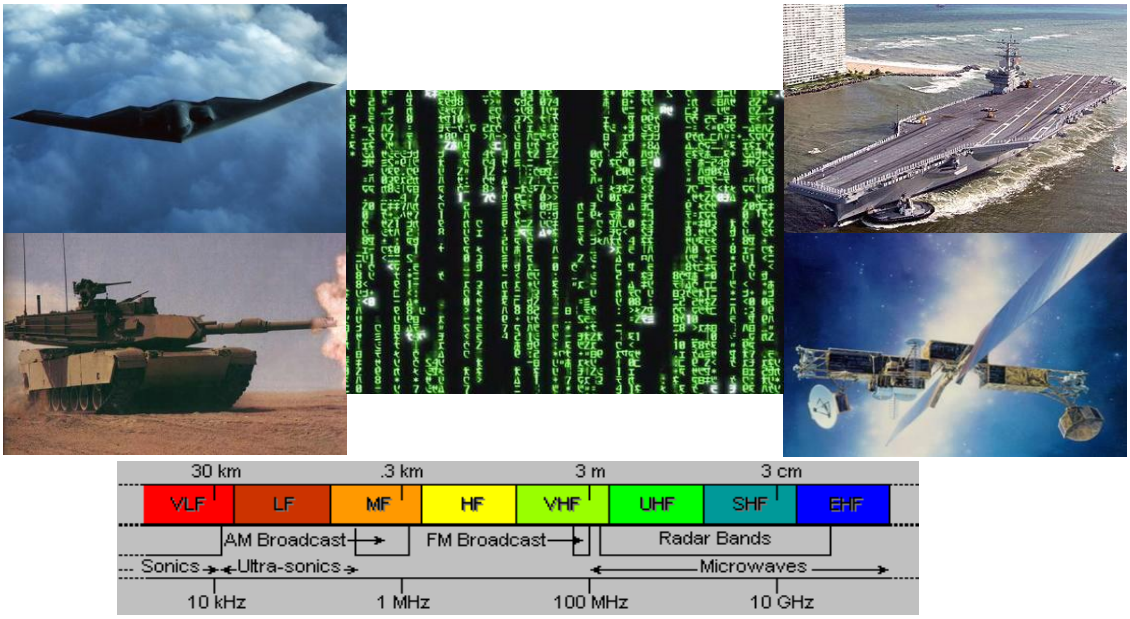
War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare



Land, Maritime, Air, Space, and Cyber domains[1]

By

Richard M. Crowell

(The views expressed in this paper are those of the author and do not reflect the official policy or position of the Naval War College, Department of the Navy, Department of Defense, or the U.S. Government.)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval War College,686 Cushing Road,Newport,RI,02841-1207**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**32**	

Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information, or information resources in order to achieve a significant advantage, objectives, or victory over an adversary.

– Winn Schwartau, InfoWarCon 2009, Washington, DC

Information Warfare Circa 1981

During the Cold War, the USSR was at least a decade behind the U.S. in computer technology. To fill that void, the Soviets developed an aggressive program to steal U.S. and Western science and technology. In 1981 French President Francois Mitterand passed vital information to U.S. President Ronald Reagan. The case was designated *Farewell* by the French Direction de la Surveillance du Territoire (DST), and later became known as the *Farewell Dossier*.

Some of the most useful information gained from the *Farewell Dossier* was the KGB's 'shopping list' for their most desired technology. In his book, *At the Abyss, an Insider's History of the Cold War*, Thomas C. Reed, a former Director of the National Reconnaissance Office, recounts an incident of early computer warfare which was prompted by a KGB theft.

> The production and transportation of oil and gas was at the top of the Soviet wish list. A new trans-Siberian pipeline was to deliver natural gas from the Urengoi gas fields in Siberia across Kazakhstan, Russia, and Eastern Europe, into the hard currency markets of the West. To automate the operation of valves, compressors, and storage facilities in such an immense undertaking, the Soviets needed sophisticated control systems. They bought early model computers on the open market, but when Russian pipeline authorities approached the U.S. for the necessary software, they were turned down. Undaunted, the Soviets looked elsewhere; a KGB operative was sent to penetrate a Canadian software supplier in an attempt to steal the needed codes. U.S. Intelligence, tipped by *Farewell*, responded and – in cooperation with some outraged Canadians – "improved" the software before sending it on.
>
> Once in the Soviet Union, computers and software, working together, ran the pipeline beautifully – for a while. But that tranquility was deceptive. Buried in the stolen Canadian goods – the software operating this whole new pipeline system – was a Trojan Horse. (An expression describing a few lines of software, buried in the normal operating system, that will cause that system to go berserk at some future date (Halloween?) or upon the receipt of some outside message.) In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset

> pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space. At the White House, we received warning from our infrared satellites of some bizarre event out in the middle of Soviet nowhere. NORAD feared a missile liftoff from a place where no rockets were known to be based. Or perhaps it was the detonation of a small nuclear device. The Air Force chief of intelligence rated it at three kilotons, but was puzzled by the silence of the Vela satellites. They had detected no electromagnetic pulse, characteristic of nuclear detonation.[2]

This event did not utilize the modern method of inserting malicious software (malware) via the internet, but it was clearly the manipulation of a Supervisory Control and Data Acquisition (SCADA) system. SCADA are real time industrial process control systems that use computers and software to monitor and control systems from nuclear power plants and electric power grids to railroad switching terminals and drinking water and sewage treatment facilities. Given advances in computers since the 1980s, one can easily envision the burgeoning risks of computer usage. Chaos can be created with the insertion of a Trojan horse, via malware into military command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems or a power company's SCADA system. This could shut down or destroy a power grid supporting military command and control (C2) systems, resulting in an impotent military. A similar attack against a civilian power grid during extreme cold weather could result in millions of civilians freezing to death. Would this be a cyberspace operation? Would this be a weapon of mass destruction or effect (WMD/E)[†]?[3] Would this merger of modes and means be classified as hybrid warfare? Who would respond? What actions would the U.S. Department of Defense take? Which command would respond? More importantly, how would the commander need to think about cyberspace operations?

Traditionally, warfare has been waged in physical domains that can be seen and touched by those who conduct operations in them.[4] Until recently, there were four domains – land, maritime, air, and space. The information age's interconnected use of electronics, which moves digitized data through the electromagnetic spectrum, has brought forth a fifth domain. Warfighters must now learn to operate and fight in this domain, called cyberspace.

This paper will describe cyberspace, discuss cyberspace operations and depict their relationship to 21st century hybrid warfare. It will present the framework of operational art, specifically operational factors and functions as a tool for understanding operations in cyberspace.[5] A series of questions will be posed for future operational commanders to help frame their thoughts on cyberspace. Additionally, it will postulate that cyberspace is a near perfect domain in which to conduct hybrid wars.

Cyberspace and the Information Environment

[†] Weapon of mass destruction (WMD) is defined as chemical, biological, radiological or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. Weapon of mass effect (WME) is defined as weapons capable of inflicting grave destructive, psychological and or economic damage to the United States.

The information age has been described by Winn Schwartau, author of numerous books on the Information Age and Information Warfare, as "computers everywhere."[6] While much has been written about the information age and its impact on modern warfare, the primary characteristic of the information age is the proliferation of information technology (IT). IT incorporates information systems and resources (hardware, software, and wetware) used by military and civilian decision makers to send, receive, control, and manipulate information necessary to enable 21st century decision making.[7]

The combining of individuals, systems, content, and resources to enable decision making forms the Information Environment (IE). The IE, a term of art, is defined in Joint Doctrine for Information Operations as:

> The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The actors include leaders, decision makers, individuals, and organizations. Resources include the materials and systems employed to collect, analyze, apply, or disseminate information. **The information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision making. …**The information environment is made up of three interrelated dimensions: physical, informational, and cognitive… **These dimensions are inextricably linked**.[8] (Emphasis added)

The ability to understand cyberspace is directly related to comprehending how and why information moves through the IE and how that information is used to influence human decision making in both peace and war. While the nature of war remains unchanged, it is the character that is malleable. Today, the battle for the hearts and minds of the people around the globe is being waged in the IE with weapons that use information instead of physical means to compel decision makers to act. Cyberspace, with its lack of traditional geometry, represents perhaps the most malleable of operating environments. It is paramount for 21st century military leaders to become comfortable working and fighting in this domain.

The military capability most often used to maneuver within the information environment is information operations. U.S. Joint Military Doctrine defines Information Operations as:

> The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (Mil Dec), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making, while protecting our own.[9]

The information operations core capability most linked to cyberspace is computer network operations (CNO), which represent the tools used to navigate cyberspace. CNO are comprised of computer network attack (CNA), computer network defense (CND), and related computer network exploitation (CNE) enabling operations.[10]

One of the primary goals of cyberspace operations is to affect decision making; in most cases, to influence a decision maker to decide in your favor. This can be done by gaining access to data resident in electronics and using it to your advantage or simply moving information to and from the decision maker in order to achieve an effect or an objective. Operation BODYGUARD, the World War II strategic deception for the Allied invasion of Northern Europe, is a 20th century example of moving information to a decision maker largely via the electromagnetic spectrum.‡ The decision maker might be a civilian or military leader, or the local populace. The information can be moved by radio, television, cell phone, e-mail, hacking, or a phishing scheme.[11] The relationship between IO, cyberspace, and human interaction is best described by Lieutenant Colonel David T. Fahrenkrug, USAF and Dr. Daniel T. Kuehl, from the National Defense University, Information Resource Management College:

> While information operations thus includes all three dimensions of the information environment, [physical, informational, and cognitive] cyberspace comprises only a part—albeit perhaps a very large part—of the connectivity and content dimensions.[12] Cyberspace is thus shaping and changing the three dimensions of the information environment: how we create information content itself (a Web page, for example), how we share that content through new forms of connectivity (the Internet links that make that Web page accessible to over a billion people), and how human interaction and communication are affected.[13]

No one disputes the explosive expansion of cyberspace use. Around the globe, more and more people are making decisions based on information gleaned from 'information age' methods rather than 'industrial age' methods. The common thread with the information age means is that they use cyberspace – electromagnetic radiation, moving information to and from electronics, and ultimately the decision makers. The number of humans utilizing cyberspace for commonplace activities (communication, news, shopping, banking, and entertainment) is growing exponentially. In Mumbai, India, a city of 13 million, use of cell phones and internet to receive news grew from 1% to 48%, between 2006 and 2008.[14] The *2008 CIA World Fact Book* states that approximately 60 % of the world population and 86 % of the U.S. population use cell phones.[15] We now have a President of the United States of America who cannot be without his BlackBerry – connecting him to his most trusted friends and staff via cyberspace.[16]

---

‡ The deception relied heavily on convincing the German decision makers of three main objectives: 1) a large force will go to Norway and threaten Germany from the North. A fictitious army was created in Scotland. The British Fourth Army sent out thousands of 'real' radio signals that were electronic deceptions; 2) the main invasion will come through the Pas de Calais, France. The First US Army Group (FUSAG) was created in the county of Kent (near Dover). Another ghost army, FUSAG with General Patton as its real commander, also sent out thousands of 'real' radio signals; 3) whatever happens in Normandy is a feint. The messages were reinforced by the truth because Dover to Calais is the shortest distance England to France, the beaches around Calais are large and flat, and it was the beginning of the shortest land route into Germany.

