

REPORT DOCUMENTATION PAGE					<i>Form Approved</i> OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>						
1. REPORT DATE (DD-MM-YYYY) 05/11/2017		2. REPORT TYPE Master's Thesis			3. DATES COVERED (From - To) June 2016 - April 2017	
4. TITLE AND SUBTITLE Warfighting in the Information Age				5a. CONTRACT NUMBER N/A		
				5b. GRANT NUMBER N/A		
				5c. PROGRAM ELEMENT NUMBER N/A		
6. AUTHOR(S) Agnoli, Matthew J., Major, USMC				5d. PROJECT NUMBER N/A		
				5e. TASK NUMBER N/A		
				5f. WORK UNIT NUMBER N/A		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068					8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)					10. SPONSOR/MONITOR'S ACRONYM(S)	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT The Marine Corps is optimized for 20th century warfare. The mechanical and industrial ways of war define how the Service organizes, trains and equips for industrial age warfighting. The operating environment has changed in the 21st century. Today's operating environment is increasingly characterized by unprecedented access to information and the proliferation of information technologies. In what has been called the information age, the Marine Corps has yet to fully assess and understand the opportunities and vulnerabilities created by the new operating environment.						
15. SUBJECT TERMS IO; Information Age; Maneuver Warfare, Warfighting;						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College	
Unclass	Unclass	Unclass			19b. TELEPHONE NUMBER (Include area code) (703) 784-3330 (Admin Officer)	

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: Warfighting in the Information Age

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Major Matthew J. Agnoli (USMC)

AY 16-17

Mentor and Oral Defense Committee Member: _____

Approved: _____

Date: _____

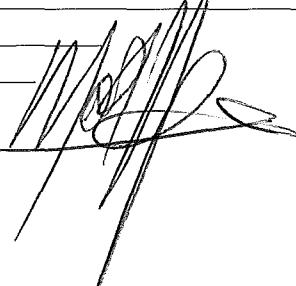
J.W. Gordon

Oral Defense Committee Member: _____

Approved: _____

Date: _____

M. Farn



5/5/17

Executive Summary

Title: Warfighting in the Information Age

Author: Major Matthew J Agnoli, United States Marine Corps

Thesis: In order to win the battles of the 21st century, the Marine Corps must adopt the means and methods of war that enable warfighting in an operating environment increasingly influenced by information.

Discussion: The Marine Corps is optimized for 20th century warfare. The mechanical and industrial ways of war define how the Service organizes, trains and equips for industrial age warfighting. The operating environment has changed in the 21st century. Today's operating environment is increasingly characterized by unprecedented access to information and the proliferation of information technologies. In what has been called the information age, the Marine Corps has yet to fully assess and understand the opportunities and vulnerabilities created by the new operating environment.

Despite these changes, the Marine Corps continues to employ its forces to dominate the physical environment. Emphasizing spatial maneuver and fires to generate overwhelming combat power, the Marine Corps has not always achieved the desired results with this approach to operations. Inversely, adversaries and competitors such as the Islamic State, the Peoples Republic of China (PRC), and Russia have studied US methods and employed strategies and capabilities that maximize the advantages provided in by the information environment. The Marine Corps inaction has effectively ceded this element of the operating environment to them.

Conclusion: The time has come to organize, train, and equip the Marine Corps for warfighting in the information age. An examination of our adversary's actions reveals that they have adapted strategies that avoid US military strengths and exploit our weaknesses in the information environment. Configured for the battles of the industrial age, the Marine Corps has been slow, even resistant, to the changes necessary to operate in the current operating environment. The Marine Corps has yet to adapt the means and methods of war that enable maneuver warfare in an environment of prolific information and information technology.

Rooted in the nature and theory of war, MCDP-1 *Warfighting* provides the intellectually framework for enabling maneuver in all dimensions, we need only to apply it. By denying adversary abilities to collect critical information, deceiving adversary decision makers, and influencing select target audiences for military advantage, the Service can directly affect the mental and psychological aspects of our adversaries through the capabilities of the information age. Fielding technical Information Operations (IO) specialists and officers, combined with IO planners to integrate these capabilities as inherent to operations, will facilitate maneuver warfare in all dimensions and combined arms in all domains as envisioned in the MOC.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Figures

	Page
Figure 1. Current USMC Application of Maneuver Warfare Doctrine	1
Figure 2. Current Adversary Application of Maneuver Warfare Doctrine.....	2
Figure 3. Ideal Application of Maneuver Warfare in the Information Age	3

Table of Contents

	Page
Executive Summary	ii
Disclaimer	iii
List of Figures	iv
Preface.....	vi
Introduction.....	1
The US Armed Forces: Optimized for Warfighting in the Industrial Age	3
The Information Age: New Opportunities and Vulnerability	4
The Information Age: Current Implications	7
The 21st Century Threat: Information Warfare	7
China: The Three Warfares.....	7
Russia: Reflexive Control	9
The Islamic State in Iraq and the Levant (ISIL)	10
Warfighting in the Information Age	12
Looking for Solutions: MCDP-1 Warfighting Revisited.....	12
Still Timeless: The Nature of War in the Information Age	13
Friction, Uncertainty, and Disorder in the Information Age	13
Revisited: The Human Dimension of War in the Information Age.....	14
Organizing for Information Age Maneuver Warfare.....	18
Information Operations: Realizing the Potential	19
Operations Security	20
Military Deception	22
Technical Information Operations	24
Implementing the Institutional Change to support Information Age Warfighting	27
Conclusion	30
Endnotes.....	32
Bibliography	33

Preface

In the information age, the character of war is rapidly changing. Prolific access to information and information technology is transforming how human beings interact, including during war. The Marine Corps must adapt to this changing operating environment and field capabilities that enable maneuver warfare in other dimensions beyond the spatial, especially the psychological dimension. Rooted in the nature of war, MCDP-1 *Warfighting* provides the intellectual framework for maneuver in all dimensions, we need only to apply it. Absent broad institutional change, our adversaries will thrive in the aspects of the environment effectively ceded to them by our inaction. This cannot continue to happen. The time has come for the Marine Corps to seize the opportunities provided by the ascendance of information and information technology and protect our many vulnerabilities. In doing so, the Marine Corps will realize the potential of maneuver warfare in the 21st century and remain ready to fight and win the battles of the information age.

I would like to acknowledge and thank the Marines and civilians of the Marine Corps Information Operations Center whose ideas provided the intellectual foundation for this paper. Your contributions to enhancing the Marine Corps understanding of maneuver warfare and combined arms is a true inspiration. I am a better warfighter because of your efforts to expand the Marine Corps understanding of the information environment and its effect on warfighting.

“Like war itself, our approach to warfighting must evolve. If we cease to refine, expand, and improve our profession, we risk becoming outdated, stagnant, and defeated.” – General Alford Grey FMFM-1

Introduction

Across human civilization, unprecedented access to information and information technology have accelerated the cycles of social and political transformation. Indeed, the late twentieth century up through the present is now commonly referred to as the “Information Age.”¹ As information technology proliferates, socio-economic norms have been challenged creating a ‘new normal’ of information flow on a global scale.² Inevitably, great change brings both progress and turmoil. The global security landscape is now heavily influenced by the rapidly evolving information environment, the information component of the operating environment, which has created ever complex dilemmas for defense and military professionals. Within the United States (US), lumbering government bureaucracies have been slow to adapt and appreciate the implications of the information age. The American way of war, whose traditions are rooted in its military successes of World War II, have been characterized by mechanical, industrial, and technological superiority. US forces today are organized for high-end, conventional conflict and the domination of the physical domains of the operating environment such as land, air, sea and space. Heavy emphasis is placed on physical battlespace and the use of overwhelming combat power to overmatch opponents. Killing enemy personnel and destroying military equipment and facilities for a political purpose is the order of the day for US forces.

