REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
(05-04-2012)	FINAL	

4. TITLE AND SUBTITLE
"Technical" Application of the Human Element in the Information Domain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Sharon Pinder

Paper Advisor (if Any): **N/A**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
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
Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Information Operations (IO) are a national priority and a critical enabling capability for every type of operation conducted by the Joint Force Commander. Although IO is recognized as a necessity for future, and arguably current irregular warfare that involves kinetic and non-kinetic options, it has been difficult to identify a service career force capable of integrating full spectrum Information Operations. The Navy Information Warfare Officer (IWO) with core skills of Signals Intelligence (SIGINT), Electronic Warfare (EW) and Computer Network Operations (CNO), although focused on the technical elements that comprise the information environment, is best suited to "subvert, coerce, attrite, and exhaust adversaries rather than defeat them through direct conventional military confrontation," while protecting our own force; and incorporate the remaining IO components of Military Deception (MILDEC), Operations Security (OPSEC) and Military Information Support Operations (MISO) into full spectrum operations. The Navy should be designated the Joint Force Information Operations Component Commander to fully integrate IO into full spectrum operations.

15. SUBJECT TERMS
Information Operations, Cyberspace, Human Element, Electronic Warfare, Computer Network Operations, SIGINT

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		24	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

"Technical" Application of the Human Element in the Information Domain

by

Sharon Pinder

LCDR USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____//s//_____

04 May 2012

Contents

Abstract

"Technical" Application of the Human Element in the Information Domain

Information Operations (IO) are a national priority and a critical enabling capability for every type of operation conducted by the Joint Force Commander. Although IO is recognized as a necessity for future, and arguably current irregular warfare that involves kinetic and non-kinetic options, it has been difficult to identify a service career force capable of integrating full spectrum Information Operations. The Navy Information Warfare Officer (IWO) with core skills of Signals Intelligence (SIGINT), Electronic Warfare (EW) and Computer Network Operations (CNO), although focused on the technical elements that comprise the information environment, is best suited to "subvert, coerce, attrite, and exhaust adversaries rather than defeat them through direct conventional military confrontation," while protecting our own force; and incorporate the remaining IO components of Military Deception (MILDEC), Operations Security (OPSEC) and Military Information Support Operations (MISO) into full spectrum operations. The Navy should be designated the Joint Force Information Operations Component Commander to fully integrate IO into full spectrum operations.

Introduction

Carl von Clausewitz wrote a masterpiece of warfare theory in *On War* nearly 200 years ago that still today guides the thinking of leaders at all levels, both military and civilian, in how to evaluate war. There has long been debate over Clausewitz's disdain for information in his magnum opus, in which he opined that a commander's imperfect knowledge of a situation could stop military actions, and that his ability to know his enemy was based upon unreliable intelligence.[i] In twenty first century irregular warfare can there be near-perfect, timely and reliable information, or intelligence, given technological advances? How can the human element be best organized congruent with technology to challenge the information environment and ensure the commander has the best knowledge of the situation?[ii]

Since technology will always change and become more complex, the pursuit of success in war should not solely focus on the information technology itself, but in developing people capable to navigate through the information domain in order to protect our own information and manipulate the adversary's perception of information. Information Operations (IO) are of supreme importance for the successful execution of military operations.[iii] The primary objectives of IO are to achieve and maintain information superiority, and provide the Joint Force Commander (JFC) with adversary intent in order to gain an advantage in information that translates into the best possible knowledge for the commander's decisions.[iv] The JFC can best position his joint force for success in irregular warfare that consists of kinetic and non-kinetic actions, and relies on use of the larger information domain, if he designates the Navy as the lead Information Operations component. The Navy Information Warfare Officer (IWO) with core skills of Signals

Intelligence (SIGINT), Electronic Warfare (EW) and Computer Network Operations (CNO), although focused on the technical elements that comprise the information environment, is best suited to subvert, coerce, disrupt, and exhaust adversaries using IO, rather than defeat them through direct conventional military confrontation, while protecting our own forces; and incorporate the remaining IO components of Military Deception (MILDEC), Operations Security (OPSEC) and Military Information Support Operations (MISO) into full spectrum operations. The IWO focus on the human element is the key to irregular warfare because these specialized, operational level leaders can employ all of the non-kinetic weapons in the information domain and ensure the commander has the best possible knowledge of the situation, while simultaneously denying the adversary information critical to their success.