Most of the information was moved via radio and Morse code signals. Additionally, in the early hours of June 6th the Allies conducted an elaborate electronic deception in the form of air and sea assets emitting false targets. This presented the appearance of an armada moving towards Calais. This information was reinforced by dozens of German agents, turned by the British XX (double cross) organization, sending electronic messages back to the Abwehr, German Intelligence HQ. All of this was done to convince the German decision makers, primarily Adolph Hitler, to decide in the Allies favor.

Cyberspace Definitions

There are disputes, however, as to the correct definition of cyberspace. As understanding and use of this new domain evolves, so too does has the definition. Earlier definitions focused on computers and computer usage. *The Oxford English Dictionary* defines cyberspace as the notional environment in which communications over computer networks occurs.[17] Schwartau, states, "Cyberspace is the intangible place between computers where information momentarily exists on its route from one end of the global network to the other."[18] Later definitions have evolved to include all manner of electronic communications. Still disputed is whether or not human activity should be included in the definition of cyberspace.

It is not surprising that our technology-oriented military exclude human activity from the definition of cyberspace. The Department of Defense (DOD) Quadrennial Roles and Missions Review Report, published in January 2009, defines cyberspace as "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."[19] The U.S. Chairman of the Joint Chiefs of Staff provides a definition of cyberspace operations that addresses human activity; "the employment of cyber capabilities where the primary purpose is to achieve military objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid[§]."[20]

Because humans are the inventors of information technology, the author supports a holistic approach to the definition of cyberspace, to include both technology and human activity. Dr. Kuehl provides an inclusive definition of cyberspace that shows intertwining of domains and human activities.

> Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communications technologies.[21]

Obviously, cyberspace would not exist without its component electronics and electromagnetic spectrum (EMS). Electronics are the computers, smart phones, and hardware that have components that direct electric current. The electromagnetic spectrum gives a physical definition to cyberspace and relates directly to how digitized information moves through cyberspace. In its most simple form, information (words, pictures, files, et al.) is converted to digital data in the form of binary code (1s and 0s) by the electronics. The digital data is placed into 'packets' and these are sent via electromagnetic radiation along the most secure and expeditious route between two points. Radio, television, voice, and data signals are sent from a transmitter to a receiver, in the same way communication of old was sent on packet ships sailing the Atlantic Ocean between England and New York.

[§] The Global Information Grid (GIG) is defined in U.S. Joint doctrine as the globally interconnected end-to-end set of capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Two modern examples are the Apple iPhone and the maritime Automated Information System (AIS). The iPhone moves information via the electromagnetic spectrum using the 850 MHz frequency for voice and 1900 MHz frequency for data. The U.S. Department of Homeland Security and the U.S. Coast Guard describe AIS as a shipboard display system (e.g. radar, chart plotter, etc.) with overlaid electronic chart data that includes a mark for every significant ship within radio range; with a velocity vector (indicating speed and heading).[22] Similar to the iPhone, the AIS uses two frequencies, 161.975 MHz and 162.025 MHz, to move information to and from the electronic displays. Incidentally, AIS can be bought in Europe for approximately US$500 and in early 2009, Somali pirates were reported to be using AIS to identify and track their targets.[23]

Electronics and the electromagnetic spectrum in the cyberspace domain may be better understood when viewed as an analogy for ships and the sea in the maritime domain. Just as crucial as the human activity planning, directing and operating in the maritime domain is the human activity in the cyberspace domain. Globally, increasingly more people get their information from electronics - satellite television, personal computers, smart phones, blogs, new media, or social networking sites[**].[24] In 2007, 84% of the population of Moscow, Russia owned cell phones.[25] In that year, 45% of Muscovites used cell phones and the internet to get news.[26] Individuals are also increasingly using cyberspace to make decisions, to interact, and to effect action. As we move deeper into the 21st century, more and more human activity will occur in cyberspace. These activities will include, but are not limited to, legal and illegal activities such as entertainment, banking, networked communication, identity theft, information theft, and monetary theft. Examples of the scope of global activity in cyberspace in the early 21st century include approximately 1.6 billion internet users (or 24 percent of people on earth);[27] approximately 190 million direct broadcast satellite (DBS) television viewers;[28] and more than 175 million Facebook users.[29] In November 2008, nearly U.S. $3Trillion were moved electronically per day in electronic funds transfers (EFT).[30]

Paralleling the rapid expansion of civilian cyberspace use is the increasing use of cyberspace by modern militaries. Many militaries now rely almost exclusively on cyberspace to move information to decision makers–commanders and troops. Military uses of cyberspace include e-mail (unclassified and classified), chat (in various commercial formats), Video Teleconference (VTC), Global Command and Control System (GCCS), Global Transportation Network (GTN), In-Transit Visibility (ITV), Joint Tactical Radio System (JTRS), Blue Force Tracker (BFT), Theater Battle Management Control System (TBMCS), Link 11 and Link 16 Data Link Systems, Unmanned Aerial Systems (UAS, i.e. Global Hawk and Predator), Global Positioning System (GPS), and Joint Direct Attack Munitions (JDAM).

DOD Cyberspace Operations

The likelihood of tactical actions in cyberspace having strategic effects has led the U.S. Department of Defense to develop specific organizational structures for cyberspace operations.

[**] New media and social networking enable near instantaneous direct communication between individuals and groups. Both use cyberspace and electronics to move information in order to influence human decision making. New media and social networking are extremely important to understanding social interaction and decision making, mainly because of the potential viral nature of this type of communication; however, they are beyond the scope of this paper.

In his 2007 article, *Warfighting in Cyberspace*, Lieutenant General Keith Alexander, USA, Director of the National Security Agency (NSA) and Commander Joint Functional Component Commander – Network Warfare (JFCC-NW), described how the U.S. Department of Defense is organized for operations in cyberspace:

> We have redefined our cyberspace mission area in terms of offensive–network warfare (NW) and defensive–network operations (NetOps)–and established JFCC–NW and JTF– GNO to address each of those mission sets, respectively. As directed by the USSTRATCOM Commander, the Joint Functional Component Command for Network Warfare (JFCC–NW) was established to "optimize planning, execution, and force management for the assigned missions of deterring attacks against the United States, its territories, possessions, and bases, and employing appropriate forces should deterrence fail, and the associated mission of integrating and coordinating [Defense Department]CNA [computer network attack] and computer network defense as directed by headquarters USSTRATCOM." The command further defines *network warfare* as "the employment of computer network operations with the intent of denying adversaries the effective use of their own computers, information systems, and networks." This mission statement recognizes the primacy of the strike or attack aspects of computer network attacks as a military fire, not merely as an enabler for cognitive effects. USSTRATCOM has also begun to develop tactics, techniques, and procedures and other concepts designed to integrate cyberspace capabilities into cross-mission strike plans. We are developing concepts to address warfighting in cyberspace in order to assure freedom of action in cyberspace for the United States and our allies while denying adversaries and providing cyberspace enabled effects to support operations in other domains. These concepts, and the cyberspace effects that they focus on, are clearly based on the military concepts of strike, fires (supporting and suppressing), and defense. While the concepts of NW and NetOps are a good start, they represent only a small subset of the elements of military power available within or enabled by cyberspace. In order to fully engage in the development of joint doctrine within the cyberspace domain, it is also necessary to develop a definition of exactly what warfare within cyberspace – or cyberspace warfare - is.[31]

In June 2009, the Department of Defense reorganized, consolidating under one command the network warfare and network operations discussed by General Alexander. Secretary of Defense Robert Gates directed that the Commander, U.S. Strategic Command (CDRUSSTRATCOM) establish U.S. Cyber Command (USCYBERCOM) as a subordinate unified command.[32] The 23 June 2009 establishment memorandum directed the CDRUSSTRATCOM to delegate authority to conduct specified cyberspace operations (the functions previously done by JFCC-NW and JTF-GNO) of the Unified Command Plan to the Commander USCYBERCOM. Secretary Gates stated,

> Cyberspace and its associated technologies offer unprecedented opportunities

> to the United States and are vital to our Nation's security and, by extension, to all aspects of military operations. Yet our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.[33]

Clearly military, civilian, friend, and foe have a vested interest in operating in cyberspace. Even Sun Tzu, in the 4th century BCE, wrote of the importance of communicating, elevating it to one of his nine crucial battlegrounds. Sun Tzu's representation of communicating ground is described as "ground equally accessible to both the enemy and me is communicating."[34] Tu Mu, an interpreter of Sun Tzu, later attempted to qualify this by stating that, "This is level and extensive ground in which one may come and go, sufficient for battle and to erect sufficient fortification."[35] Both of these prophetic descriptions of communicating ground are applicable to cyberspace. Cyberspace is a domain in which both friendly and enemy forces have ability to achieve equal access.