Despite an ever-changing operating environment, the US Marine Corps (along with the rest of all US armed forces) has changed very little and remains optimized for twentieth century warfighting. Today’s Marine Corps organizes, trains, and equips for industrial age warfare and

is managed by rigid and cumbersome bureaucratic institutions. Operating in an ever changing and rapidly adaptive environment, Marine units have become increasingly vulnerable and have yet to fully exploit the opportunities created by the information age. Inversely, adversaries and competitors such as the Islamic State, the Peoples Republic of China (PRC), and Russia have studied US methods and employed strategies and capabilities that maximize the advantages provided in by the information environment. In order to win the battles of the 21st century, the Marine Corps must adopt the means and methods of war that enable warfighting in an operating environment increasingly influenced by information. For decades, the Marine Corps has employed its forces to dominate the physical environment by using maneuver and fires to generate overwhelming combat power and a combined arms advantage over its adversaries. While the combination of spatial maneuver and integrated fires can create operational advantages, new opportunities have been created in the information age that have thus far been unexploited by the Marine Corps. Today, combat power can be generated through information and must be integrated to fully achieve 21st century combined arms. The nature of war in the information age remains as it always has been but its character, including the means and methods of war, have evolved and the Marine Corps must evolve with it. The recently released Marine Corps Operating Concept (MOC) and Ellis Group essays on 21st Century Maneuver Warfare published in the Marine Corps Gazette acknowledge this but only begin the discussion for institutional change. The paper that follows will examine the implications of the information age on military operations, provide an analysis of current and emerging threats, assess current Marine Corps doctrine in relation to the information age, and provide recommendations on how the Marine Corps should organize, train, and equip for warfighting in the 21st century.

The US Armed Forces: Optimized for Warfighting in the Industrial Age

In the 20th century, the United States was the beneficiary of its superior industrial and manufacturing capacity. During World War II, war material production was made possible through a mobilized population and a strong industrial base that produced an “arsenal of freedom.” Untouched by the destruction and carnage of the European and Pacific theaters, the industrial capacity of US factories was able to produce the weapons of war on a massive scale without disruption. While US equipment was outmatched early in the war, production capacity and material improvements were continuous. With the development and usage of the atomic bomb and the end of World War II, American military production was perceived to have been a decisive contributor to the overall victory of the Allies. In the Cold War era that would follow, the mechanical and industrial capacity of the nations of the West would create a decisive advantage for NATO in contrast to the state controlled economies of the Soviet Union and nations of the Warsaw Pact. While the Cold War militaries of the West never engaged in direct combat with the Soviet Union and its armies, these forces would be unveiled during the 1991 Gulf War against Iraq. Saddam Hussain employed the world’s fourth largest army and his military forces would be defeated in just one hundred hours following a prolonged air campaign. During the Gulf War, the technologically superior militaries of the West were on full display, further reinforcing the perception that the technological advances brought by the industrial age processes would deliver decisive results for all future conflicts. Notably, many in the military establishment believed that US technological innovations, particularly in information technology, would remove uncertainty and ambiguity from the conduct of future war.³

During this period, the United States Marine Corps would organize, train, and equip to maximize the use of US industrial and technological strength. Using speed, mobility, and combined arms, the Marine Corps would generate overwhelming combat power through the superior use of maneuver and fires. The Marine Division would provide the nucleus of the Marine Expeditionary Force (MEF), the Marine Corps principle warfighting unit. The Division, possessing the organic combat power of three infantry regiments, an artillery regiment, and a combination of reconnaissance and armor assets would prove to be a formidable conventional force. The configuration of the Marine Division could be seen as a full realization of the industrial era, a conventional combined-arms force capable of generating unrivaled combat power when compared to units of similar size. Its configuration has remained relatively unchanged for decades up to the first quarter of the twenty-first century.

Observing closely the results of the Cold War and especially the 1991 Gulf War, adversaries and competitors began to take notice of US military superiority with increasing alarm. The Gulf war especially was a catalyst for anyone who wished to oppose the United States, to begin to develop a new military option.⁴ Nations such as China, came to see the relative industrial and technological superiority of US forces as a direct threat to their interests. China, and nations that shared this concern, began to look to develop ways to counter US technological supremacy. Corresponding with this period, the creation of the internet, the mass production of the personal computer, and the reduced cost of cellular communication were all providing the means for new opportunity to counter directly (or indirectly) US political and military advantages.

The Information Age: New Opportunities and Vulnerability

Today, access to information and associated technologies is influencing perception and how people relate to one another. Just two short decades ago, people across the globe received news by reading a newspaper or magazine, listening to a radio, or watching a news broadcast on their television. We now have 24/7 access to global information feeds via cellular, satellite, and Wi-Fi signals⁵. Where once the US military was an exclusive beneficiary of information technology for Command and Control (C2), long range communications, and intelligence collection (to name a few), adversaries, competitors, and neutrals alike now have access to a wide range of information technologies. Once dominant in the information technology arena, the US has grown accustomed to the use of this technology and created a dependence on networked systems, large military databases, global positioning systems, and satellite based communications.

This dependence, once a great advantage, now has created increased vulnerability. As costs of information technology continue to drop, more and more state and non-state actors have gained access to low cost information systems. It is through this access that our adversaries can coordinate actions via internet connected devices (faster than most current US C2 systems), collect imagery intelligence on US forces and installations from public access software such as Google Earth, or counter US media and narratives with focused influence operations via social media platforms such as Twitter and Facebook. Adversaries are now investing in low cost capabilities such as GPS jammers and computer hacking, to exploit US dependency on unclassified internet based systems and GPS satellites. Once a great advantage, reliance on technology has made the US military vulnerable and worse yet, complacent.

Along with the rest of the joint force, the Marine Corps has become increasingly reliant on these systems. In order to realize the combined arms potential of the Marine Air Ground Task Force (MAGTF), long range communications are required over great distances. In many cases, the MAGTF's maneuver and fire support elements now outrange their C2 and communications capabilities. Further, the networks to coordinate maneuver and fires increasingly represent a 'single point of failure' that if exploited, could greatly reduce the ability of the MAGTF to utilize its greatest strength: overwhelming combat power via combined arms.

Marine Corps operations in both Iraq and Afghanistan have reinforced the dependence on these technologies. One example is the Marine Corps reliance on GPS. In order to prevent fratricide and minimize collateral damage during counter insurgency operations (COIN), Marines increasingly use GPS enhanced systems. While beneficial in accomplishing the COIN missions, an unintended effect was the false assumption by Marines that GPS would always be available and accurate across the range of military operations (ROMO). Absent an enemy that could employ GPS jamming technology, the Marine Corps has installed GPS systems on everything from aircraft navigation, artillery howitzer fire control systems, and logistics tracking systems. This dependence on GPS provides a lucrative, high-payoff target for adversaries should they choose to exploit it.

Information age technology has also made larger amounts of information available and reduced the need for physical storage of records. As information has moved to digital storage means, bureaucratic processes have become streamlined. Massive amounts of data can be created, stored, and transmitted rapidly creating greater efficiency. The US Office of Personnel Management (OPM) is one such bureaucracy that has benefitted from information age technology. Responsible for processing security clearances for Federal workers, OPM is a single

stop repository for massive amounts of personnel data on all manner of US government employees. OPM maintains information on all federal workers requiring a security clearance. Each employee who applies for a clearance, must complete Standard Forms (SF) 86, Questionnaire for National Security Positions. SF-86 forms contain detailed information including, but not limited to, social security numbers, family members, close associations, foreign contacts, business transactions, and psychological information. While digital technology made the processing, handling, and storage of SF 86 easier, it also provided the opportunity for foreign intelligence services. In June 2015, OPM reported that it had been the target of a data breach targeting its database. It is believed the PRC breached OPM's system and obtained the SF-86s for millions of federal employees. This is considered the worst data breaches in US history and gives China an incredibly valuable intelligence database on all US federal workers from military service members, intelligence professionals, to nuclear engineers working the Department of Energy.