Technology vs. The Human Element

The Navy has always concentrated heavily on technology because the nature of naval warfare requires that all tools necessary for battle set sail with the platform when it departs homeport. Dr. Vego argues that the hyper-focus on technology is at the peril of achieving balanced naval combat force, adequate doctrine above the tactical level to govern naval force actions, and definitive theory that defines naval operations.[v] The cumulative effect of focusing too heavily on technology and not supporting the naval warfare ethos with doctrine inadvertently withers the true center of gravity, the human element.[vi] The center of gravity concept originated from Clausewitz and is defined by the Department of Defense as "the source of power that provides moral or physical strength, freedom of action, or will to act."[vii] So, even though technology has changed the dynamic of warfare and the information domain from the days of Clausewitz, the human investment still remains the best possible weapon against future threats.

The information domain looms larger than the technologies that feed it – it is an enabling function for everything that the military does. As a result, the Secretary of Defense indicated in the 2001 Quadrennial Defense Review (QDR) Report that "information operations have become the backbone of networked, highly distributed commercial civilian and military capabilities."[viii] Instead of attempting to incorporate all Information Operations (IO) core capabilities into a single career force, it is best to further subdivide the IO "elephant" into manageable components – those that can operate through the information domain notwithstanding technology, and those that operate on the information domain. [ix]

The Navy IWO community is positioned as a human/doctrine/resource alignment success story for the Navy and the joint force because the structure is focused on developing leaders to facilitate maneuver through the information domain. [x] Specifically, the focus on the technical aspects that enable the information domain combined into a single career force result in a cadre of people who understand how to deliver the effects -disrupt, deny, protect, coerce, etc. - through the information domain and incorporates non-technical IO components as well. The information domain is complex, adaptive and difficult to predict. The Navy IWO inclusion of each technical core capability into a single workforce doesn't focus on new, niche technologies, such as cyberspace, but a holistic approach to manipulating the information domain to compete against asymmetric threats in irregular warfare. The evolution of the Navy IWO from SIGINT to EW and CNO and combination of these skills make it best suited of all the services to lead the joint force in achieving full spectrum IO integration.

Possible Counter-Arguments – Is it Possible? or Chasing Technology?

Although combing the technical IO core capabilities of SIGINT, EW and CNO into a single career force appears to address the evolving complex nature of the information domain, current Navy IWOs lack a common career background, baseline training, and level of knowledge.[xi] As a result, while they are expected to be specialists and experts in the technological aspects of the information domain, they have difficulty operational SIGINT, EW, and CNO. Additionally, the alignment of the core capabilities was not rooted in a training program that adequately prepared the IWO in each of the core capabilities. While SIGINT is a foundational skill that a Navy IWO brings to the table, the EW and CNO specialties introduced later were not heavily indoctrinated or native capabilities. SIGINT, EW and CNO each require specific attention to the intricacies inherent to their segment of the information domain. The challenge to having a human that understands each of these functions implicitly, combined with an overemphasis on technology in the Navy, make it unlikely that the Navy IWO model can truly revolutionize modern warfare.

Another possible argument is that including so many technical specialties into one career field is arguably chasing stove-piped technology and not centered on human beings having the ability to surmount the technology. Dr. Vego highlights the overemphasis of technology, stating, "One of the most pernicious effects of all [this] is a general neglect and underestimation of the role of people."[xii] Focusing the Navy IWO community on the latest technological advances such as cyberspace may be exactly that – a press towards technology, not people.

Regardless of technology and in line with Clausewitz's theories, the human capacity to collect, analyze and process information will likely still result in inaccurate

intelligence/information in war. A Navy IWO that attempts to integrate the SIGINT, EW and CNO capabilities will still be chasing stovepiped technologies rather than achieving a macro-view of the information domain. The joint force is no closer to achieving an all-encompassing IO workforce than it was in 2001, when it was first directed in the Quadrennial Defense Review (QDR) Report and subsequently reinforced in the 2006 version.[xiii]

Why the Navy? Evolution from Cryptology

Navy IWOs today are positioned to lead the joint force at the operational level in conducting Information Operations. Similar to the Surface Warfare Officer (SWO) who leads myriad professional specialties on the maritime domain to achieve objectives, the IWO leads technical professionals that employ various tools on the information domain, regardless of platform, for non-kinetic effects. The Navy IWO construct is ideal for organizing the human element to meet the challenges associated with changing information mediums. Although the IWO core competencies are technically intricate, combining these capabilities is not focused on the different types of information environments, but on the ability of professionals to operate through the information domain for a desired operational effect.

