for risk analysis methods and tools for cyber threat modeling include the following:

- **Agility**: The ability of the risk assessment process to accept and analyze dynamic threats from an asymmetric attack environment. Attack surfaces or threat vectors are not always clearly defined therefore agility is a necessary feature in any cyber risk assessment process. This includes discovery of new attack surfaces via an iterative testing process which addresses the issue of "we don't know what we don't know".
- **Proactivity**: The ability to take the initiative by acting rather than reacting to threat actors and cyber-attacks. Take offensive action to either preoccupy the opposition and ultimately its ability to directly harm or destroy its ability to attack.
- **Resiliency & Elasticity**: The ability to recover quickly and accurately from setbacks and changes.
- **Rapid assessment capability**: Rapidly changing technologies and their applications (including methods of application) demand a capability to rapidly assess attack surfaces and associated threat vectors.
- **Scalable**: The capability of a system to increase total throughput under an increased load when resources are added. It also needs to address the scope of the analysis to include subsystems, system and/or system of systems.
- **Center of Gravity**: The hub of all power and movement on which everything depends, the point at which all energies should be directed. Focus is a key attribute in protecting HVUs and combating cyber-attacks.

2.3 Sun Tzu and Cyber War

No essay addressing military theory can go without engaging Sun Tzu. His *The Art of War* is an ancient Chinese military treatise dating from the 5th century BC. Attributed to the ancient Chinese military strategist Sun Tzu. It is commonly thought of as a definitive work on military strategy and tactics…and has long been the most influential strategy text in East Asia. It has had an influence on Eastern and Western military thinking, business tactics, legal strategy and beyond for centuries [13]. Selected Sun Tzu quotes from *The Art of War* applicable to cyber warfare are presented as follows and having digested the above theoretical attributes generate a kinship to those concepts and associated principles as are noted in italics:

- "Appear weak when you are strong, and strong when you are weak." *(Relates to Clausewitz)*
- "If you know the enemy *(threat and threat actor)* and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every *(cyber)* victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle *(cyber-attack)*."
- "Supreme excellence consists of breaking the enemy's resistance without fighting."
- "If your enemy is secure at all points, be prepared for him. If he is in superior strength, evade him. If your opponent is temperamental, seek to irritate him. Pretend to be weak, that he may grow arrogant. If he is taking his ease, give him no rest. If his forces are united, separate them. If sovereign and subject are in accord, put division between them. Attack him where he is unprepared, appear where you are not expected."
- "Engage people *(threat actor)* with what they expect; it is what they are able to discern and confirms their projections. It settles them into predictable patterns of response, occupying their minds while you wait for the extraordinary moment — that which they cannot anticipate."

- "The art of *(cyber)* 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."

2.4 Military Information Operations

We conclude the section with the present by defining something DoD calls the Information Environment (IE). "The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive. The physical dimension is composed of command and control systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information." [15]

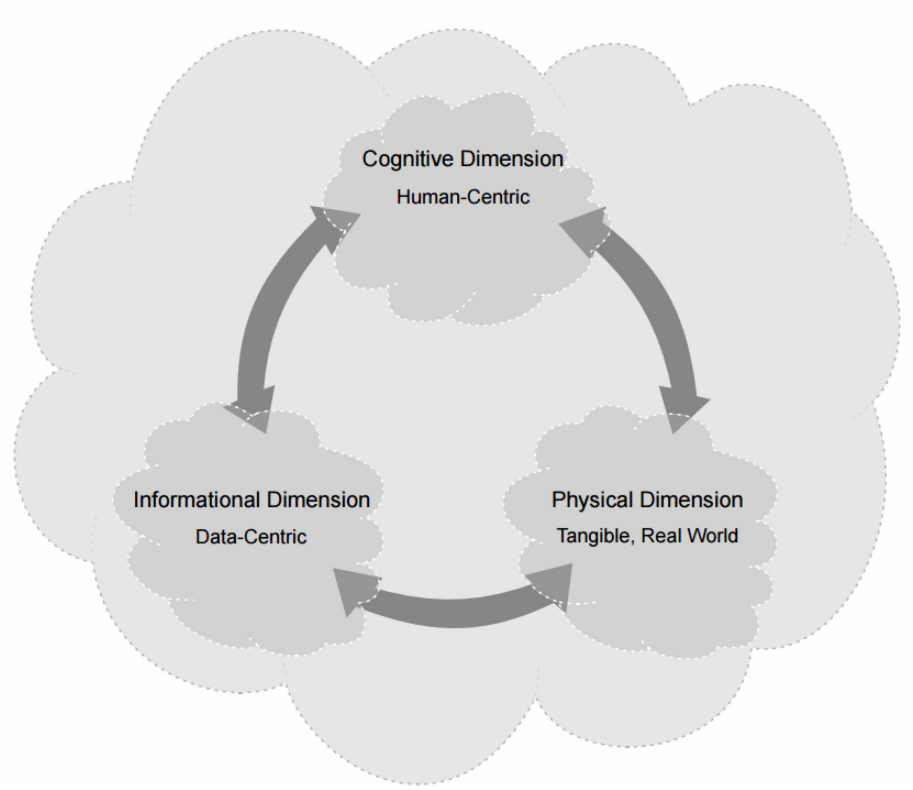

Figure 4: The Information Environment [16]