The Information Age: Current Implications

Proliferation of information and information technologies greatly reduce the advantages once enjoyed by technologically superior US forces. Dependency on these technological systems has further resulted in ever increasing vulnerability for the armed forces. This problem is magnified by reliance on technology and an industrial age bureaucracy that slows the Marine Corps ability to adapt to a rapidly changing environment. Meanwhile, adversaries have demonstrated a growing proficiency in utilizing the opportunities created by the information age for military advantage. In order to develop an understanding of the challenges facing the Marine Corps in the current operating environment, the following provides further study of three current adversaries in the use of information in warfighting.

21st Century Threats: China & The Three Warfares

For decades, the US and the Peoples Republic of China (PRC) have been engaged in a geopolitical contest for supremacy in the Asia-Pacific region and around the world. China understands that armed conflict with the US is not in their interest and that open hostilities could have disastrous consequences. Alternatively, China has chosen to avoid US military strength and has looked into its ancient history for a strategy in the tradition of Chinese general Sun Tzu. Today, the PRC seeks to "win without fighting" in the Pacific by avoiding US military strength and using indirect means to displace US influence in Asia.

To achieve this, China has embraced the opportunities of the information age and employed unorthodox operations to influence and deceive regional nations, international organizations, and US policymakers for their advantage. Within the last decade, Chinese military officers have written that contemporary war uses trade, ecological, cyberspace or a host of other forms of warfare.⁶ In their words, warfare uses “all available means to include the use of force, non-armed force, military and non-military, and lethal and non-lethal capabilities to compel an enemy to accept their interest.”⁷ The Chinese currently employ the doctrine of “The Three Warfares” which combines psychological, media, and legal warfare to advance political aims.⁸ This indirect approach, combined with the modernization of its military, demonstrates a contemporary example of information age maneuver warfare. China purposefully avoids US military strength by investing in resources to achieve parity/superiority or adapts means to negate US conventional military supremacy.⁹

Marines stationed in the Pacific today are insufficiently trained and equipped to deal with Chinas indirect strategy. Once again, institutional bias focuses on Chinas material military strength such as the deployment of their first aircraft carrier or the fielding of anti-access/area

denial (A2AD) weapons. This focus misses the full scope of the PRCs efforts in the region. The Marine Corps has yet to fully adapt means and methods of war that counter Chinese efforts to reduce US influence in the region without the overt use of force.

Russia: Reflexive Control

Russia is another nation that uses information warfare to achieve their national aims. From interference in western elections to the annexation of the Crimea in Ukraine, Russia employs a combination of conventional, asymmetric, deception, and psychological operations to achieve their national aims. Like China, they have studied the patterns established by US politicians, diplomats, and military officials to devise strategies that exploit weaknesses and avoid strengths. Russia is currently heavily invested in a strategy of disinformation meant to undermine western influence, degrade confidence in western institutions, and confuse adversaries as to their true intentions. In order to fully understand and combat the effects of Russian actions, we must understand the concept of what is known as reflexive control and how it fits into the greater Russian strategy.

Reflexive control is a unique Russian concept based on what the West calls *maskirovka*, or “concealment.”¹⁰ This is an old Soviet notion in which one “conveys to an opponent specifically prepared information to incline him/her to voluntarily make the predetermined decision desired by the initiator of the action.”¹¹ Reflexive control is conducted as a sustained campaign that provides a target audience with select information so that the target is inclined to make decisions and act in a desired way. Reflexive control “clogs, corrupt, and corrodes” the information going into a system in order to manipulate a target audience.¹² The method to do this is to identify a weak link in a system and exploit it through moral arguments, psychological tactics, or appeals to specific decision makers character.¹³

Today, reflexive control represents a key component of Russia's hybrid warfare strategy. Reflexive control is taught at Russian military schools and training programs, and is integral to Russian national security strategy informed by the Gerasimov Doctrine.¹⁴ A recent example of how Russia has employed reflexive control in practice is their actions in Ukraine in 2014. During this campaign, Russia used deception and misinformation to conceal the presence of their forces. Russian forces infiltrated into Ukraine by deploying military personnel without uniforms or identifiable insignia. They also mislead international media and observers through the purposefully concealed their goals and intentions by publicly denying Russian participation. Simultaneously, Russia warned the North Atlantic Treaty Organization (NATO) through overflights of naval vessels and even threatened the use of nuclear weapons if the West interfered. Through an active 'denial and deception' operation, Russia combined these actions in a way that is consistent with the concept of reflexive control.

Once again, Marine units operating throughout Europe and the Middle East are not fully prepared to face Russian forces employing these strategies. To compete in the "information war" and combat Russian influence, the Marine Corps must invest in methods to protect critical information, detect and unmask deception efforts, protect decision making, and discredit disinformation programs designed to weaken US military efforts. Russia has now demonstrated the effectiveness of reflexive control in the Ukraine. The Marine Corps must orient on our adversary and implement measures to protect our vulnerability and maneuver in dimensions beyond the spatial in order to achieve an operational advantage in Eastern Europe.

The Islamic State in Iraq and the Levant (ISIL)

ISIL, or the Islamic State in Iraq and the Levant, grew from the remnants of Al Qaeda in Iraq. This movement, once dismissed by Western policy makers, has grown to become a global

insurgency which has recruited tens of thousands of fighters to their cause. The inflow of jihadists from around the world, has been unprecedented in its pace and volume, and has continued to this day. Led by Abu Bakr al-Baghdadi, once a guerrilla fighter during the US led occupation of Iraq, he has named himself the first caliph in generations who would command all Muslims. In the pursuit of establishing a caliphate, ISIL now controls parts of Iraq and Syria whose territory includes a population estimated at between six and seven million people.

Exploiting information age means to their advantage, ISIL is especially skilled in the use of global social media networks to indoctrinate and recruit.¹⁵ Using well produced videos and other media, ISIL has been able to inspire and radicalize Muslims around the world. Carefully crafted narratives and messages are specifically designed to influence there intended target audience, dissatisfied young Muslims. These videos and messages have had global effects. Around the world, ISIL or individuals inspired by them, have conducted 143 attacks in 29 different countries.¹⁶ These attacks further support ISIL narratives regarding their global moral struggle against their enemies.

Predictably, the response of the US has been conventional military force. Under Operation INHERENT RESOLVE (OIR), coalition airstrikes have been aggressively targeted ISIL forces throughout Iraq and Syria. While these strikes are effective in the short-term, they do very little to defeat the moral struggle being waged by ISIL. In order to ultimately defeat them in the long term, the US must attack the ideas of ISIL as the main effort supported by other military means such as fires and maneuver. The ideology of ISIL cannot be defeated with superior firepower alone. Marines deployed in support of OIR must learn to integrate and employ information and psychological operations in order to delegitimize ISIL claims and their

leadership. Marines must be trained and equipped to target the real center of gravity of the ISIL: Abu Bakr al Baghdadi's claim that he and his followers are the only authentic Muslims.¹⁷

Looking for Solutions: MCDP-1 *Warfighting* Revisited

Adversary actions demonstrate that material and technological solutions will be insufficient to counter their current approach to warfighting. Assertions that wars underlying nature has been changed due to technology have continually been disproven. A study of past Military Revelations from the French and Industrial Revolution to the Nuclear Age show that technology alone cannot change now, or in the future, war's underlying nature.¹⁸ The nature of war remains constant and stubbornly persistent in the current era of proliferated information and information technologies. Despite this fact, it would be unwise for military planners to ignore the implications of the information age on the character of war. While the nature of war remains constant, the means and methods of war evolve constantly. It is the rapid impact of war's changing character in the information age that Marines must study and understand. Fortunately for Marines, a guidebook already exists that will help Marines understanding the implications of information on military operations. Marine Corps Doctrinal Publication (MCDP) 1, *Warfighting* is the capstone doctrinal reference for the Service. This publication is a guidebook for the Marine Corps' warfighting philosophy of maneuver warfare. Within its pages, *Warfighting* synthesizes the ideas of military theorists such as Carl Von Clausewitz, Sun Tzu, and John Boyd. The following is an examination of key elements of *Warfighting* and how they can be applied to understand the impacts of the information age on warfighting.