In March 2012, the Navy celebrated 77 years of cryptologic operations and Information Warfare. The first wireless radio transmission sent from a U.S. Navy ship in 1899 during the Civil War established a need for radio signals intelligence in the maritime domain.[xiv] Navy cryptologists rose to the challenge and were involved in every major conflict following the turn of the century. The accomplishments of Navy cryptology contributed to the allied victories in World War II, both in Japan and Europe.

The Chairman of the Joint Chiefs of Staff realized the need to optimize allied and U.S. military information potential in 1993 when he revised the 1990 Memorandum of Policy 30 with a new Joint definition of Command and Control Warfare (C2W):

> The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict.[xv]

Command and Control Warfare gave way to the name Information Operations (IO), and in 2002, the Chief of Naval Operations underpinned the SECDEFs emphasis on IO from the 2001 QDR Report, and established IO as a warfare area on the same plane as space, air and maritime operations.[xvi] Recognizing the need to evolve with the dynamic information environment, Navy cryptologists were re-named Navy Information Warfare Officers in 2005 as they expanded their specialized SIGINT capability to formally include Information Operations responsibilities.[xvii]

Naval Security Group (NAVSECGRU) was previously in charge of Navy SIGINT until it was disestablished in 2005. Naval Network Warfare Command (NNWC) assumed the Navy SIGINT missions from NAVSECGRU and added SIGINT to its networks, space and IO missions.[xviii] Changing the name of the Officer corps and subsequently re-aligning under NNWC was significant because the Navy recognized the complexity of new information technologies and the need to have a professional workforce capable to surmount the associated challenges. In May 2009 the Chief of Naval Operations, Admiral Roughead, spoke before the House Armed Services Committee on the Fiscal Year 2010 Department of Navy posture. He stated:

> "Our Navy has provided cyber capabilities to the joint force for more than 11 years and we continue to make security and operations in the cyberspace domain a warfighting priority…We are taking steps to effectively organize, man, train, and equip our Navy for cyber warfare, network operations, and information assurance..."[xix]

The Navy took the next step in January 2010 as a part of Admiral Roughead's vision by establishing Fleet Cyber Command (FLTCYBERCOM) and re-commissioning the U.S. TENTH Fleet (C10F) to position the force for excellence in the maritime, cyberspace and information domains.[xx] The Navy was the first service component to stand up and incorporate these changes. FLTCYBERCOM serves as the "central operational authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and ashore."[xxi] The evolution of the Navy IWO community to encompass the technical core capabilities of SIGINT, EW and CNO into a single Officer is a unique characteristic amongst the services. This combination of factors creates a synergy that helps to focus the IO capabilities through advance knowledge of adversary intent using SIGINT/cryptology and non-kinetic defensive and offensive operations in CNO and EW. This rich history and evolution makes the Navy the best component to assume duties as the Joint Force Information Operations Component Commander (JFIOCC).

Core Capability – SIGINT **-** Navy cryptology, or SIGINT, is the oldest discipline of the three IWO core capabilities and has been used in every war since the 1900s. One of the most successful stories of Navy cryptology was WWII in the Pacific where successful code breaking helped turn the tide of the war. SIGINT includes Communications Intelligence (COMINT), Electronic Intelligence (ELINT) and Foreign Instrumentation and Signals Intelligence (FISINT) and is used interchangeably with the term cryptology. Naval

cryptology refers to "action taken to exploit and attack foreign communications and other electromagnetic signals, while protecting our own, for the purposes of command and control warfare, electronic warfare, signals intelligence, and signals security."[xxii]

The Battle of Midway is a historical example of that demonstrates how the art of cryptology can provide the commander with adversary intent by exploiting vulnerabilities created by operating on the information domain. In the spring of 1942, the U.S. Pacific Fleet, commanded by Admiral Nimitz was reduced to 3 aircraft carriers, 45 combatant surface ships and 25 submarines to oppose a much larger Japanese fleet led by Admiral Yamamoto.[xxiii] Since Nimitz's fleet was so diminished it was critical that he know in advance the Japanese plans for their next attack so he could conduct a surprise counter-attack.