Perhaps no nation state understands cyberspace, its potential and the integral nature of human activity within cyberspace better than China. In the late 20th century, China made the astute decision to focus on the asymmetric possibilities of cyberspace, dedicating precious resources to this mission. There have been innumerable Chinese military strategy books written on cyberspace operations, information warfare, information operations, and electronic warfare. The 1999 classic *Unrestricted Warfare*, written by two Chinese Colonels (Liang and Xiangsui), frames future war as 'war beyond its traditional military domain'. Importantly, the colonels describe 'domain' as a concept derived from the concept of territory and used to delineate the scope of human activities.[36] In their 'war beyond limits' treatise, the colonels state that, 'All of these things are rendering more and more obsolete the idea of confining warfare to the military domain…'.[37] Two other leaders in the Chinese movement are Shen Weiguang and Dai Qingmin. One of Shen's primary works is titled "*World War, The Third World War–Total Information Warfare*". Dai has written works on integrating network and electronic warfare. Colonels Liang and Xiangsui state, "The expansion of the domain of warfare is a necessary consequence of the ever-expanding scope of human activity, and the two are intertwined."[38] China understands the crucial intertwining of human activity with electronics and the electromagnetic spectrum and that cyberspace will play a huge role in future war.

Given the passive nature of civilian and military cyberspace use, and given the distinct advantage others have in this field, America's military must develop expertise in how war is waged in cyberspace. One hurdle is our national tendency to gravitate toward technical solutions rather than abstract solutions. With the exception of the electronics, cyberspace cannot be seen or touched. Another hurdle is our natural human tendency to favor familiar (the original four domains–land, maritime, air and space) and to approach the new domain of cyberspace with confusion and/or apprehension. Both of these hurdles must be overcome, as armed forces reluctant to evolve are destined for failure. While all the possibilities for waging war in this

domain have not yet been unearthed, military leaders must be comfortable with this domain. They must understand the domain–human activity as well as technology; be familiar with the methods used to wage war in this domain to date; and be open and creative enough to envision new possibilities.

Perhaps the first step in understanding the domain is to view the current state of flux through the lens of the then changing 19th century maritime domain. While men had been sailing ships at sea for thousands of years, moving cargo and currency and conducting trade, communications, and logistics; the mid-19th century brought forth the first wrought iron steamship, the SS Great Britain. Some say Isambard Kingdom Brunel's invention changed the way men thought about the maritime domain. Prior to this ship, the movement of mail and priority cargo was conducted between the United States and the United Kingdom on the most reliable and secure sailing ships. These ships were known as packet ships.

An 1858 New York Times article titled *The Last of the Packet Ships*, documented this transition. The article lamented the downfall of New York's thriving ship building and communication industries that was brought about by the changes in shipping from wood and canvas to iron and steam. The article stated, "The obvious advantages of such an arrangement were so great that passengers and shippers gave preference to the ships that could be relied on to sail on a certain day…and their ships were as remarkable for their great speed…and their regularity of sailing."[39] The article continued, "In accomplishing this work, England has gained a greater victory than she did at the Nile or Trafalgar, and Britannia may again wave her trident in triumph."[40] The SS Great Britain and her sister ships could virtually guarantee that a passenger (and cargo to include mail) would arrive on time, well ahead of any sail powered rivals.[41] The steam ship became a reliable means of transportation that was less dependent on wind and other forces of nature. This reliability lead to coal fired, steam powered dreadnoughts at the turn of the 20th century and eventually oil fired battleships and aircraft carriers during World War II. Even nuclear fueled submarines and aircraft carriers are steam powered.

Some felt the steam ship caused the navies of the world to think differently about warfare at sea. Did it? Did the fact that trade, commerce, communication, and military actions all happened faster by more reliable means result in war at sea somehow being new or different? How did Admiral Nelson come to think 'operationally' in the years and months prior to the Battle of Trafalgar? Was Admiral Nimitz's employment of what we now call operational art, when Nimitz conducted Operation GRANITE, the island hopping campaign in the central Pacific Ocean during World War II, different from Admiral Nelson's devices?

Whatever the domain, the importance of understanding operational art and a commander's ability to 'think operationally' cannot be overstressed. In the words of Dr. Milan Vego, operational art "…occupies an intermediate position between policy and strategy on the one hand and tactics on the other. Operational art serves as both a bridge and as an interface between these two areas of study and practice"[42]

21st Century Hybrid Warfare and Cyberspace

In the 2007 document, *A Cooperative Strategy for Maritime Security*, the maritime service chiefs describe conflicts for the early 21st century.

> Conflicts are increasingly characterized by a hybrid blend of traditional and irregular tactics, decentralized planning and execution, and non-state

> actors using both simple and sophisticated technologies in innovative ways.[43]

Hybrid wars were described by General James N. Mattis, USMC and LtCol Frank Hoffman, USMC (Ret.) in 2005 as a merger of different modes and means of war.[44] These modes and means include conventional, psychological, networked, irregular, terror, violence, coercion, information, and crime. It is "multi-modal or multi-variant rather than a simple black and white characteristic of one form of warfare."[45]

In the *Origins and Development of Hybrid Warfare,* Hoffman discusses new principles appropriate to Liang and Xiangsui's "beyond-limits combined war."

> **Omni-directionality** – requires that commanders observe a potential battlefield without mental preconditions or blind spots. The designing of plans, employment measures, and combinations must use all war resources which can be mobilized. The commander is enjoined to make no distinction between what is or is not the battlefield. All the traditional domains, (ground, seas, air, and outer space) as well as politics, economics, culture, and moral factors are to be considered battlefields.
> **Synchrony** – enjoins on commanders to link the disaggregated nature of multiple battlefields in different domains with consideration of the temporal dimension. In other words, "conducting actions in different spaces in the same period of time" to achieve desired effects. Instead of phases with the accumulated results of multiple battles, strategic results can now be attained rapidly by simultaneous action or at designated times.
> **Asymmetry** – here the authors recognize that asymmetry manifests itself to some extent in every aspect of warfare. However, asymmetry has been sought in operational terms within traditional military dimensions. In war beyond limits, the spectrum for overlooking the normal rules is much wider.[sic][46]

Cyberspace and hybrid war are natural partners. As the intertwining of domains with human activities continues to grow, so will the utilization of cyberspace operations to achieve objectives. In discussing the activities associated with hybrid war, Frank Hoffman states,

> These multimodal activities can be conducted by separate units, or even the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical *and* psychological dimensions of conflict. The effects can be gained at all levels of war. [47]

A recent example of hybrid war is the summer 2006 war between Israel and Hizballah. Hizballah proved successful in mixing an organized political movement with decentralized cells that were able to conduct hybrid warfare. The Israeli Defense Force (IDF) thought it was facing the same old guerilla force, but soon found out it was fighting a hybrid force in the air, land, maritime, space and cyberspace domains. Hizballah fought Israeli tanks with Russian made anti-tank weapons; fired C-802 anti-ship cruise missiles at Israeli ships; fired surface to air missiles at Israeli Air Force (IAF) aircraft; kidnapped IDF soldiers; conducted armed reconnaissance with

unmanned aerial systems (UASs); intercepted IDF cell phones; and even intercepted and decrypted U.S. - made single channel ground and airborne radio system (SINCGARS) frequency hopping combat radio transmissions.[48]

Hizballah also hacked into several websites to communicate the message of Al-Manar (Arabic for the beacon) television to a global audience. Specifically, they hacked into a Texas cable company in order to use their internet protocol address as a base to run web sites that broadcast Al-Manar television.

> Al-Manar, widely considered a mouthpiece for Hizballah and categorized as a terrorist group by the U.S., linked into the small cable company's IP (Internet Protocol) address, which can be thought of, in simple terms, as a telephone number. Hizballah essentially added an extension on that telephone line allowing their traffic to flow. Hizballah then gets word the out through e-mail and blogs that it can be found at that IP address and the hijack is complete.[49]

Hybrid warfare is often described as the blurring and blending of war forms in combinations of increasing frequency and lethality.[50] The seemingly amorphous Hizballah achieved success by utilizing disciplined, highly trained and distributed cells to conduct omni-directional, synchronous, and asymmetric operations. A significant portion of their success can be linked to cyberspace operations. Hacking computer systems, communicating via the internet, flying computer controlled UASs, and intercepting cell phone and radio communications clearly demonstrate the employment of cyberspace operations where the primary purpose is to achieve military objectives in or through cyberspace. Less conspicuous, but still extremely successful, uses of cyberspace in Hizballah's hybrid warfare are the extensive communication, recruiting, training, fundraising and propagandizing. In addressing irregular methods, General Mattis provides sound guidance: "They seek to accumulate a series of small tactical effects, magnify them through the media and by information warfare…This is our most likely opponent in the future."[51]

General Alexander states that the ultimate strategic objective of these [cyberspace] operations is to ensure freedom of action within cyberspace and to deny the enemy the same."[52] Similarly, "Autonomous communication is the paramount objective for Hizbollah [sic]."[53] Hizballah hybrid warfare employs various modes of modern communication to link actions to human decision makers in order to terrorize, thereby influencing human decision making. Josef Goebbels, Hitler's Minister of Propaganda, once said: 'We do not talk to say something, but to obtain a certain effect'.[54]

Goebbel's statement demonstrates that human activity – decision and the intent behind those decisions – is as fundamental to cyberspace as the technology. Our society is bewitched with technology, often seeing it as the decisive, sanitary answer to whatever problem is on the table. Many modern decision makers, both civilian and military, view cyberspace operations as interconnected, globalized, clean and precise. Indeed in his 1996 essay *The Emerging Primacy of Information*, Martin Libicki put forth the argument that "cyberspace will tend to eliminate geopolitics through its influence on military security, rather than (or at least in addition to) its influence on international politics."[55] This belief in the 'magic bullet' is as dangerous today as it was during all previous wars. As Clausewitz so eloquently stated,

> Kind-hearted people might of course think there was some ingenious way to disarm or defeat an enemy without too much bloodshed, and might imagine this is the true goal of the art of war. Pleasant as it sounds, it is a fallacy that must be exposed: war is such dangerous business that the mistakes which come from kindness are the very worst. The maximum use of force is in no way incompatible with the simultaneous use of the intellect.[56]

Cyberspace is an important and evolving domain of warfare, but the reality is that no matter how much technology is used to conduct kinetic or non-kinetic operations in any or all of the domains; war is still as Clausewitz states "an act of force to compel our enemy to do our will."[57] Cyberspace operations are just as capable of violent, dirty, and deadly facets of the Battle of Thermopylae, Nelson's Battle of Trafalgar, and Strategic Bombing of World War II. Further, cyberspace operations do not occur in a vacuum. Enemies are not a machine or a piece of technology. Clausewitz states, "In war, the will is directed at an animate object that *reacts*."[58]

Examples of Early 21st Century Cyberspace Use

Cyberspace warfare is warfare. Our military must understand the possibilities – offensive and defensive within this domain. However, the domain is so new that most have not yet dipped their toes into the pool. The following examples of cyberspace operations to date should not be considered an all-inclusive list of options; rather they should be considered a springboard to new possibilities.