Still Timeless: The Nature of War in the Information Age

Chapter One of *Warfighting*, the Nature of War, defines wars essence as "a violent struggle between two hostile, independent, and irreconcilable wills, each trying to impose itself

on the other”.¹⁹ It further states that war is essentially an “interactive social process”.²⁰ So, the warfighter must appreciate the social and human dynamics that characterize the clash of human wills. Today, means and methods exist that can influence or effect an individual or groups will. In the information age, the proliferation of information and information technologies has changed the way individuals see themselves and the world around them. With the click of a link on a smartphone, individuals can confirm or deny assumptions about their circumstances. Likewise, individuals or groups can inspire others to action via social media posts. Access to information increasingly opens an individual to the world around them when once they were isolated by physical circumstances or geography. Information increasingly can bolster or diminish an individual or group’s will if manipulated for a military purpose. The Marine Corps must develop the means and methods to exploit the opportunities of information if we are to defeat the will of our adversaries in this new information environment.

Friction, Uncertainty, and Disorder in the Information Age

Warfighting also describes other characteristics of war’s inherent nature such as friction, uncertainty, and disorder. In the information age, many have drawn the wrong conclusions about information technologies ability to reduce these characteristics.²¹ Use of sophisticated command and control systems, incorporation of advanced intelligence collection capabilities, and ever more capable communications technologies have given many commanders a false sense of what they know about the operating environment. It is thought that increased levels of certainty and understanding are now possible through the use of technology. This assumption is not only incorrect, it can also be dangerous and leave a commander vulnerable to coercion and deception. Information technology does not reduce uncertainty and friction it often increases them.²² Commanders with access to advanced information technology are often overwhelmed by the raw

data that these technologies create. Often, commanders and analysts have more information than they know what to do with and this can overwhelm command and control processes and slow the ability to generate greater operational tempo. This abundance of information can also be purposefully manipulated for military advantage. A cunning opponent could protect his critical information and present false data for the purpose to mislead and gain a position of advantage. The increased opportunity to create technologically based ambiguity, through planned deception, must be considered carefully in modern warfare. In summary, friction, complexity, and uncertainty are increased in the information age, not decreased.

Revisited: The Human Dimension of War in the Information Age

Warfighting highlights what it calls the human dimension of war. Since war is ultimately a violent clash between two irreconcilable wills, the human element of conflict will always play a central role in a war's outcome. Regardless of the information environment or the proliferation of information technologies, human nature and its intangible mental and moral components will always play a critical role in warfare. However, understanding how information and new technology influences an individual or group's perceptions, motives, decisions, and ultimate actions can be very useful in the current operating environment. Today, access to information motivates groups to rise up against governments across the middle east. The Arab Spring is one example of a political movement fueled by access to information. All at once, oppressed peoples were able to voice their grievances with like-minded people due to access to social media and other news sources via mobile devices. Now able to find individuals who shared their views, opposition groups were able to organize at the speed of the internet in near real time. The passion of human beings that is central to war, now has a means to mobilize groups far more quickly. While no single technological development will diminish the human dimension, they

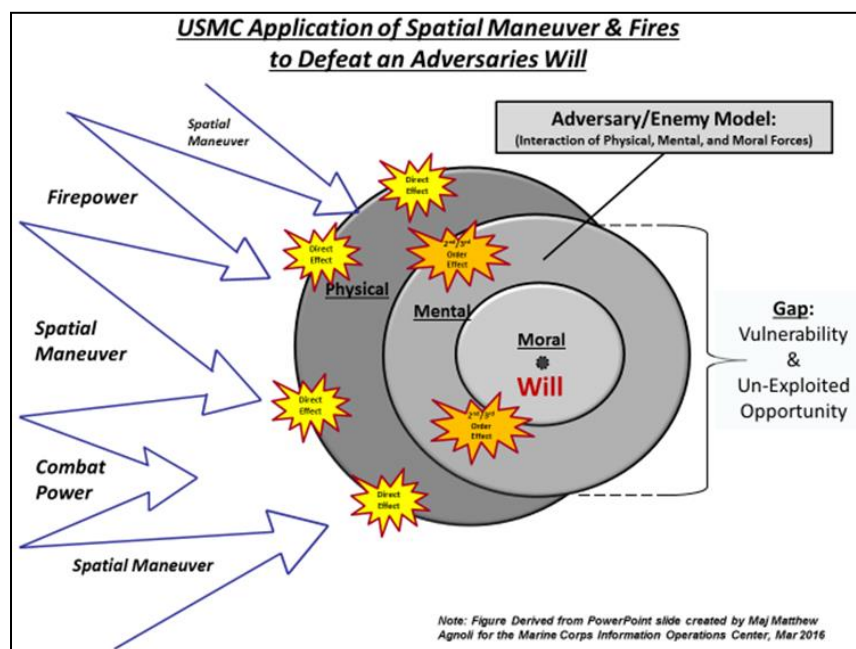
will provide new opportunities and outlets for individuals and groups to impose their will on one another.

Warfighting additionally provides an incredibly useful modal for understanding the human dimension. It states that “war can be characterized by the interaction between physical, mental, and moral forces.”²³ Today, Marines generally focus on physical characteristics of an adversary or system. Physical characteristics are easy to see and measure. Planning tools such as relative combat power analysis (RCPA) are commonly used by Marine planners to measure the physical strength of a Marine unit in relation to an adversary formation. These tools are often used to determine our own course of action (COA) leading up to execution of an operation. But what about mental and moral characteristics? *Warfighting* provides an ominous warning to those who would take an easy path and focus on only the physical characteristics of war. It states that “while material factors are easily quantifiable, the moral and mental forces exert the greater influence on the nature and outcome of war.”²⁴

Marines today overemphasize the physical dimension of war during planning and execution in spite of *Warfighting's* warning not to do so. In applying the doctrine of maneuver warfare in this regard, Marines plan for only spatial maneuver to gain a physical, positional advantage over an adversary. Direct effects on the physical characteristics of an adversary, or adversary system, thus have second and third order effects on the mental and moral dimension. The effects of overwhelming fire power and combined arms can have mental and psychological effects that can shatter unit cohesion and lead to the defeat of an adversary's will. While this method can achieve desired results, today's Western political sensibilities tolerate the terrible human cost of warfare far less than they once did in the 20th century. While very much the American way of war, using overwhelming firepower to kill enemy personnel and destroy

military equipment and property can prove to be counterproductive in achieving political objectives. Information age methods can allow the global media to see the results of highly lethal and destructive weapons in real time. Adversaries can exploit this by producing false or deceptive narratives of US operations killing innocent civilians. This can undermine the moral strength of the US policy makers and the armed forces by eroding the belief that the military mission is a justified use of force. New opportunities have also been created in the information age that have thus far gone unexploited by the Marine Corps. Figure 1 provides a visualization depicting the current Marine Corps application of maneuver warfare and the impact on the physical, mental, and moral characteristics of an adversary or human system.