In order to achieve operational surprise and succeed in an offensive strike against the superior Japanese fleet, Nimitz relied upon the Navy radio intelligence group, commanded by Commander Rochefort, to collect the Japanese Navy command code (COMINT), JN-25, to reveal the planned location of Yamamoto's fleet.[xxiv] The cryptologic art applied by Rochefort and staff combined complex traffic analysis and technical skill to determine the "identity of enemy call signs" and "pattern and extent of [their] radio transmissions."[xxv] As a result, the operational commander, Nimitz, was able to properly position his limited naval force to defeat the Japanese Fleet and shift the momentum of the war in favor of the allies.

Cryptology/SIGINT is collecting and exploiting communications and electronic emissions in order to gain warning of an adversary's intention and achieve the information advantage to determine appropriate force apportioning against a threat. This is the oldest, indigenous capability that a Navy IWO has to enable focused, full-spectrum IO.

Core Capability – Electronic Warfare- The Navy IWO core capability of EW was chronologically the next capability and was used during World War I. SIGINT/cryptology is technically a component of EW that falls in the Electronic Warfare Support (ES) category but has significant, complicated nuances that warrant an individual entry for the art. The difference between conducting an ES mission or a SIGINT mission is written in JP 3-13.1 as being separated by who "tasks or controls the collection assets, what they are tasked to provide, and for what purpose are they tasked." Regardless of the task-er, ES is passive collection that produces early warning, adversary intent, location and identity of a threat.[xxvi] The Navy regularly uses the same equipment to conduct both EW and SIGINT missions and those units may be tasked at the same time to do both types of missions. The amalgamation of SIGINT and EW resources necessitates a human trained in both core capabilities. This is an indigenous skill of the IWO and is not centered on a particular platform but on manipulation of the Electromagnetic Spectrum (EMS), which is a part of the information domain.

EW is a significant non-kinetic capability that requires constant adaptation and creativity inside of the EMS to gain and maintain an advantage over an adversary. EW has three basic components: "(1) Electronic Attack (EA), the offensive use of electromagnetic energy to deny, degrade or disrupt enemy capabilities; (2) Electronic Protection (EP), the defensive measures taken to guard equipment against such attacks; and (3) ES, the detection, localization and identification of hostile emitters to understand an adversary's use of the spectrum."[xxvii] Attaining superiority in the EMS is similar to the discussion of sea control or air superiority. The desired end state with control of the EMS is to be able to do what you

want to do, how and when you want to do it. The Navy started early in history in the race to EMS superiority because of its heavy reliance on technology.

By World War II, the benefit of communicating, increasing command and control capability and countering enemy emissions outweighed the risk of electronic communications being intercepted by the adversary. A recent success story of EW is derived from Operations IRAQI and ENDURING FREEDOM where EP significantly reduced a threat to coalition forces. In the beginning of the war, the U.S. and coalition ground forces suffered heavy casualties as a result of Radio-Controlled Improvised Explosive Devices (RCIED) employed by insurgents. The insurgents were using cellular phones, garage door openers, and other electronic implements to remote detonate explosive devices.[xxviii] In 2005, the Chief of Naval Operations recognized the Navy's strong history and unique EW expertise, and directed Navy to support the joint missions in Iraq. [xxix] The U.S. Army had not sustained its EW capability following the Cold War and did not have the indigenous capability to conduct EP and disrupt the signal between the radio device and the IED. The U.S. Navy has a strong history of EW capability and maintains a nucleus of EW personnel from the EA-6B (Prowler) Aviation and IWO communities. As a result, it is possible to have an IWO with experience conducting EW missions in the space, air, land and sea domains that truly understands the technical nuances of EW not associated with a specific platform.