Cyberspace is used for communication, research, banking, shopping, entertainment, record keeping, recruiting, planning, and just about any activity that can be done in the other domains. Therefore, any of these activities can be adversely affected by cyberspace. It is important to understand how our adversaries can and will use operations in cyberspace for their advantage. Most Americans are aware of familiar cyberspace dangers, like malware, phishing, whereby personal information is illegally, and sometimes unknowingly, accessed, resulting in identity theft. Other common cyberspace dangers are detailed by Melissa Hathaway, Cyber Coordination Executive for the Office of the Director of National Intelligence, in an October 8, 2008 Op-Ed piece, describing cyber 'attacks' on information:

- **Information theft.** Stealing data from a target personal device, system or network is the most common threat. For example, a disgruntled Boeing employee was charged last year with lifting more than 320,000 sensitive company files by using a thumb drive to tap the corporate system. Boeing estimated that the stolen documents would have cost it between $5 billion and $15 billion in lost revenue had they been given to competitors.
- **Information disruption.** Hackers who sneak into government systems and alter crucial operating data are a growing concern. In 2006, a disgruntled Navy contractor inserted malicious code into five computers at the Navy's European Planning and Operations Command in Naples, Italy. Two computers were rendered inoperable when the program was executed. Had the

other three computers been knocked offline, the network that tracks U.S. and NATO ships in the Mediterranean Sea and helps prevent military and commercial vessels from colliding would have been shut down.

- **Information denial.** Cases in which private or government computer systems are shut down by floods of automated hits are also on the rise. In April 2007, Russian nationalists used such a "distributed denial of service" attack to block access to the networks of the Estonian parliament, the president's office and many of that country's banks, news organizations and Internet service providers.[sic] [59]

Attacks of this nature are serious on a small scale, but could be catastrophic on a large scale. There have been recent examples of cyberspace used in terrorists operations, as one segment in hybrid warfare, as the foundation for both state and non-state actor security ambitions, and in privateering.

Mumbai, India

In November 2008 a little known terrorist group named Lashkar-e-Taiba (LeT) conducted three days of terror in the Indian metropolis of Mumbai, killing 179 and wounding over 325 people. Their operation was extremely well planned and executed, utilizing cyberspace operations to achieve their objectives. Voice over Internet Protocol (VoIP) was used extensively to orchestrate their operations.[60] Global Positioning Systems (GPS) were used to navigate from the home base, and Google Earth maps were used to survey the operations area.[61] To highlight the global and near instantaneous aspects of cyberspace, an interesting point in the use of VoIP is that the call server used by the terrorist organizers was based in the U.S. The fact that the communication nodes were physically located on the other side of the earth had little or no adverse effect on the operation. In fact it aided the terrorists in that when the security forces tried to locate those directing the attacks, they had great difficulty because of the use of VoIP. The New York Times reported:

> Indian security forces surrounding the buildings were able to monitor the terrorists' outgoing calls by intercepting their cellphone signals. But Indian police officials said those directing the attacks, who are believed to be from Lashkar-e-Taiba, a militant group based in Pakistan, were using a Voice over Internet Protocol (VoIP) phone service, which has complicated efforts to determine their whereabouts and identities.[62]

Russia-Georgia

There was a dedicated attack on Georgian government web sites in the summer of 2008. The cyber attacks pre-dated the actual movement of forces and kinetic operations. While it has not been proved that the Russian government conducted or condoned the cyber attacks, it has been generally accepted that many of the computers orchestrating the attacks were controlled by Russian hackers. A Los Angeles Times editorial reported,

> Analysts say the online attacks, which appear to have begun well before

> Russian tanks rolled in, resembled the work of garden-variety cyber pranksters. Georgian government websites were overwhelmed with swarms of data, and some were defaced by hackers. There was no clear proof of Russian military involvement (investigators have reportedly traced some of the data to Russian servers tied to organized-crime groups), so the perpetrators may have been nationalists. Still, the timing suggests that even if the responsible parties weren't in uniform, they coordinated their moves with the Russian military.[63]

Most of the media reports centered on the use of BotNets to conduct distributed denial of service (DDoS) attacks against Georgian government and civilian web sites.[††] Bots or robots are remote controlled pieces of malicious software that are inserted into one or more computers. Once a computer becomes infected by the Bot, it becomes a tool or weapon–a lasting legacy of the hacker. Typically, a small group of hackers can create and control a network of bots–a BotNet. BotNets have been known to exceed 100,000 computers. A Bot herder, a hacker with oversight of the BotNet, gives a signal and his network can launch tens of millions of packets of information all aimed at the same or multiple targets. If the target is a server that runs a government website or communications node, the massive amount of information packets sent by the BotNet can simply overload the server and supporting infrastructure, shutting them down, and denying service to legitimate users. This is what is commonly termed a distributed denial of service (DDoS).

In the Russia-Georgia incident, the individuals conducting the DDoS had at least two objectives-one physical and one cognitive. The first objective was disabling the communications network of the Georgian leadership prior to the movement of Russian Forces into South Ossetia. This can be seen as synchronizing command and control and operational fires. The DDoS shut down much of the Georgian government's communication inside Georgia and to the outside world.

The second objective was to create fear and discontent within the Georgian population. The attackers inserted pictures of Adolf Hitler into government web sites.[64] These pictures were linked to existing and modified pictures of Georgian President Mikheil Saakashvili to make him appear *Hitleresque*. This had a great psychological impact on the citizens of Georgia due to their history with Nazi Germany. Additionally, the Russian government broadcast into Georgia television and radio programming that supported Russian interests. The people in control of the computers, television, and radio were able to manipulate the information environment.

The use of cyberspace operations to control the information environment created great problems for the Georgian government. President Saakashvili could not communicate with his leadership or his people and he could not allow the attackers (cyber, television, and radio) to continue. Ultimately, the Georgian government took down the television and radio broadcasts from Russia to prevent further manipulation of the Georgian people.[65] In this case, the adversary (Russia) was able to link cyberspace operations and information operations to control the narrative.

Al-Qaeda

[††] BotNets are a network of remotely controlled bots.

Following Operation ENDURING FREEDOM in 2001, Al-Qaeda and its Associated Movements (AQAM) moved from planning and training in their strongholds in Afghanistan to a distributed form of distance learning on the World Wide Web. Muaskar al Battar and numerous other web sites provide support, education, and training that leads to kinetic actions. The Muaskar al Battar web site opens with:

> Oh Mujahid [holy warrior] brother, in order to join the great training camps you don't have to travel to other lands. Alone, in your home or with a group of your brothers, you too can begin to execute the training program. You can all join the Al Battar Training Camp.[66]

The name of this organization is significant in that Al Battar is the sword of the prophets. Swords in general represent prominent themes in Islamic thought. "Swords are seen as noble weapons that embody the purity, nobility, and overall righteousness that is associated with early Islamic heroes and their jihadi campaigns."[67]

> The al-Battar sword was taken by the prophet Muhammad as booty from the Banu Qaynaqa. It is called the "sword of the prophets" and is inscribed in Arabic with the names of David, Solomon, Moses, Aaron, Joshua, Zechariah, John, Jesus, and Muhammad. It also has a drawing of King David when he cut off the head of Goliath to whom this sword had belonged originally. The sword also features an inscription which has been identified as Nabataean writing.[68]

Since its inception Al-Qaeda's on-line training has evolved "to include small unit infantry tactics and intelligence operations such as collecting data, recruiting members of state security services, and setting up phone taps."[69]

Web sites such as Al Battar, Al-Manar and the manipulation of the Georgian government sites are examples of how cyberspace operations are used to achieve objectives. In the words of Dr. Kuehl, these web sites are using cyberspace in shaping and changing the three dimensions of the information environment. They create information content itself (a Web page), share that content through new forms of connectivity (the Internet links make that Web page accessible to a billion plus people), and affect human interaction and communication. Web sites are a key to the intertwining of cyberspace and human activity in that they represent some of the most prolific ways to influence people to decide and act in ones favor.