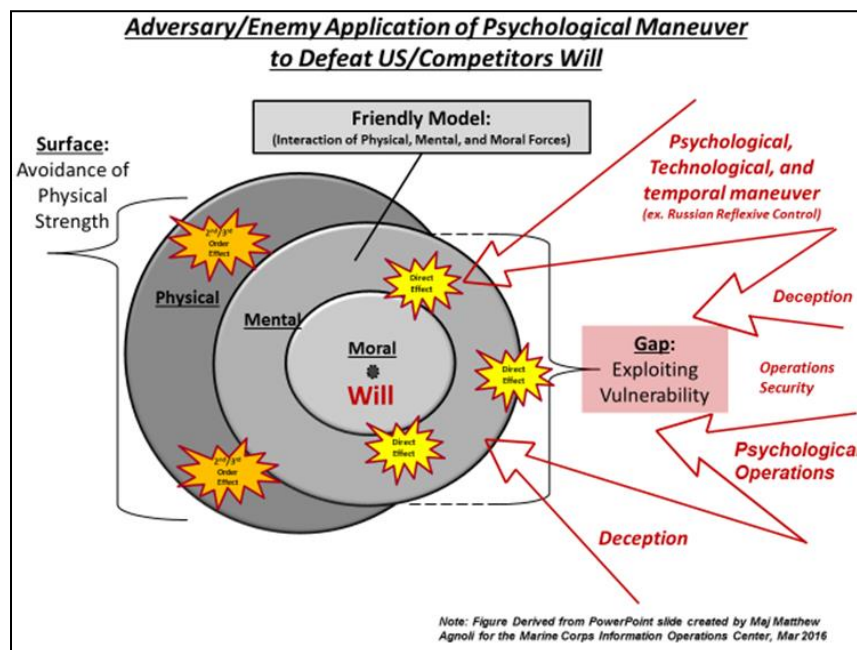
Figure 1. Current USMC Application of Maneuver Warfare Doctrine.



In contrast, adversaries and enemies have studied US military operations and are actively exploiting US vulnerabilities created in the information age. Adversaries know well that direct confrontation with the armed forces of the US would come with a tremendous cost. Rather than attack into our strength, they avoid this surface and attack the mental and moral sources of US

power. Using combinations of deception and psychological operations, our adversaries seek to undermine US credibility, create ambiguity and confusion, and mask their true intentions. These adversaries effectively maneuver via the psychological, temporal, and technological dimensions to gain advantages over US political and military efforts. Using a form of 21st century combined arms, they use the means and methods provided in the information age to bypass US strength and achieve their political and military aims. This often happens without overt military action and mostly without our complete understanding of adversary and enemy objectives. Figure 2 provides a graphical depiction of our adversaries application of maneuver warfare.

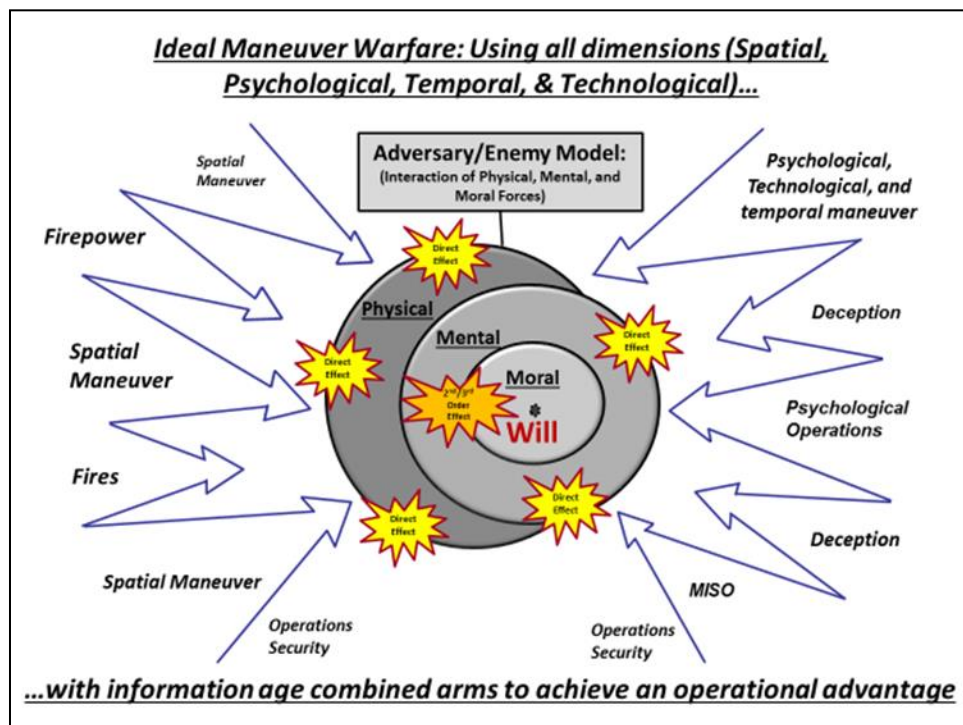
Figure 2. Adversary Application of Maneuver Warfare.



Today, it is imperative for Marines to revisit *Warfighting* and apply the complete doctrine of maneuver warfare within the context of the information age operating environment. Marines limit the potential of maneuver warfare when they apply only the spatial and positional advantages of the doctrine. Using maneuver warfare across all dimensions (spatial, temporal, psychological, and technological) with the means and methods created in the information age

would have a devastating effect on an adversary or enemy system. Figure 3 below provides a visualization of how maneuver can be conducted through all dimensions to achieve direct effects against the physical and mental components of an adversary system. Through combined arms in all domains (land, air, sea, space, and cyber), these attacks would more efficiently erode adversary's strength and ultimately, their will to resist and fight.

Figure 3. Ideal Application of Maneuver Warfare in the Information Age.



Now, with a conceptual understanding of how the Marine Corps can conduct maneuver warfare and warfighting in the information age, we must examine the means and methods required to achieve this concept.

Organizing for Information Age Maneuver Warfare

Throughout the late 1990s up to the present day, the Marine Corps has haphazardly incorporated new information age technology and associated tactics, techniques, and procedures (TTPs) into MAGTF operations. In what became known as Information Operations (IO), the

Marine Corps sought to “integrate, coordinate, and synchronize all actions taken in the information environment to affect a decision maker in order to create an operational advantage.”²⁵ Despite decades of effort, IO today is mostly an afterthought of Marine Corps planning and execution. Ironically, as the information age continues to disrupt social, political, and military norms across the globe, the need for IO has only increased. Within the Marine Corps, the previously discussed cultural resistance to non-physical forms of warfighting and maneuver have helped prevent the full implantation of IO. Within the Marine Corps, IO remains under resourced with incomplete training and education across the Service. Also, trained IO subject matter experts continue to be rare across the Service. When Marines are trained, there is a limited understanding of how they can be employed to support MAGTF operations. Organizing the Marine Corps to achieve the MOC’s vision of “maneuver within all dimensions and across all domains”²⁶ will require broad training in IO and the associated capabilities.

Information Operations: Realizing the Potential

In a Marine Corps organized for warfighting in the Information age, IO will take on greater importance. IO today is an inherent part of Marine Corps operations even though the Service generally fails to recognize it is conducting IO. Realizing the full potential of IO will necessitate a Marine Corps that is capable of integrating the effects of Information Related Capabilities (IRCs) within a MAGTF concept of operations. As the information environment takes on greater importance in the information age, the ability to create effects within it will be of paramount importance. IO will also provide a means for the MAGTF to maneuver psychologically in order to gain cognitive advantages over an adversary. With IO, the MAGTF will be able to fully realize the promise of a combined arms force for the information age.

Trained IO planners will be required within the G/S-3s of all MAGTF CE echelons as well as within each MAGTF major subordinate element (MSE).

Developing IO as the integrating function of IRCs is only the beginning for the Marine Corps. The Service must also focus on the further development of capabilities that enable maneuver within the information environment. In the information age, IO will need to integrate capabilities that will deny enemy collections efforts, deceive decision makers, and influence target audiences and adversaries. In order to do this, the Marine Corps will need to create technical fields and subject matter experts (SMEs) in areas that they traditionally have not. Ever changing information technology and the growing importance of the cyber domain and electromagnetic spectrum necessitate technical expertise. The following will provide recommendations for the development of four specific areas as a means to fight and win the battles of the information age: Operations Security (OPSEC), military deception (MILDEC), Military Information Support Operations (MISO) and technical IO SMEs.