***Core Capability – Computer Network Operations*-** The Navy IWO core capability of CNO is the most recent capability and newest focal point given the new medium of cyberspace in which to wage war, and the significant impact a war within the cyber domain would have. The modern western world is extremely reliant on information technology and cyberspace for communication, critical infrastructures

such as energy and water, and transportation. Cyberspace is a part of the larger information domain and at many different levels, the EMS. The Department of Defense 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."[xxx] Subsequently, cyberspace operations are actions such as CNO that use cyber capabilities to achieve desired military effects.[xxxi] CNO is comprised of Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defense (CND). Cyberspace requires both wired and wireless nodes in the information technology infrastructure in order to deliver information from one point to another.

Cyberspace operations require professionals with a unique set of analytical and technical acumen to conduct non-kinetic offensive (CNA) and defensive (CND) actions. Admiral Leigher indicates a critical vulnerability of current CNO is that the cyberspace operations are mostly reactive to an intrusion and are only capable in defending against known threats.[xxxii] Additionally he indicates that although operating in cyberspace has national level priority and significant effects at all levels, there still remains a lot to be done to codify laws, doctrine and "on-net" operator training to ensure full cyberspace freedom of action.[xxxiii]

What About The Other Three IO Competencies?

The Navy IWO has the technical components of IO, EW (including SIGINT) and CNO, but what about MILDEC, MISO and OPSEC? The argument is clear that one Service cannot dominate all areas of IO simultaneously in a single career field and be exceptional in

all. The Army excels in MISO; the Air Force excels in CNO. Leveraging the strengths of the Services will best strengthen our national defense and ensure the focus remains the human element in IO. The Navy IWO is best positioned to lead the JFIOCC including the remaining three elements of IO because of their comprehension of the information domain, mindset to create operational effects and tactical background that allow seamless integration into operations.

Manipulating cyberspace and the information domain are critical enablers for MILDEC, MISO and OPSEC. Centuries before technology came to the forefront of military operations, MILDEC, MISO and OPSEC were incorporated into operational planning.[xxxiv] Offensive IO such as EA and CNA "shape the operational environment and create the conditions for employing the other elements of combat power."[xxxv]

MILDEC – Sun Tzu wrote of deception over 2,500 years ago that "All warfare is based on deception. A skilled general must be master of the complementary arts of simulation and dissimulation; while creating shapes to confuse and delude the enemy he conceals his true dispositions and ultimate intent."[xxxvi] Irregular warfare uses an asymmetric or indirect approach to minimize an adversary's power. IO specifically uses the information environment, both physical and non-physical, in MILDEC to "erode an adversary's power, influence and will."[xxxvii] The advent of information technology only changes the means by which an enemy can be deceived. In order to target adversary decision-making, increase the probability of success of friendly actions and deter hostile actions, SIGINT, EW and CNO have a pivotal role. The IWO with a SIGINT background can focus resources to determine adversary intentions and apply deception in support of protecting friendly operations.[xxxviii] Next, using information gained from SIGINT, they incorporate knowledge of the adversary's

method to receive information and construct non-kinetic effects in the EMS to alter his perceived information. Finally, the adversary is targeted with a deception plan using EA, CNE or CNA. Some examples include:

- Manipulating the adversary RADAR to show false images[xxxix]
- Confusing the adversary decision-making by changing resource and personnel information systems through CNE

OPSEC – The IWO can protect friendly intentions that travel and reside on the information domain. Using SIGINT combined with OPSEC allows friendly forces to change or adapt an operation based on knowing what the adversary knows. After an adversary's knowledge of an operation is determined, the IWO can alert the JFC if the adversary is able to interpret friendly intentions and take action to modify the method of friendly transmission of information. Additionally they can plan offensive EW to deny an adversary the capability to intercept and interpret our friendly information. An IWO could then employ CNE to change the key friendly elements of information that are viewable to the adversary in order to protect the specific details of the operation. Lastly, they can conduct a critical assessment of the information environment and determine vulnerabilities based upon their knowledge of the technical intricacies by which information travels and is intercepted. Some examples include:

- Recommend changing call signs or algorithms, or adding Public Key Infrastructure encoding to encrypt information if an adversary has determined specific force information from computer or communications systems

- Changing radiation frequencies of electronic systems based on enemy capability (determined through SIGINT) to intercept friendly emissions in certain frequency ranges

MISO – To support influence operations of MISO, SIGINT should be used to determine the methods an adversary receives information and the nodes that allow information to pass. The world populace receives a large amount of information through cyberspace and mobile communications (see Fig. 1). Given the increased reliance on technology, EW and CNO can be used in the greater MISO plan to deliver messages through cyberspace or the EMS. The Navy IWO does not have the core skill of MISO but can orchestrate an Army MISO component to develop the plan and subsequently determine the best way to coerce or influence the target audience. With an understanding of how to maneuver through the information domain an IWO can project coercion for the JFC using MISO to the desired audience. Some examples include:

- Conducting EA to force the adversary to receive information in a manner desirous for friendly influence
- Delivering MISO messages through email, FaceBook, Twitter, etc.