Spend a few moments considering the figure above and re-read the DoD definition. Each of these dimensions are important, and what is sometimes lost in this discussion of the "cyber" domain is that, ultimately, this information is used by a person. For a reason. The author's contention is that organizations will be more successful if they strictly control the who's and the why's, along with the what's and the where's. (translation: use proven methods like OPSEC [17] to identify what is important, who else wants it, what they can get to and what you can do to protect it). Further, that current DoD doctrine, the culmination of centuries of study and practice is extremely useful and applicable to civilian organizations.

3 DERIVED PRINCIPLES FROM MILITARY THEORY AS MAY BE ADAPTED TO CYBERSECURITY

Following an analysis of selected military theories proffered above, we offer key principles of cybersecurity for defense of our high value units (HVUs) within business and/or government entities to help defend against all levels cyber threat:

- Harmonize the risk management leadership / command structure from top to bottom with a firm understanding of their respective roles, responsibilities and relationships (3 R's). This is essential to ensure unified command and control, particularly in the time of crisis. No military goes without this clearly understood with each level having a complete understanding of the mission, their role(s) and the reporting structure.
- Adapt the best risk management model and framework for the business. This goes to mission, what is being protected, and the plans that support the mission.
- Devise and adopt rules of engagement (ROE) for combating cyber threat particular to the entity targeted. The ROE must be clearly understood by everyone in the chain of command.
- Exercise the incident response plan and with all stakeholders often with red and blue team participation at all levels. This goes to training, vulnerability assessment and recovery.
- Continually address tool assessment and realignment. This goes to agile protection, cost abatement, training, and effectivity of the adopted tools. Use Case Studies are an excellent means for tool assessment and getting all of the appropriate stakeholders to understand the results.
- Understand the continuous cyber related intelligence offered from deep technology data to business applications. This requires highly trained researchers and analysts to explore the cyber threat, apply the threat knowledge by mapping the threat against the organizational needs and vulnerabilities.

- Cybersecurity training and education, to include certifications, is continual. The cyber threat is dynamic therefore our understanding of the threat and how we adapt our defenses is a journey, not a destination.
- Consider the military theories proffered in this paper and if any or all resonate with your particular business environment and cyber threat posture we invite further study into the adoption of them into your business processes from a people, technology, process and strategic perspective.
- Just like the military, cybersecurity and risk management is a culture. And likewise, it is a journey of many dynamic attributes and never a destination.
- We are *all* at cyber risk… therefore we need to ensure that processes to protect from cyber threat are understood and are dynamically cooperative in creating a resilient defense. In so doing we seize the initiative in creating innovative protections for all critical organizational infrastructures.

Figure 4: Cyber Warfare Takes on a Whole New Perspective [14]

4 FUTURE WORK

Cyber warfare is an emerging science from the business perspective in both government and the private sectors. The concepts introduced in this paper will be entertained as potential course content in certificate and advanced cybersecurity and risk management courses. Secondly, the authors will approach the Professional Military Schools to further expand these concepts by the Service Professionals attending these schools.

REFERENCES

[1] Sheera Frenkel, BussFeed News Reporter, BuzzFeed News, March 19, 2017

[2] Adam Segal, Contributor, The Christian Science Monitor, March 20, 2017

[3] John Costello, GCN Magazine, March 20, 2017

[4] George W. Bush, National Strategy to Secure Cyberspace, (Washington DC: The White House, February 2003)

[5] From introduction of history of Carl Philipp Gottfried (or Gottlieb) von Clausewitz, author unknown

[6] Danielle Reust, "Resource pool security procedures in a virtual infrastructure", November 2009, Resolution Enterprises Ltd.

[7] "The Machiavelli of Maryland", The Guardian online, Dec 9, 2015 (source: https://www.theguardian.com/world/2015/dec/09/edward-luttwak-machiavelli-of-maryland)

[8] Luttwak, Edward. Strategy: the logic of war and peace. Harvard University Press, 2001.

[9] Gartner; "Emerging Technology Analysis: Deception Techniques and Technologies Create Security Technology Business Opportunities" 16 July 2015 (updated 30 Sep 2016)

[10] Luttwak, Edward. Strategy: the logic of war and peace. Harvard University Press, 2001, p.6

[11] Ibid., p. 253

[12] From Introduction to history of Brigadier General Huba Wass de Czege, author unknown.

[13] Ibid.

[14] Image: DarkGovernment - 22 Jul 2011

[15] Joint Publication 3-13, Information Operations, (2012, November 27) with Change 1 (2014, November 20). Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

[16] Ibid, Figure I-1, page I-2.

[17] Operations Security, US program since 1988, see
https://en.wikipedia.org/wiki/Operations_security