Operations Security

In the current operating environment where information can be shared globally at the speed of the internet, it will be essential for military units to protect critical information that is vulnerable to adversary collects efforts. For the Marine Corps, critical information is information that if known by an adversary, could cause a mission to fail. Knowledge of the disposition and strength of Marine units or the location and readiness of mission critical capabilities are examples of critical information that Marines may need to protect in support of operations. In military lexicon, the protection of critical information through deliberate planning and the implementation of measures is known as OPSEC. Traditionally, OPSEC is commonly associated with posters in Marines workspace that inform the reader “loose lips sink ships” or

other catchy slogans. Currently, just like IO in general, OPSEC is an afterthought of the military and rarely incorporated into planning and execution.

Slowly, Marine Corps leadership is starting to view OPSEC as a needed discipline within the Service. In the MOC, the Commandant discusses “a battle of signatures” where if a unit can be detected, it can be targeted and destroyed.²⁷ Including these ideas in the MOC is a step in the right direction but does not go far enough. Joint OPSEC training is currently provided by the Joint Forces Staff College in Norfolk Virginia and the curriculum details the 5-step OPSEC planning process, OPSEC indicators, and the role/responsibilities of the OPSEC officer. No such training exists for the Marine Corps. In order to professionalize OPSEC, the Marine Corps must establish a formal training course to create a pool of professional OPSEC planners. OPSEC plans and the implementation of OPSEC measures should be evaluated in training exercises at all levels as the environment and mission requires.

The Marine Corps should also ensure OPSEC plans and programs are fully established within HQMC and the supporting establishment, not just OPFOR units. The global reach of cyber based foreign collections efforts, such as the OPM hack, demonstrate the vulnerability of digital repositories of large amounts of personnel and sensitive information regarding Marines and their families. Basic OPSEC measures could have prevented the OPM disaster had they been planned for and implemented.

Lastly, the Marine Corps has been setting operational patterns during the last 15 years of war that our adversaries now understand all too well. These operational patterns provide indicators to foreign intelligence analysts that if identified, could give an adversary early warning that an operation is in planning or execution. Per OPSEC doctrine, there are five OPSEC indicators that should be considered including: Association, Profile, Signature, Contrast, and

Exposure. Curiously, the MOC discusses signature but neglects the remaining four indicators. While detecting, masking, or projecting signatures (electromagnetic, visual, audible, etc.) is a critical capability on the modern battlefield, understanding the others will be equally important in the combat operations to come.

Military Deception

Deception is not new in warfare. The ancient Chinese military theorist Sun Tzu stated “All warfare is based on deception” in his seminal writing, *The Art of War* circa 400BC.²⁸ The US military has long used deception in support of operations for its many advantages. Deceptive actions such as faints, ruses, demonstrations, and displays are fully embedded within military doctrine, mission planning, and tactical executions. Today, the opportunities to deliberately mislead have increased exponentially compared to the days of Sun Tzu. Information access and flow provide many conduits to decision makers that can be manipulated to elicit a desired action or inaction for military purposes. The Marine Corps must understand and exploit this opportunity to corrupt, disrupt, or mislead a target audience for a specified military objective and develop the means and methods to do so. Additionally, Marines must develop counter-deception techniques in order to detect deception and protect decision makers from adversary attempts to mislead.

Within the US military, deception is generally separated into three categories: Joint military deception (MILDEC), deception in support of OPSEC (DISO), and tactical deception (TAC-D). Joint MILDEC is planned and conducted at the Geographical Combatant Command (GCC) or Joint Task Force (JTF) levels and support campaigns at the operational level of war. Joint MILDEC is highly sensitive, controlled by certified Joint MILDEC planners, and uses compartmentalized programs specifically designed to support joint MILDEC operations.

Specialized training and MILDEC certification is required for joint MILDEC planners provided again by the Joint Forces Staff College. Today, most Marines are unaware of Joint MILDEC programs, lack MILDEC certification, and are unable to leverage current MILDEC capabilities to support MAGTF operations.

DISO is military deception that protects friendly operations, programs, and other assets against foreign intelligence and security services (FISS) collection. DISO is intended to create multiple false indicators to confuse FISS, limiting their ability to collect accurate intelligence on friendly forces. In today's operating environment, despite our best efforts to protect critical information, a foreign collection agency may be able to penetrate the OPSEC or information assurance (IA) measures implemented by friendly forces. In order to fill this security gap, DISO can provide an additional layer of protection to create ambiguity and mislead an adversary able to defeat friendly OPSEC measures. DISO makes it difficult for an adversary to make sense of the information they are able to collect. Unable to identify what information is useful or true, adversary collections can be discouraged and their assets directed to softer targets. Once OPSEC is integrated into Marine Corps planning and execution, incorporating DISO will become a key component to countering sophisticated adversary collects efforts.

Lastly, TAC-D is deception conducted to support battles and engagements. TAC-D is planned and executed by tactical-level commanders to cause adversaries to take actions that are favorable to the US commanders' objectives. The Marine Corps plans and executes TAC-D by conducting deceptive actions such as feints and ruses. Unfortunately, Marine maneuver units rarely get an opportunity to practice TAC-D in exercises or training. Exercises such as the Integrated Training Exercise (ITX), a live fire maneuver exercise at 29 palms, is highly scripted and controlled with little opportunity to employ TAC-D. A limitation of ITX and other training

venues is the lack of a thinking opposing force (OPFOR) that could be the target of TAC-D. It is difficult for Marine leadership to see the operational value of TAC-D when it is not assessed or required in an exercise focused on the employment of weapons systems against tire stacks and static tank hulks. Absent an opposing force, free play exercise, the Marine Corps will not have the opportunity to employ TAC-D prior to actual combat operations.

Overall, more must be done to institutionalize MILDEC within the Marine Corps. The current operating environment requires the Service to create a professional body of trained Joint MILDEC planners who can access JTF or GCC MILDEC plans and programs to support MAGTF operations. DISO must be developed to enhance security, compliment OPSEC plans, and counter adversary collections efforts. Training and exercises must allow for “free play” opportunities in order to practice TAC-D against an OPFOR. In order to support DISO and TAC-D, the Marine Corps must invest in the development of 21st century decoys that mimic the signature or profile of Marine Units. Marines must also receive the necessary security clearances and program read-ins to access current deception programs. Fully operationalizing MILDEC will greatly enhance the Marine Corps ability to maneuver physiologically and attack or disrupt the mental capacity of an individual, adversary, or system.

Military Information Support Operations (MISO)

Like MILDEC, MISO is not new to military operations. Influencing the behavior of foreign target audiences in a way that is favorable to military objectives has been done for centuries. MISO, formerly psychological operations (PSYOPs), are planned operations to convey selected information and indicators to audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of governments, organizations, groups, and individuals.²⁹ Within the US military, the Army has long been the standard bearers for MISO

within the armed forces. Only recently has the Marine Corps begun to invest in MISO. During the heights of Operations Enduring and Iraqi Freedom, the Army could no longer provide tactical MISO detachments to the Marine Corps. In 2006, the Marine Corps grew in size to an end strength of 202,000 personnel and decided to invest in creating the Marine Corps Information Operation Center (MCIOC). As a part MCIOC's structure, the Marine Corps' first ever MISO Company was established. Since becoming operational in 2009, the Marines of MISO Company have been subject to a high operational tempo as they are deployed to support of contingency and combat operations. As a small unit of approximately 60 Marines, meeting the MAGTF's demand for MISO at all levels presents major challenges. Since MISO is not a primary military occupational specialty (PMOS) within the Marine Corps, turnover of personnel makes it difficult to establish a professional force with experienced leadership. Also, fielding of MISO specific equipment and sustaining it has been a challenge for MCIOC and MISO CO.