WORLD INTERNET USAGE AND POPULATION STATISTICS
December 31, 2011

World Regions	Population (2011 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2011	Users % of Table
Africa	1,037,524,058	4,514,400	**139,875,242**	13.5 %	2,988.4 %	6.2 %
Asia	3,879,740,877	114,304,000	**1,016,799,076**	26.2 %	789.6 %	44.8 %
Europe	816,426,346	105,096,093	**500,723,686**	61.3 %	376.4 %	22.1 %
Middle East	216,258,843	3,284,800	**77,020,995**	35.6 %	2,244.8 %	3.4 %
North America	347,394,870	108,096,800	**273,067,546**	78.6 %	152.6 %	12.0 %
Latin America / Carib.	597,283,165	18,068,919	**235,819,740**	39.5 %	1,205.1 %	10.4 %
Oceania / Australia	35,426,995	7,620,480	**23,927,457**	67.5 %	214.0 %	1.1 %
WORLD TOTAL	**6,930,055,154**	**360,985,492**	**2,267,233,742**	**32.7 %**	**528.1 %**	**100.0 %**

Figure 1: World Internet Usage Statistics (http://www.internetworldstats.com/)

Colliding on the Information Operating Environment

The information operating environment consists of cyberspace the EMS, physical and non-physical layers, human components and is integrated throughout every other domain – space, air, sea and land. The linkages between SIGINT, EW and CNO create an opportunity to integrate human understanding into a very complex web of technical infrastructure that operates on physical and non-physical space. Cyberspace has a significant amount of overlap with the EMS. Rear Admiral Filipowski, the former director for Electronic and Cyber Warfare, offered the following alternative definition to cyberspace:

> "When I talk about cyber, I view it as more than e-mail and internet type activities on IP-based networks. Information moving through RF in digital form such as tactical data links, UAV control systems, and satellite-based communications are also cyber in my book. My other point of clarification is about the electromagnetic spectrum (EMS) versus cyberspace. Some would argue these are separate and distinct. However, I would submit that one is a physical domain, which is the electromagnetic spectrum, and that cyberspace is a manmade infrastructure that operates in part in the EMS."[xl]

The increase of wireless capabilities, integrated computer networks and methods of radio frequency communication will challenge the dividing line between EW and CNO.[xli] The SIGINT understanding, as shown in the Battle of Midway example, enables proactive, predictive actions in order to gain situational awareness and concentrate efforts to defeat an adversary. The battlefield is the information environment and it is so vast that Department of Defense efforts must be focused and joint to best defend the nation. SIGINT in conjunction with EW and CNO helps to narrow the focus of operations, based on enemy intent.

Before technology entered the game, Sun Tzu noted of the physical battlespace that, "When the enemy disperses and attempts to defend everywhere he is weak everywhere, and at the selected points many will be able to strike his few."[xlii] Without SIGINT (fused with other intelligence) coupled to EW and CNO, our defensive efforts are reactive once an attack

has happened because protection is limited to the enemy signatures that are already known. Supporting this idea, Vice Admiral Dorsett stated in his discussion of information dominance that, "To be successful in 21st century warfare, the U.S. Navy must create a fully-integrated information, intelligence, C2, cyber & networks capability ... and wield it as a weapon"[xliii] The U.S. Navy brings all of these weapons to bear and is able to fully integrate the JFC IO components to best fight regular and irregular wars.