People's Republic of China (PRC)

Demonstrating a nation state's perspective on cyberspace, numerous Chinese authors have written on the importance of utilizing the 'information superhighway'. In their influential 2005 document *Warfare Strategy Theory*, Major Generals Peng Guangqian and Yao Youzhi assert that:

> It is necessary to be proficient at utilizing the information superhighway, creating misleading information, spreading the fog of war, and jamming and destroying the enemy's strategic awareness, thereby using strategy

> to control the adversary. It is necessary to be proficient at using electronic feints, electronic camouflage, electronic jamming, virus attacks, and space satellite jamming and deception leading the enemy to draw the wrong conclusion and attaining the goal of strategic deception. [70]

China's use of cyberspace centers on computer network exploitation to achieve its national strategic objectives. Their strong reliance on the electromagnetic spectrum defines the essence of Chinese Information Warfare (IW). However, the human element of warfare remains equally important. Shen Weiguang, China's "father of information warfare" lists the main tasks of IW as disrupting the enemy's cognitive system and its trust system.[71] In the early 21st century, China has used cyberspace to data mine terabytes of information from U.S. science, technology and military computers. One of the most well known of these cyber incidents is Titan Rain, an attack independently corroborated by other nations. The joint program, Information Warfare Monitor Project, between Canada's University of Toronto and the United Kingdom's Cambridge University, expands on Chinese cyberspace operations:

> The cyber attacks against the U.S. stand out because security researchers have traced them back to the Chinese government. "Normally it is not possible to attribute the source of an attack, because source addresses can be spoofed," says Alan Paller, director of research at the SANS (SysAdmin, Audit, Network, Security) Institute in Bethesda, Md., which trains and certifies technology workers in cyber security. In China's case, though, analysts tracked a series of 2005 cyber assaults against U.S. computers—dubbed "Titan Rain"—to 20 computer workstations in China's Guangdong province, Paller says.[72]

TIME Magazine reported in 2005 that the hackers were "…eager to access American know-how…"[73] The article continued,

> Beyond worries about the sheer quantity of stolen data, a Department of Defense (DOD) alert obtained by TIME raises the concern that Titan Rain could be a point patrol for more serious assaults that could shut down or even take over a number of U.S. military networks.[74]

In April 2009 the Wall Street Journal reported that the U.S. electric grid had been penetrated by cyber spies. "The Chinese have attempted to map our infrastructure, such as the electric grid."[75] The article continued, "Authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure components, the senior intelligence official said. He added, "If we go to war with them, they will try to turn them on."[76]

There are now many organizations at work attempting to understand China's objectives. The Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas has been studying China for a while.[77] In *Dragon Bytes–Chinese Information Warfare Theory and Practice*, Tim Thomas a senior analyst at FMSO quotes from one of the primary Chinese publications - *Information Warfare*.

> There will be point-to-point confrontation between computers as well as theater-to-theater confrontation. There will be wireless confrontation as well as via cables…there will be wartime confrontation as well as confrontation in peacetime. There will be confrontation between military computers as well as between civilian computers.[78]

China's use of the electromagnetic spectrum has become increasingly pervasive - so much so that it is easy to see the threads in modern Chinese writings of Sun Tzu's strategies of "Know the enemy and know yourself; in a hundred battles you will never be in peril and … those skilled in war subdue the enemy's army without battle."[79] Mr. Rafal Rohozinski, the Principal Investigator, Information Warfare Monitor and the SecDev Group speaking at the April 2009 Information Warfare Conference–InfowarCon stated that 51% of all malware reports back to computers located in China.[80] In his article *China's Electronic Long-Range Reconnaissance*, Tim Thomas discusses China's People's Liberation Army's (PLA) use of electronic stratagems for their computer network operations:

> Computer network operations have become part of the peacetime strategic activities of the PLA. More worrisome is the purpose of these incursions. Is it reconnaissance? Or is the purpose of these incursions to place Trojan horses or some other device into U.S. and other partner systems to disable or destroy them in case of war?[81]

Privateers and Information Currency

Direct linkages to the nation states of Russia and China are sometimes difficult to solidify due to the ubiquitous nature of human activities in cyberspace. Many cyber analysts feel that nation states are now making attacks even more difficult to track by the new practice of issuing 'letters of marque' to individuals and groups, who then act on behalf of the nation state.[82] These cyberspace privateers use their personal computers to navigate the cyber domain and are 'authorized' by the nation states to perform functions necessary to those nations' interests.

Information is a currency. Information resident in the electronics, computers, smart phones, servers et al. of the 21st century is just as important today as the information needed by the Soviet Union to run its SCADA systems was in the early 1980s. While privateers of old were allowed to keep a percentage of the booty taken from enemy ships captured at sea, the 21st century prize and booty consist of access to computers and their resident information. Nation states are often looking to obtain military, science, technology, engineering, and math information. The privateers utilize computer network operations (exploitation and attack) to access that information. Information not deemed valuable enough for a nation state to process and utilize for its own gain can easily be left as booty for the cyberspace privateers. Examples of privateer booty are identity or financial information such as social security or credit card numbers. This type of information has value; it can be sold to organized criminals who can use it to create fraudulent identities or fake credit cards.

Whether it is a non-state adversary such as Hizballah, Al-Qaeda, or nation states such as China and Russia, the future is bright for those who can operate and fight in the cyberspace domain.

Operational Art and Cyberspace

The challenge of understanding this global domain and what it means to military leaders can be aided by embedding the events that happen in cyberspace in the context of operational art (Op Art). The study of the operational art of war can and should take time. Volumes have been written on the art of warfare. Sun Tzu's *Art of War*, Clausewitz's magnum opus *On War,* and Dr. Milan Vego's tome *Joint Operational Warfare–Theory and Practice* are but a few of the great works that investigate and analyze operational art. Op Art is "…the field of study that orchestrates all available sources of military and nonmilitary power in order to accomplish the ultimate strategic or operational objective."[83]

Op Art begins with basic questions: What are the objectives of the person or people conducting operations? What effects are they trying to achieve? Op Art can be broken into smaller parts in order to build an 'operational' picture. For the purposes of this paper, the discussion of Op Art will be confined to the elements of operational factors and functions. These elements include the factors of space, time, and force. U.S. Joint doctrine identifies the following functions: command and control, intelligence, fires, movement and maneuver, protection, and sustainment.[84] Dr. Vego states, "For maximum effectiveness in the employment of one's combat forces, a number of supporting structures and activities, arbitrarily called "functions," should be fully organized and developed."[85] It should be noted that U.S. Joint doctrine and Dr. Vego differ slightly on what elements should be included as operational functions.[86] However, Dr. Vego goes on to say, "The list of what constitutes an operational function should not be considered something unchangeable."[87]

In his 1989 article *The Loose Marble–and the Origins of Operational Art*, James Schneider states, "The Hallmark of operational art is the integration of the temporally and the spatially distributed operations into one coherent whole."[88] He goes on to say that the two characteristics at the heart of operational art are simultaneous and successive operations.[89] The ubiquitous nature of cyberspace means that understanding operational art is key to understanding cyberspace operations.

Cyberspace is unique in that it provides the avenue for huge amounts of data and information to cross all levels of war from the tactical to the strategic and to move from one domain to another–nearly instantaneously. Movement through cyberspace is not constrained by the traditional physical movements normally considered by humans. This speed and unrestricted movement requires the military commander to seriously consider the relationship between the operational factors of time, space and force, and how the factors affect the operational functions. The relationship between factors and functions is important in that if a commander has a disadvantage in one, he needs to utilize strengths from the others to overcome that disadvantage. Conversely, if the commander has an advantage in one, he needs to utilize the others to achieve victory.[90]

Nimitz and Nelson

Admirals Nimitz and Nelson displayed an intuitive understanding of operational art. Each achieved great success only after he had studied his profession of arms and planned for multiple contingencies. The following examples show why our military should study the cyberspace domain in the context of operational art.

Much has been written about Operation GRANITE, Admiral Nimitz's island hopping campaign through the Central Pacific. Operation GRANITE, a series of amphibious landings

and battles, was a component of the U.S. efforts that led to the unconditional surrender of Japan. An understanding of the manner in which U.S. and allied forces successfully defeated the Japanese serve as an in depth study of operational art.

Nimitz displayed his understanding of operational factors and functions in many ways; bypassing certain islands to offset a temporal disadvantage, having the right forces to attack; conducting operational fires in the bombing of the Japanese long range aircraft on Formosa, organizing the logistics necessary to support mobile forces, and combining the command organization of 3rd and 5th Fleets-one conducting planning and one conducting operations (the key to maintaining tempo and keeping the Japanese off balance) were all parts of the successful employment of operational art.

Suffice it to say Admiral Nimitz understood the factors of space, time, and force and balanced the use of functions to achieve success. He did not have to think differently about operations because his ships were steam vice sail powered, or because he had carrier based aviation and amphibian tractors to project force instead of cannon and Royal Marines in longboats. Nimitz's ability to achieve victory through the balancing of operational factors and functions came in part from his year at the Naval War College. In a letter written to the President of the War College forty years after his attendance, he said:

> The enemy of our games was always–Japan–and the courses were so thorough that after the start of WWII – nothing that happened in the Pacific was strange or unexpected. Each student was required to plan logistic support for an advance across the Pacific – and we were well prepared for the fantastic logistic efforts required to support the operations of war…I credit the Naval War College for success [as] I achieved in strategy & tactics both in peace & war.[91]

When speaking of Nelson's great victories, his ability to lead and achieve decisive victories is most often mentioned. Both leadership and experience are major parts of what make up the ability to "think operationally." Geoffrey Till discussing an operational approach to securing command of the seas, states,

> Although we tend to focus on Nelson's tactical conduct *at* the Battles of the Nile or Trafalgar, his ultimate operational skill lay less in that than in the successful campaigns he had conducted *beforehand* to ensure that those battles were indeed fought and conducted under favourable conditions.[92]

The Royal Navy's *Fighting Instructions* of the day were focused on fighting an enemy at long range utilizing their superior cannon and strict operational command. This often led to indecisive battles. Geoffrey Till's *beforehand* in part refers to the winter and spring of 1805 Nelson spent chasing his opponent across the Atlantic and back. During this time Nelson refined both his skills and operational thinking.