The current model for Marine MISO is not sustainable to meet the demands of the service and will soon drive a decision point. What should the future look like for Marine MISO and does the service need to establish a PMOS? As *Warfighting* tell us, a full appreciation of maneuver warfare must move beyond the spatial and physical application. Maneuver can also be conducted within the psychological dimension and the Marine Corps must have a professional force to accomplish this. In today's operating environment, the ability to plan and execute influence operations in support of MAGTF operations will be vital throughout the range of military operations. During shaping, MISO could be used to influence friends, neutrals, and potential friends or deter adversarial behavior before conflict. During combat operations, MISO can influence adversary target audiences (surrender appeals) or civilian populations (non-interference messages) in support of combat operations. To enable psychological maneuver for

the MAGTF, MISO planners will be required within the MAGTF command elements and expeditionary MISO teams must be established at the Marine Expeditionary Force (MEF) level to be employed as required.

Technical Information Operations Professionals

As the electromagnetic spectrum (EMS) and the cyberspace domain take on greater importance in the current operating environment, the need for technical experts within the Marine Corps will be critical. In order to conduct information warfare, the Marine Corps will need SMEs for electronic warfare and cyberspace operations. Currently, the Marine Corps creates free MOS (FMOS) 8834 or technical IO Officer. This FMOS is awarded following completion of a two-year master degree program offered at Naval Postgraduate School (NPS) in Monterey California. The curriculum for this course involves systems engineering to include information systems and operations. This is exactly the technical expertise that is required with the Marine Corps in the information technology rich operating environment of today. Surprisingly, across the Marine Corps, there are few 8834 billets. All must be filled by the few NPS graduates as payback tours for the graduate degree they were awarded. There is currently an insufficient number of billets considering the importance of information systems and the EMS on current military operations. Of further concern, 8834s are routinely not employed using the systems engineering degree they have earned through the NPS program. Many are used in IO planning roles, a position many are untrained for. Currently IO planning is the responsibility of FMOSs 0510 (Basic IO Staff Officer), 0550 (Advanced IO planner), 0551s (IO Specialist). The planning focused IO AMOS's are not interchangeable with the technical focus of an 8834.

Moving forward, the service must re-evaluate the employment of 8834s across the Marine Corps. The current population of 8834s is a fraction of what is required in the current

operating environment. Also, technical specialists in information systems, the EMS, and cyber domain must be created. Within a contested information environment, where adversaries are maneuvering and conducting sophisticated information and cyberspace operations, the Marine Corps must field professionals who are training to support, defend, and conduct offensive operations within the information and cyberspace domains. While the service has invested in cyber professionals and created Marine Forces Cyber Command (MARFORCYBER), very few resources are allocated to support MAGTF operations. In the MAGTF of the future, the Marine Corps must fully integrate technical IO specialists and officers who can support defensive and offensive operations in a contested information environment, EMS, and cyber domain. Where electronic warfare and cyberspace operations were once considered small and specialized fields, they must now take a prominent position within the MAGTF. These assets, long held at the CE level, must be developed and fielded at the lowest level possible in support of the MSEs of the MAGTF. Operations personnel (S-3/G-3) must be trained in IO planning in order to integrate these capabilities with the advice of 8834s and technical specialists. Only with broadly fielded tech IO specialists can the MAGTF maneuver within the contested technological dimension, cyber domain and EMS.

Implementing the Institutional Change to support Information Age Warfighting

Change does not come quickly for the Marine Corps. As stated earlier, cultural and structural limitations prevent sweeping changes across the service. Current efforts to promote institutional changes across the Marine Corps are focused on implementing the MOC. Under the Marine Corps Combat Development Command (MCCDC), the Marine Corps Warfighting Lab (MCWL) and Futures Directorate has conducted a series of wargames to inform future requirements and capability development aligned to Future Force 2025 and the MOC.

Throughout the past year, the results of the wargames have included many recommendations for organizational changes to the MAGTF to realize many of the MOCs objectives. One objective, to develop a broader concept of combined arms and information warfare has led to recommended changes to HQMC and the MEF Command Elements. These changes will include the establishment of the Deputy Commandant for Information Warfare (DC IW) which will be a three-star position to advise the Commandant and act as the Service advocate for information warfare. Within the MEF, the MEF information group (MIG) will be created to integrate the information warfare capabilities across the MEF in support of MAGTF operations.

Throughout this process, a key limitation has been the focus on organization and structure. PowerPoint briefs summarizing MOC implementation recommendations emphasis line and block diagrams with associated billet lists. The official process for determining requirements and capabilities for the Marine Corps seems to have been replaced by good ideas and individual community advocacy. Where is the clear articulation of the need for the MIG in each MEF? What essential tasks will the MIG perform or support and to what standard? What personnel, equipment, and training is required for the MIG? All of these questions are currently unanswered. It can be perceived by Marines that the Service wishes to create these organizations now and then figure out what they do later. Absent a complete capability based assessment (CBA), the fielding of the MIG may not consider all doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) considerations.

In order to not repeat the mistakes of the past, the Marine Corps should examine past failures to field new capabilities completely. A good example is the before mentioned fielding of MISO within the Marine Corps. The creation of the first Marine Corps MISO company was conducted outside the traditional CBA and DOTMLPF framework. The result has been a unit

with train, man, and equip issues that undermine its ability to support MAGTF operations. For years, the MCIOC MISO company was not linked to a mission essential task list (METL) until the winter of 2017. Without a MCIOC METL, MISO CO had no personnel, equipment, training, or certification standards. This meant that the MCIOC and MISO Company Commanders had only a subjective ability to assess their unit's readiness to conduct MISO. Also, the Marine Corps had no visibility on the readiness of a very limited resource because MISO Company was not represented in the Defense Readiness Reporting System Marine Corps (DRRS-MC).

To further complicate the issue, as MISO Company deployed detachments in support of MAGTF exercises and deployments, the gaining units had the same issues. As a priority MAGTF to receive MISO detachments from MCIOC, the Marine Expeditionary Unit (MEU) has no MISO representation in its Core METL. If there is no essential task or standard that the MCIOC MISO detachments supports, why do they exist or deploy at all? What specific task do the MISO Marines support and to what standard? Without METL representation, the MEU Training and Readiness (T&R) manual does not include collective MISO training standards. Expeditionary Operations Training Group (EOTG) and MAGTF Staff Training Program (MSTP) who organize and conduct the MEU training and certification programs, have no standards to evaluate MEU readiness to conduct MISO. The results have been very detrimental to MISO in support of MAGTF operations. Gaining Commanders do not fully understand the MISO capability or how it supports their unit. Also, individual MISO Marines are unable to fully explain how they support the tasks and missions of the MAGTFs they support. All of these issues have resulted from a failure by the Service to field the MISO capability within the Service outside the CBA and DOTMLPF process.

As the Marine Corps continues the MCWL Wargames to develop requirements for implementing the vision of the MOC, it should do so in a deliberate and complete manner. To conduct warfighting in the information age, IO, MISO, OPSEC, and MILDEC professionals will be needed to maneuver the technological and psychological dimensions. As the Marine Corps seeks to organize, train, and equip to fight and win in the information age, the Service must learn the lessons the failure to integrate MISO into the Service or risk repeating them. A complete review of the requirement for these capabilities must be conducted across Headquarters Marine Corps (HQMC), the supporting establishment, and the operating forces (OPFOR) in order to identify current gaps across the Marine Corps as a whole. HQMC must ensure that these capabilities receive the proper advocacy and that they are developed and fielded completely across the DOTMLPF framework. Within the MAGTF, the Marine Corps must ensure that information age, warfighting capabilities are represented within appropriate unit METLs. Accurate and complete METLs will ensure that resourcing (personnel, equipment, funding, etc.) and training are aligned with mission requirements. Relevant and useful assessment criteria will then enable the evaluation of individual and unit readiness to conduct information age warfighting as a part of MAGTF operations. Taking these steps will enable the Marine Corps to realize the potential of these capabilities and help set the conditions for the Service envisioned in the MOC.