Current Force Structure

According to joint doctrine, "Combatant commanders normally assign responsibility for IO to the J3. When authorized, the director of the J3 has primary staff responsibility for planning, coordinating, integrating, and assessing joint force IO."[xliv] Conversely, in most operational level commands, SIGINT professionals reside in the J2, separated from the CNO and EW personnel in the J3. As indicated, the three core capabilities SIGINT, EW and CNO, combined in the IWO share resources, create synergy and are inextricably linked. The J2 observes info on the information domain while the J3 operates in and through the domain both kinetically and non-kinetically. The distinction on effects desired from the information domain require a culture change to not look at the IWO as an intelligence professional but as a non-kinetic fires operational leader.

At the tactical level, the Navy IWO serves as the Deputy Information Warfare Commander for the task force and integrates all components of IO. They bring this experience to the operational level, underpinned by the very technical specialties as indicated by the FLTCYBERCOM missions. The IWO is presently a high-demand, low-density member of the JFCs staff because of their unique perspective of the information domain.

Each Combatant Command has approximately two O-4 level IWOs assigned to the staff.[xlv] The Army has focused on the MISO portion of IO and recently, through help of the Navy and Air Force, the EW portion. The Air Force has focused on CNO and EW, but doesn't have a career force that includes both. Neither Air Force nor Army includes the SIGINT capability in their EW, CNO or MISO forces. The Navy IWO career force is the only one that combines the three with a net effect of a single person who has exceptional situational awareness of enemy capabilities, can understand the technical intricacies of the information domain and deliver desired non-kinetic effects in space, air, sea, land and cyberspace.

Conclusion

The Navy IWO has a long history of manipulating the EMS and various types of information networks for desired effects. In 2005, the Chief of Naval Operations envisioned how the Navy could best support the joint "fight" in Iraq and Afghanistan and began the process of sending Sailors downrange to add their technical EW skill to the land force. The idea of Navy personnel operating on land was a strange concept, but in reality it was a visionary move by the Chief of Naval Operations who recognized it was not about the physical domain -space, air, sea or cyberspace -but the skill to maneuver through the information domain writ large with SIGINT, EW and CNO capabilities. Although combining SIGINT, EW and CNO into one career field is not without challenges, it is the best possible solution to the SECDEFs direction in 2001, and again in 2006 to establish an IO workforce. The Navy IWO as the JFIOCC is able to produce desired military, non-kinetic effects on any type of network – computer, human, communications regardless of future changes in capabilities, because of their understanding of the components of the information environment. Joint Maritime Operations Professor and senior Navy IWO, CAPT Petty,

notes: “As a force, our SIGINT background provides a perspective that understands not only how to exploit information but also how to fuse information with other sources to provide an information advantage to the commander.”[xlvi] This is the key capability each Navy IWO brings to the JFC, regardless of level of experience in each specific core capability.

Recommendations

The JFC will best improve his imperfect knowledge of a situation by implementing the following recommendations:

1. Change the mindset that currently places the Navy IWO in the J2 because of the SIGINT capability. The best optimization of the low density IWO is in the J3. The Navy IWO community needs a culture change to realize there is no longer a division between SIGINT/cryptologic capability and IO responsibilities. These are inter-dependent, mutually inclusive, given modern warfare.

2. Increase the number of Navy IWOs assigned to staff. Having two IWOs at the O-4 level are not enough for leadership that incorporates specialists from all other elements of IO. The rank of the Navy IWO on the Combatant Commander’s staff should be increased along with responsibility for the other elements of IO.