In May 1805, Nelson published his own *Instructions*, which led ultimately to the document that became known as his "Trafalgar Memorandum." The Trafalgar Memorandum lays out Nelson's understanding of the operational factors at hand and how he envisioned operational command. The most significant change to *Fighting Instructions* comes from what has been

labeled as the 'Nelson's Touch'. "Captains are to look to their particular line as their rallying point. But in case signals can neither be seen nor perfectly understood, no Captain can do very wrong if he places his ship alongside that of an enemy."[93] When Nelson's instructions were disseminated to his Captains, he wrote: "When I came to explain to them the *Nelson touch*, it was like an electric shock. Some shed tears, all approved–'It was new–it was singular– it was simple! And from admiral downward, it was repeated–It must succeed, if ever they will allow us to get at them.'"[94]

Like Nimitz, Nelson displayed his understanding of operational factors and functions in various ways. Upon arrival off the Spanish coast on 14 September 1805, he found the opposing fleet in the port of Cadiz. Understanding that winter and foul weather would soon approach, Admiral Nelson instructed his larger ships of the line to remain out of sight and his smaller faster frigates to move in close. His purpose was to collect intelligence and to entice the combined French and Spanish fleets to come out and fight. Nelson's operational movement and maneuver worked and the combined fleets sailed 20 October. As the battle approached, Nelson knew that command and control would be nearly nonexistent once the enemy was engaged. He instructed the now famous signal to be hoisted, "England expects every man to do his duty." The Battle of Trafalgar took place the 21st of October. The combination of the Trafalgar Memorandum and the signal flags became Nelson's command and control of the fleet. In an official dispatch following the battle, Admiral Collingwood, who took command of the battle when Nelson was mortally wounded stated, "as the mode of attack had been previously determined on and communicated to flag-officers and captains, few signals were necessary."[95] Clearly Nelson's ultimate operational skill off Cape Trafalgar in October 1805 was in part due to his understanding and employment of what would become known as operational art.

Thoughts on Operational Art and Cyberspace Operations

Some of the challenges that operational commanders face will be knowing where and how the cyberspace operations are being used. For example, when a bomb falls on a target, did it come from a manned aircraft or a UAS - did the attacker employ cyber capabilities to achieve the objective? Could the UAS have been interdicted by attacking the electromagnetic spectrum; the links between the vehicle and the controller? If the adversary has disrupted the electromagnetic spectrum – can you still use it? What are the objectives of the cyberspace operation? Are they physical or cognitive objectives? The importance of understanding the relationship between factors and functions is stated by Dr. Vego, "A commander's need to fully understand the factors of space, time, and force and then to balance them against the objective is as old as warfare itself."[96]

Operational Factors

Given the examples of Admiral Nimitz and Admiral Nelson, a review of cyberspace in the context of operational art is relevant. A comparison of the fastest ship (approximately 35 knots) and the fastest plane (flies mach 3+ (~2200 mph at sea level)) with digital information (moves via electromagnetic radiation at nearly 670 million miles per hour (or 186,000 miles per second)) shows truly the global nature of cyberspace. The military commander must understand the relationships of time, space, and force when conducting operations in his area of responsibility. A discussion of cyberspace as seen through the lens of the operational factors follows.

Time –There is no set time, as we know it, for cyberspace. Digital packets moving through cyberspace travel at approximately the speed of light. A digital message or an image can move around the world nearly instantaneously.
Space – Cyberspace is all around us–it is truly a global domain. The nodes made up by electronics exist in the four traditional domains. Examples include: servers, computers, cellphone towers, and power plants et al. on land; planes, radars, UASs et al. in the air; ships, radars, missile defense ships et al. at sea; and satellites in space. Traditional lines are blurred when messages covertly hosted on a server in Texas are read in the Middle East. These messages then influence people to act. VoIP companies in the U.S. unwittingly provide C2 networks for non-state and nation states wanting to harm U.S. forces.
Force – David can defeat Goliath with an asymmetric attack. A single hacker or Bot Herder can coordinate thousands of computers to accomplish millions of actions in a cyber attack. A belligerent or privateer with a personal computer can obtain corporate or military information or worse shut down a SCADA power grid, which could result in death.

How does the operational commander utilize cyberspace in managing the IE to get his message out in Counter Insurgency or Humanitarian Assistance / Disaster Relief Operations? In an 18th century example of commander understanding the IE, when he felt his story was not being told 'correctly', Napoleon formed or took control of various newspapers that then presented his side of the story.[97] In fact, Napoleon was reputed to have said, "Four hostile newspapers are more to be feared than a thousand bayonets."

Operational Functions - (Joint Publication 3-0)

As warfare becomes more complex, the intertwining of activities among all five domains will only increase. The increased complexity can be mitigated by understanding which functions need to be performed. Dr. Milan Vego provides keen insight into the importance of operational functions. "The operational commander is responsible for properly sequencing and synchronizing not only joint forces but also operational functions, prior to and in the course of a campaign or major operation."[98] In early 21st century warfare the manner in which the commander thinks about, sequences, and synchronizes the operational functions with respect to cyberspace and cyberspace operations will be crucial to success.
Command and Control – How does a commander organize his joint force when conducting cyberspace operations? Or, perhaps more importantly, how does the commander organize his joint force when the adversary will conduct cyberspace operations against his force? How do Plans and Orders move up and down the chain of command when the electromagnetic spectrum is disturbed or denied? Is it possible to counter an adversary's use of cyberspace? How should a commander organize his/her command to get his/her message out before his/her adversaries? In a disrupted or denied electromagnetic environment can the operational commander communicate with his subordinates and superiors? Can the adversaries' command and control be countered?
Intelligence – What does a commander do when his Special Forces team is conducting strategic reconnaissance and he cannot communicate with them via cyberspace? How much 'secure' information is stored on a computer or moved through cyberspace? How much knowledge about you has your adversary gained by observation, investigation, analysis, and understanding via cyberspace?
Fires – If GPS is degraded or denied, will precision guided munitions work? What other options does the commander have to put fires on targets? Can cyberspace be used to facilitate or conduct

operational fires, either by you or your adversary?
Movement and Maneuver – In a disturbed or disrupted electromagnetic environment, how do you navigate at sea or in the desert if GPS does not work? How does the fact that the U.S. military uses unclassified, commercial off- the-shelf software similar, to FEDEX and UPS, in tracking global shipments of military cargo affect the Time Phased Force Deployment Data (TPFDD) and receipt of cargo at a Seaport of Debarkation (SPOD) or Airport of Debarkation (APOD)? What decisions must the commander make when he is told by his TRANSCOM Liaison Officer (LNO) that significant parts of his combat power has been sent to the wrong SPOD by a hacker accessing U.S. Transportation Command (USTRANSCOM) computers? ‡‡
Protection – How does a commander need to think about protecting his military and non-military sources of power? How do you protect your force when the enemy is using a C2 node halfway around the world and the combat power (the information) moving through it moves 25,000 miles in nanoseconds? How do you neutralize the C2 in New Jersey or Texas? One of the strengths of the U.S. military is its ability to utilize the IE to integrate information (via technology) and move it to our decision makers faster and more securely than our adversary. Can the data resident in our computer systems be manipulated by outside sources? What happens when our decisions are delayed or we can no longer use the technological advantage we rely on? What happens when a previously low tech adversary gets UASs and precision guided munitions (PGMs) and uses them to collect intelligence or attack? What about hackers gaining access to .mil web sites? Would it be useful to know what types of training manuals (i.e. explosives or biological warfare) people are reading about in the region to which you are deploying? How are Radio Controlled Improvised Explosive Devices (RCIED) being set off?
Sustainment – How does the Combatant Commander's Deployment and Distribution Operations Center (DDOC) track beans, bullets and black oil when the computers don't work?

The 21st century military commander must be able to 'think operationally' about the relationships of the operational factors of time, space, and force and how to balance them against operational functions happening in or through cyberspace.

Conclusion

In discussing cyberspace operations at the National Defense University, Kuehl raised the question, "Has warfare as we understand it, featuring "blast, heat, and fragmentation," become obsolete?"[99] The effects created by the 1981 manipulation of Soviet Union SCADA controls were clearly kinetic and resulted in blast, heat, and fragmentation. The difference between 1981 and now is that the insertion of the computer codes does not have to be done through a person loading a hard drive or floppy disc on to a computer. All an adversary needs is the internet, malware and a good hacker to attack operational forces and/or employ WMD/E.

‡‡ USTRANSCOM is a functional combatant commander whose mission is: Develop and direct the Joint Deployment and Distribution Enterprise to globally project strategic national security capabilities; accurately sense the operating environment; provide end-to-end distribution process visibility; and responsive support of joint, U.S. government and Secretary of Defense-approved multinational and non-governmental logistical requirements. Federal Express (FEDEX) and United Parcel Service (UPS) are commercial cargo and package shippers that pioneered the use of the internet to track the global movement of their cargo. They rely heavily on digital signals sent from their trucks and planes in order to have near real time knowledge of where every piece of cargo is while in transit. USTRANSCOM has adopted a version of these commercial tracking systems.

Cyberspace is a domain in which human activity occurs on a daily basis, and civilian, military, friend and foe utilization of this domain will only continue to grow. Referring back to Frank Hoffman's analysis of 'Beyond Limits Warfare', cyberspace is the medium in which actions can become omni-directional, synchronous, and asymmetric. If the operational functions are properly balanced with operational factors in cyberspace operations, cyberspace and hybrid warfare can be natural partners.

Sun Tzu's thoughts on communicating ground, where all parties have equal access, is as appropriate today as it was in the 4th century BCE. Sun Tzu stated, "In communicating ground, I would pay strict attention to my defences [sic]."[100] This thought can be updated for 21st century warfare; commanders should think defensively about what can and cannot be done in and through cyberspace and with cyberspace operations. If commanders plan to use 'technology' to win, they will need to think first, "What do I need to defend in order to have freedom of action?" Commanders should also think, "What if the technology I need to use is denied?" "Are my computers 100% secure?" The effects created by cyberspace operations can be both kinetic and non-kinetic (lethal and non-lethal). The manipulation of SCADA controls can easily cause mass destruction, as in the 1981 Soviet Union example. But what are the objectives of cyberspace operations? Attempting to achieve ones objectives through cyberspace operations is directly related to compelling humans to act in your favor. Non-kinetic effects can be obtained by manipulating the physical, information and cognitive dimensions of the IE to achieve objectives. As Shen Weiguang said, these could be simply 'disrupting the enemy's cognitive system and its trust system'. If a JTF commander loses trust in the force's systems or capabilities and/or fails to properly employ them–our adversaries have won. Additionally, if a population loses faith in its government or military–the adversary has won. This type of psychological victory fits squarely into the definition of WME. Our enemies and competitors have the capabilities to use cyberspace operations to achieve military objectives and to compel their enemy to do their will.