Conclusion

The time has come to organize, train, and equip the Marine Corps for warfighting in the information age. The recently published MOC and Ellis Group essays for the *Marine Corps Gazette* demonstrate that the Marine Corps of the future will be required to conduct warfighting in all domains, not exclusively the physical components of the operating environment. An

examination of our adversary's actions reveals that they have adapted strategies that avoid US military strengths and exploit our weaknesses in the information environment. Configured for the battles of the industrial age, the US military has been slow and resistant to the changes necessary to operate in the current operating environment. The Marine Corps has yet to adapt the means and methods of war that enable maneuver warfare in an environment of prolific information and information technology.

In order to fight and win the battle of the information age, the Marine Corps must adapt to wars changing character and field capabilities that enable maneuver warfare in its psychological and technological dimensions, not just the spatial and temporal. Rooted in the nature and theory of war, *Warfighting* provides the framework for enabling maneuver in all dimensions, we need only to apply it. By denying adversary abilities to collect critical information, deceiving adversary decision makers, and influencing select target audiences for military advantage, the Service can directly affect the mental and psychological aspects of our adversaries through the capabilities of the information age. Fielding technical IO specialists and officers, combined with IO planners to integrate these capabilities as inherent to operations, will facilitate combined arms in all domains as envisioned in the MOC. Absent the type of conceptual and functional changes advocated in this paper, our adversaries will continue to thrive in the aspects of the environment effectively ceded to them by our inaction. This must not be allowed to happen. The time has come for the Marine Corps to seize the opportunities provided by the ascendance of information and information technology. In doing so, the Marine Corps will realize the potential of maneuver warfare in the 21st century and remain the military's premiere force in readiness across the spectrum of conflict, ready to fight and win the battles of information age.

-
- ¹ Lonsdale, David J. 2004. *The Nature of War in the Information Age: Clausewitzian Future*. Cass series-strategy and history, 9; Cass series-strategy and history, 9. London: Frank Cass, 1.
- ² Marine Corps Intelligence Activity. *2015-2025 Future Operating Environment: Implications for Marines*. (March 2015): 39.
- ³ Knox, Macgregor. 2001. *The Dynamics of Military Revolution 1300-2050*. 178.
- ⁴ Berkowitz, Bruce D. 2003. *The New Face of War : How War Will Be Fought in the 21st Century*. 18.
- ⁵ Joint Chiefs of Staff. *Joint Operating Environment 2035 (JOE 2035): The Joint Force in a Contested and Disordered World*, Washington, DC: US Department of Defense. (2016). 39.
- ⁶ Brown, Ian T. "Warfighting 3.0" *Marine Corps Gazette* 100, no. 8 (August 2016). 66.
- ⁷ Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare: China's Master Plan to Destroy America*. Panama City, Panama: Pan American Publishing Company. 2002., pg 38-43.
- ⁸ Lee, Sangkuk. "China's 'Three Warfares': Origins, Applications, and Organizations." *Journal of Strategic Studies* 37 (2014): 198.
- ⁹ Brown, Ian T. "Warfighting 3.0" *Marine Corps Gazette* 100, no. 8 (August 2016). 66.
- ¹⁰ Ibid. 67.
- ¹¹ Mark Mateski, "Russia, Reflexive Control, and the Subtle Art of Red Teaming" *Red Team Journal*, October 13, 2016.
- ¹² Brown. "Warfighting 3.0" 70.
- ¹³ Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* Vol. 17 (2004): p.237-256.
- ¹⁴ Adamsky, Dmitry. "Cross-Domain Coercion: The Current Russian Art of Strategy" *Proliferation Papers* 54 (2015).
- ¹⁵ Gorka, Sebastian L. 2015. *The Islamic State and Information Warfare: Defeating ISIS and the Broader Global Jihadist Movement*, <http://www.threatknowledge.org>, 1.
- ¹⁶ CNN <http://www.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/index.html>
- ¹⁷ Gorka, Sebastian L. 2015. *The Islamic State and Information Warfare: Defeating ISIS and the Broader Global Jihadist Movement*, <http://www.threatknowledge.org>, 2.
- ¹⁸ Knox, Macgregor. 2001. *The Dynamics of Military Revolution 1300-2050*. Cambridge: Cambridge University Press. 178.
- ¹⁹ Headquarters US Marine Corps. *Warfighting*. MCDP 1. Washington, DC: Headquarters US Marine Corps, (June 30, 1991): 3.
- ²⁰ Ibid. 3.
- ²¹ Knox, 178.
- ²² Ibid. 176.
- ²³ *Warfighting*, 15.
- ²⁴ Ibid. 16.
- ²⁵ Headquarters US Marine Corps. *Marine Air Ground Task Force Information Operations*. MCWP 3-40.4. Washington, DC: Headquarters US Marine Corps, (March 2014): 1-1.
- ²⁶ Headquarters US Marine Corps. *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. Washington, DC: Headquarters US Marine Corps, (September 2016): 8.
- ²⁷ Ibid. 6.
- ²⁸ Tao, Hanzhang, Shibing Yuan, and Sunzi. 1987. *Sun Tzu's Art of War: The Modern Chinese Interpretation*. New York: Sterling Pub. 23.
- ²⁹ Marine Air Ground Task Force Information Operations. 3-6.

Bibliography

- Adamsky, Dmitry. "Cross-Domain Coercion: The Current Russian Art of Strategy" Proliferation Papers 54 (2015).
- Berkowitz, Bruce D. 2003. *The New Face of War: How War Will Be Fought in the 21st Century*. New York: Free Press. <http://catdir.loc.gov/catdir/enhancements/fy0641/2003042405-s.html>.
- Brown, Ian T. "Warfighting 3.0" *Marine Corps Gazette* 100, no. 8 (August 2016).
- Gray, Colin S. *Another Bloody Century: Future Warfare*. London: Phoenix. 2006.
- Headquarters US Marine Corps. *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. Washington, DC: Headquarters US Marine Corps, September 2016.
- Headquarters US Marine Corps. *Warfighting*. MCDP 1. Washington, DC: Headquarters US Marine Corps, June 30, 1991.
- Headquarters US Marine Corps. *Marine Air Ground Task Force Information Operations*. MCWP 3-40.4. Washington, DC: Headquarters US Marine Corps, March 2014.
- Joint Chiefs of Staff, *Joint Operating Environment 2035 (JOE 2035): The Joint Force in a Contested and Disordered World*, (Washington, DC: US Department of Defense, 2016).
- Knox, Macgregor. 2001. *The Dynamics of Military Revolution 1300-2050*. Cambridge: Cambridge University Press.
- Lee, Sangkuk. "China's 'Three Warfares': Origins, Applications, and Organizations." *Journal of Strategic Studies* 37 (2014): 198.
- Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare: China's Master Plan to Destroy America*. Panama City, Panama: Pan American Publishing Company. 2002.
- Lonsdale, David J. 2004. *The Nature of War in the Information Age: Clausewitzian Future*. Cass series--strategy and history, 9; Cass series--strategy and history, 9. London: Frank Cass.
- Marine Corps Intelligence Activity. *2015-2025 Future Operating Environment: Implications for Marines*. March 2015.
- Mateski, Mark. "Russia, Reflexive Control, and the Subtle Art of Red Teaming" *Red Team Journal*, October 13, 2016.
- Tao, Hanzhang, Shibing Yuan, and Sunzi. 1987. *Sun Tzu's Art of War: The Modern Chinese Interpretation*. New York: Sterling Pub.