War in cyberspace is no different than the other four domains. We need to understand the new technology and the human activity behind it. As Clausewitz said, "The invention of gunpowder and the constant improvements of firearms are enough in themselves to show the advance of civilization has done nothing practical to alter or deflect the impulse to destroy the enemy, which is central to the very idea of war."[101] The dangers and risks associated with cyberspace are numerous and great. The importance of learning to fight in the cyber domain cannot be overstated. In the 2009 Quadrennial Roles and Missions Review Report the Secretary of Defense states:

> Our national security is inextricably linked to the cyberspace domain, where conflict is not limited by geography or time. The expanding use of cyberspace places United States' interests at greater risk from cyber threats and vulnerabilities. Cyber actors can operate globally, within our own borders, and within the borders of our allies and adversaries. The complexity and amount of activity in this evolving domain make it difficult to detect, interdict, and attribute malicious activities.[102]

Way Ahead – Information Warfare and Cyberspace Operations

In his futuristic book, *7 Deadly Scenarios, A Military Futurist Explores War in the 21st Century*, Andrew Krepinevich, describes a set of military capabilities that support Chinese

military philosophy. Krepinevich is President of the Center for Budgetary Assessments and consultant to numerous U.S. government agencies. His job has been described as thinking the unthinkable–and to prepare a response in the event our worst nightmare becomes a reality.[103] The Chinese philosophy is called *Shashou jian* or Assassin's Mace. Shashou jian was a club with which the "assassin" incapacitated his enemy, suddenly and totally, instead of fighting him according to traditional rules of combat.[104] Krepinevich states,

> As the U.S. Military increasingly relies on Information as a critical component of its military effectiveness, and the use of networks to gather, organize, and move information, PLA theorists have, for years, argued that the Americans' heavy reliance on cyberspace may be their Achilles heel.[105]

Whether wars are termed asymmetric or hybrid, 21st century cyberspace operations will continue to take advantage of the intertwining of domains and human activity. In discussing hybrid warfare, David Kilcullen states, "today's conflicts clearly combine new actors with new technology and new or transfigured ways of war, but the old threats also remain and have to be dealt with at the same time and in the same space, stressing the resources and overloading the systems of western militaries."[106]

Cyberspace operations can and will be used by current and future adversaries to achieve their objectives. The ability to think 'operationally' is one of the most important attributes for military leaders. The study of operational art creates a foundation for this thinking. While the new DOD structure designates the Commander, U.S. Cyber Command as the primary military actor for cyberspace operations, all commanders need to understand cyberspace operations.

Commanders should expect in future war our adversaries will utilize cyberspace operations to manipulate and/or control information systems and information to decision makers and machines. Here again, Clausewitz has some wisdom for the commanders,

> War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty[107]…The general unreliability of all information presents a special problem in war: all action takes place, so to speak, in a kind of twilight, which like fog or moonlight tends to make things seem grotesque and larger than they really are[108]…But a commander must submit his work to a partner, space, which he can never completely reconnoiter, and which because of the constant movement and change to which he is subject he can never really come to know.[109]

Clausewitz suggests the importance of knowing how to fight a war without the benefits of modern technology and communication systems. How then should an operational commander prepare for war in the 21st century? Certainly, the ability to 'think operationally' begins with a firm understanding of operational art. Secondly, a commander should be prepared to fight with little or no reliable information, as our adversaries have the ability to degrade or deny access to cyberspace. Future operational commanders would do well to heed the words of Colonels Liang and Xiangsui:

> In warfare and non-military warfare, which is primarily national and supra-national,

there is no territory which cannot be surpassed; there is no means which cannot be used in the war; and there is no territory and method which cannot be used in combination.[110]

End Notes

[1] Representation of domain relationships provided by Dr. Daniel Kuehl, National Defense University
[2] Thomas C. Reed. *At The Abyss*, New York, NY. Ballantine Books. 2004, 268
[3] Weapon of Mass Destruction (WMD) defined in U.S. Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication (JP) 1-02, (Washington, DC: CJCS, 12 April 2001 as amended through 19 August 2009). Weapon of Mass Effect defined in Homeland Security Advisory Council Weapons of Mass Effect Task Force on Preventing Entry of Weapons of Mass Effect. January 10, 2006.
[4] Oxford English Dictionary, 11th ed. Domain is defined as an area owned or controlled by a ruler or a government> a sphere of activity or knowledge.
[5] The author is indebted to Captain Stephanie A. Helm, USN for suggesting the operational art framework for this part of the paper.
[6] Winn Schwartau, Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, 2nd edition (New York, Thunder's Mouth Press, 1996), Ch.2, pp. 71-86
[7] Oxford English Dictionary, 11th ed. Wetware is defined as human brain cells viewed as counterparts of computer systems.
[8] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Information Operations*. Joint Publication (JP) 3-13, (Washington, DC: CJCS, 13 February 2006), I-1
[9] Joint Pub 3-13, (Washington, DC: CJCS, 13 February 2006), ix
[10] JP 3-13 defines the CNO capabilities as **computer network attack,** actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves; **computer network defense,** actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks; and **computer network exploitation,** enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
[11] Phishing is a scam where Internet fraudsters send spam or pop-up messages to lure personal and financial information from unsuspecting victims. For more information on phishing see, http://www.onguardonline.gov/topics/phishing.aspx (accessed March 16, 2009)
[12] See David T. Fahrenkrug (Lt Col, USAF), "Cyberspace Defined", in *The Wright Stuff* (Air University, 17 may 2007), at http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html . The Air University has a number of sources on cyberspace; see http://www.au.af.mil/info-ops/cyberspace.htm for a list.
[13] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Eds., *Cyberpower & National Security* (Potomac Books, 2009), 32.
[14] Center for International Media Assistance. Special Report. National Endowment for Democracy. 4. http://cima.ned.org/648/cell-phone-report-2.html (accessed March 16, 2009)
[15] CIA World Fact Book. https://www.cia.gov/library/publications/the-world-factbook/ (Accessed May 5, 2009)
[16] BlackBerry is the registered trademark of Research in Motion. BlackBerry has a variety of smart phones that over 21 million people use on over 375 wireless networks in 140 countries around the world.
[17] Oxford English Dictionary, 11th ed.
[18] Winn Schwartau. *Information Warfare – Chaos on the Electronic Superhighway*, New York: Thunder's Mouth Press, 1994. 49
[19] Robert M. Gates, U.S. Secretary of Defense, Quadrennial Roles and Missions Review Report, January 2009, 15.
[20] General James E. Cartwright, USMC, Vice Chairman of the Joint Chiefs of Staff Memo, August 18, 2009. Definition of Cyberspace Operations,
[21] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Eds., 28
[22] The DHS/USCG goes on to state, Each ship "mark" could reflect the actual size of the ship, with position to GPS or differential GPS accuracy. By "clicking" on a ship mark, you could learn the ship name, course and speed, classification, call sign, registration number, MMSI, and other information. Maneuvering information, closest point of approach (CPA), time to closest point of approach (TCPA) and other navigation information, more accurate and more timely than information available from an automatic radar plotting aid, could also be available. Display information previously available only to modern Vessel Traffic Service operations centers could now be available to every AIS-equipped ship. http://www.navcen.uscg.gov/enav/ais/ (Accessed May 4, 2009)

[23] Raymond Gilpin, U.S. Institute for Peace, April 10, 2009. http://www.usip.org/on_the_issues/somalia_piracy.html (accessed May 4, 2009)

[24] Blog - a contraction of the word weblog. Weblog – a personal website on which an individual record opinions, links to other sites, etc. on a regular basis. Oxford English Dictionary 11th Ed. New media is broadly defined as those consumer level digital devices and the forms of instantaneous, interactive communication they make possible because of their integration with global communication networks. Center for Strategic Leadership, US Army War College and the SecDev Group, Bullets and Blogs New Media and the Warfighter. Carlisle, PA: Center for Strategic Leadership, 2009

[25] Center for International Media Assistance. Special Report. 4

[26] Ibid.

[27] http://www.internetworldstats.com/stats.htm (accessed March 3, 2009)

[28] Florence LeBorgne. IDATE, Communications & Strategies no 67, 3rd quarter 2007, 185

[29] http://www.facebook.com/press/info.php?statistics (accessed March 3, 2009)

[30] Conversation with Mr. Mark Clancy Citigroup, Inc. November 5, 2009.

[31] Alexander. 61

[32] Robert M. Gates, U.S. Secretary of Defense, Memorandum for the Secretaries of the Military Departments, et al. *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, June 23, 2009.

[33] Ibid.

[34] Sun Tzu, *The Art of War*. Translated by Samuel B. Griffith. New York: (Oxford University Press, 1971), 130

[35] Ibid. Tu Mu was a Chinese writer between A.D. 803-52.

[36] Qiao Liang and Wang Xiangsui. *Unrestricted Warfare*. (Beijing: PLA Literature and Arts Publishing House) February 1999. 188

[37] Ibid. 189

[38] Ibid.

[39] The New York Times. November 9, 1858.

[40] Ibid.

[41] http://www.historic-uk.com/HistoryUK/England-History/ssGreatBritain.htm (accessed February 3, 2009)

[42] Milan Vego, *Joint Operational Warfare Theory and Practice*, Newport, RI, Naval War College Press, 2007. I-3

[43] General James T. Conway, USMC, Admiral Gary Roughead, USN and Admiral Thad W. Allen, USCG *A Cooperative Strategy For Maritime Security*, Washington, D.C., October 2007, 4

[44] James N. Mattis and Frank Hoffman, "Future Warfare: The Rise of Hybrid Wars" *U.S. Naval Institute Proceedings* (Annapolis, MD: U.S. Naval Institute, Issue November 2005, Vol. 132/11/1,233

[45] Frank Hoffman, "Hybrid Warfare and Challenges." *Joint Force Quarterly*, (Washington D.C.: National Defense University Press), Issue 52, 35

[46] Frank Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, December 2007, 35

[47] Hoffman, "Hybrid Warfare and Challenges" 36

[48] Mohamad Bazzi, "Hizballah cracked the code," Newsday.com, September 18, 2006. http://www.newsday.com/news/printedition/stories/ny-wocode184896831sep18,0,2368668.story (Accessed February 11, 2009)

[49] Hilary Hilton. TIME. August 8, 2006. http://www.time.com/time/world/printout/0.8816.1224273.00.html (accessed February 12, 2009)

[50] Frank Hoffman, "Hybrid Warfare and Challenges." *Joint Force Quarterly*, (Washington D.C.: National Defense University Press, Issue 52, 35

[51] Mattis and Hoffman. "Future Warfare: The Rise of Hybrid Wars."

[52] Keith B. Alexander, "Warfighting in Cyberspace." *Joint Force Quarterly*, (Washington D.C.: National Defense University Press, Issue 46, 59

[53] Maura Conway. *Cybercortical Warfare: The Case for Hizbollah.org.* 11

[54] Ibid. 13

[55] Martin Libicki, *The Emerging Primacy of Information.* Orbis, 00304387, Spring 96, Vol. 40, Issue 2, 1.

[56] Clausewitz. 75

[57] Ibid.

[58] Ibid. 149
[59] Melissa Hathaway. October 8, 2008. McClatchy-Tribune News Service. Op-Ed.
[60] Voice over Internet Protocol (VoIP) is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers. Also, while some VoIP services only work over your computer or a special VoIP phone, other services allow you to use a traditional phone connected to a VoIP adapter. http://www.fcc.gov/voip/, (accessed February 27, 2009)
[61] Google Earth is a registered trademark of Google. Google Earth lets you fly anywhere on Earth to view satellite imagery, maps, terrain, 3D buildings, from galaxies in outer space to the canyons of the ocean. You can explore rich geographical content, save your toured places, and share with others. http://earth.google.com/#utm_campaign=en&utm_medium=ha&utm_source=en-ha-na-us-sk-eargen&utm_term=earth%20download (accessed November 9, 2009)
[62] http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html?_r=1 (accessed February 27, 2009)
[63] http://www.latimes.com/news/opinion/la-ed-cyberwar17-2008aug17,0,5922456.story (accessed March 9, 2009)
[64] Russian Invasion of Georgia. Report of Russian Cyberwar on Georgia 9 October 2008. Regular updates can be found on the Georgia Update website: www.georgiaupdate.gov.ge
[65] *Cyberwarfare: 2008 Russian Invasion of Georgia*. Presentation to InfowarCon 2009 by Mr. Jeffrey Carr, Principal of GreyLogic LLC and Principal Investigator for Grey Goose, Mr. Rafal Rohozinski, Principal Investigator, Information Warfare Monitor and the SecDev Group, Ms. Eneken Tikk, Head of Legal Team, NATO Cooperative Cyber Defence Centre of Excellence.
[66] Steve Coll and Susan B. Glasser, e-QAEDA - From Afghanistan to the Internet - Terrorists Turn to the Web as Base of Operations, Washington Post, August 7, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html (accessed August 11, 2009)
[67] The Combating Terrorism Center. *The Islamic Imagery Project, Visual Motifs in Jihadi Internet Propaganda*. (Department of Social Sciences, West Point, March 2006), 96
[68] http://www.usna.edu/Users/humss/bwheeler/swords/batar.html
[69] Philip Seib. *The Al-Qaeda Media Machine*. (Ft Leavenworth KS: Military Review May-June 2008), 76
[70] Peng Guangqian and Yao Youzhi, ed. *The Science of Military Strategy* (Beijing: People's Republic of China: Military Science Publishing House, 2005), 475-476
[71] Thomas. *Dragon Bytes Chinese Information War Theory and Practice*. 32
[72] http://www.infowar-monitor.net/modules.php?op=modload&name= News&file=article&sid= 1472&mode= thread&order=0&thold=0 (accessed February 19, 2009)
[73] Time Magazine. http://www.time.com/time/magazine/article/0,9171,1098961,00.html (accessed March 4, 2009)
[74] Ibid.
[75] Siobhan Gorman, *Electric Grid in U.S. Penetrated by Spies*, Wall Street Journal, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html (Accessed April 29, 2009)
[76] Ibid.
[77] FMSO conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. http://fmso.leavenworth.army.mil/ (accessed March 26, 2009)
[78] Timothy Thomas. *Dragon Bytes Chinese Information-War Theory and Practice*. Fort Leavenworth, KS, Foreign Military Studies Office, 2004. 18
[79] Sun Tzu. 84 and 79
[80] InfowarCon is a recurring conference of IO professionals sponsored by the Association of Old Crows. Mr. Rohozinski spoke on both Russian and Chinese cyber and information warfare activities.
[81] Thomas. *China's Electronic Long Range Reconnaissance*. 47
[82] The theory of cyber privateers was put forth by Mr. Rohozinski at InfowarCon 2009 and support by other cyber analysts at the conference.
[83] Vego. I-3
[84] Joint Publication 3-0, III-1
[85] Vego. VIII-3

[86] Dr. Vego identifies key operational functions as command organization, intelligence, command and control warfare, fires, logistics, and protection. Ibid.
[87] Ibid. VIII-4
[88] James J. Schneider. "*The Loose Marble- and the Origins of Operational Art"*, Parameters. (Carlisle, PA, Journal of the U.S. Army War College, Vol XIX, No. 1, March 1989. 87
[89] Ibid.
[90] Conversation with COL William Hartig, USMC (Ret'd) February 20, 2009
[91] E.B. Potter. Nimitz. (Annapolis, MD: Naval Institute Press, 1976), 136
[92] Geoffrey Till. *Seapower A Guide for the Twenty-First Century*. (Oxford, UK: Frank Cass, 2006), 162
[93] Geoffrey Bennett. *The Battle of Trafalgar*. (London: B.T. Batsford Ltd, 1977), 140
[94] Ibid. 138
[95] Julian S. Corbett, *The Campaign at Trafalgar* (London: Longmans, Green and Co, 1910), 342
[96] Vego. III-3
[97] Napoleon accomplished this by establishing (or achieving control of) six newspapers: the *Journal de général Bonaparte et des hommes vertueux*, the *Courrier de l'Armée d'Italie*, and *La France vue de l'Armée d'Italie*, in 1797, and the *Journal de Malte*, the *Courier de l'Égypte*, and *La Décade Égyptienne* in 1798. http://www.gutenberg-e.org/haw01/frames/fhaw03.html (Accessed 20 Nov 2008)
[98] Vego. VIII-3
[99] Dan Kuehl referencing a discussion with Lt Gen Alexander, USA at Cyber Education Workshop December 2, 2008.
[100] Sun Tzu, 130
[101] Clausewitz.76
[102] Robert M. Gates, U.S. Secretary of Defense. *Quadrennial Roles and Missions Review Report*. (Washington D.C., January 2009), 14
[103] Commentary on dust jacket of *7 Deadly Scenarios A Military Futurist Explores War in the 21st Century*. (New York, Bantam Dell 2009)
[104] Lev Navrozov, Chinese Geostrategy: 'Assassin's Mace' http://archive.newsmax.com/archives/articles/2005/10/20/172811.shtml (accessed September 17, 2009)
[105] Andrew F. Krepinevich. *7 Deadly Scenarios A Military Futurist Explores War in the 21st Century.* (New York, Bantam Dell 2009), 194.
[106] David Kilcullen. *The Accidental Guerrilla*. (Oxford, UK: Oxford University Press 2009), 5-6
[107] Clausewitz. 101
[108] Ibid. 140
[109] Ibid. 109
[110] Liang and Xiangsui. 199

Selected Bibliography

Bennett, Geoffrey. *The Battle of Trafalgar*. London: B.T. Batsford Ltd, 1977

Combating Terrorism Center, *The Islamic Imagery Project, Visual Motifs in Jihadi Internet Propaganda*. Department of Social Sciences, United States Military Academy. West Point, NY, 2006

Corbett, Julian S., The Campaign of Trafalgar. London, Longmans, Green and Co, 1910

Clausewitz, Carl von. *On War*. Princeton, NJ. Princeton University Press, 1976

Hoffman, Bruce. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, VA, 2007

Kilcullen, David, *The Accidental Guerrilla*. Oxford, UK: Oxford University Press, 2009

Kimmage and Ridolfo, *Iraqi Insurgent Media: The War of Ideas and Images* An RFE/RL Special Report. RFE/RL, Inc., Washington, DC, 2007

Kramer, Franklin D., Starr, Stuart H., Wentz, Larry K. Eds., *Cyberpower and National Security*. Washington, DC, Potomac Books, 2009

Krepinevich, Andrew F., *7 Deadly Scenarios*. New York, NY: Bantam Books, 2009

Potter, E.B., *Nimitz*. Annapolis, MD: Naval Institute Press, 1976

Qiao Liang and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999

Schwartau, Winn. *Information Warfare – Chaos on the Electronic Superhighway*. New York. Thunder's Mouth Press, 1994

_____. *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, 2nd edition.* New York, Thunder's Mouth Press, 1996

Thomas, Timothy. *Cyber Silhouettes – Shadows Over Information Operations*. Fort Leavenworth, KS, Foreign Military Studies Office, 2005

_____. *Dragon Bytes Chinese Information-War Theory and Practice*. Fort Leavenworth, KS, Foreign Military Studies Office, 2004

Till, Geoffrey. *Seapower A Guide for the Twenty-First Century*. London. Frank Cass, 2004

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1971

U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Operations*. Joint Publication (JP) 3-0, Washington, DC: CJCS, 17 September 2006, Change 1 13 February 2008

_____. *Information Operations*. Joint Publication (JP) 3-13, Washington, DC: CJCS, 13 February 2006

Vego , Milan. *Joint Operational Warfare*. Newport, RI. U.S. Naval War College, 20 September 2007