3. The Navy should lead the JFIOCC with doctrinally codified supported-supporting relationships with other commanders.

NOTES

[i] Carl von Clausewitz, On War, trans and ed: Michael Howard and Peter Paret (New Jersey: Princeton University Press, 1989) Kindle Edition, 84
[ii] Joint doctrine defines the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (JP 3-13)
[iii] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 13 February 2006), I-1
[iv] Ibid.
[v] Milan N. Vego, "Technological Superiority is NOT a Panacea," *United States Naval Institute. Proceedings* 136, no. 10 (2010), http://search.proquest.com/docview/815414790?accountid=322 (accessed April 17, 2012).
[vi] Ibid.
[vii] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 08 November 2010, as amended through 15 March 2012), 44
[viii] Secretary of Defense, Quadrennial Defense Review (QDR) Report, (Washington, DC: The Pentagon, February 2001),7
[ix] The IO "elephant" refers to all five IO core capabilities of CNO, EW, OPSEC, MILDEC and MISO
[x] Information Warfare Officer Detailer Brief, April 2012, Slide 7
[xi] SIGINT is a component of EW. Future text will describe why the SIGINT element is important to consider
[xii] Milan N. Vego, "Technological Superiority is NOT a Panacea," *United States Naval Institute. Proceedings* 136, no. 10 (2010).
[xiii] Quadrennial Defense Review (QDR) Report, (Washington, DC: The Pentagon, February 2001), 7
[xiv] Targeted News Service, "Navy Information Warfare/Cryptology Community Celebrates 77th Anniversary," 09 March 2012, http://search.proquest.com/docview/926976827?accountid=322 (accessed 12 April 2012).
[xv] Note Chairman, U.S. Joint Chiefs of Staff, *Memorandum of Policy (MOP) 30: Command and Control Warfare* (Washington, DC: CJCS, 1993), 2.
[xvi] - Note Chief of Naval Operations. To Naval Administration, Message NAVADMIN 233/05 151308Z SEP 05. 15 September 2005.
[xvii] Ibid.
[xviii] *History*, Naval Network Warfare Command. http://www.netwarcom.navy.mil/ (accessed April 20, 2012)
[xix] Admiral Roughead, Chief of Naval Operations"Testimony" Before the House Armed Services Committee on FY10 Department of Navy Posture, 14 May 2009, http://www.au.af.mil/au/awc/awcgate/navy/navyposture2009.pdf (accessed 21 April 2012)
[xx] Fleet Cyber Command/Tenth Fleet, Press Release, #10-01, June 29, 2010. http://www.fcc.navy.mil/ (accessed 10 April 2012).
[xxi] Fleet Cyber Command/U.S. TENTH Fleet Website. http://www.fcc.navy.mil/ (accessed 10 April 2012).

[xxii] U.S. Navy, *Naval Intelligence*, Naval Doctrine Publication (NDP) 2 (Washington, DC: Department of the Navy, 30 September 1994),65.
[xxiii] U.S. Navy, "Battle of Midway," http://www.navy.mil/midway/how.html (accessed 16 April 2012).

[xxiv] U.S. Navy, "Battle of Midway," http://www.navy.mil/midway/how.html (accessed 16 April 2012).
[xxv] Jonathan Parshall and Anthony Tully. *Shattered Sword* (Washington D.C.: Potomac Books, 2005), 60.
[xxvi] Chairman, U.S. Joint Chiefs of Staff, *Electronic Warfare*, Joint Publication (JP) 3-13.1 (Washington, DC: CJCS, 08 February 2012),
viii.
[xxvii] Association of Old Crows. *Electronic Warfare: The Changing Face of Combat* http://www.myaoc.org/EWEB/images/aoc_library/Government_Affairs/AOC%20report.pdf (accessed April 14, 2012).
[xxviii] Ibid.
[xxix] Hinkley, Brian E., "Fleet Electronic Warfare Center: Changing the Face of Combat," *InfoDomain Decision Superiority for the Warfighter*, Summer 2009 Issue (2009), 4
[xxx] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 08 November 2010, as amended through 15 March 2012), 83
[xxxi] Ibid.
[xxxii] Rear Admiral William Leigher, "Learning to Operate in Cyberspace." *United States Naval Institute Proceedings* 137, no. 2 (2011): http://search.proquest.com/docview/850462363?accountid=322 (accessed 2 April 2012).

[xxxiii] Ibid.
[xxxiv] Joint Pub 3-13, *Information Operations* (13 February 2006), x.
[xxxv] U.S. Army, *Operations*, Field Manual (FM) 3-0 (Washington, DC: 14 June 2001), 4-10
[xxxvi] Sun Tzu, *The Art of War*, trans. Samuel Griffith (New York: Oxford University Press, 1963), Kindle edition, 41
[xxxvii] Secretary of Defense, *Quadrennial Roles and Missions Review Report*, (Washington, DC: The Pentagon, January 2009), 9
[xxxviii] The intent of a Deception In Support Of OPSEC is to create multiple false indicators to confuse or make friendly force intentions harder to interpret by Foreign Intelligence and Security Service (FISS), limiting the ability of FISS to collect accurate intelligence on friendly forces (JP 3-13.4)
[xxxix] Batson, Mickey and Matthew Labert. "Expanding the Non-Kinetic Warfare Arsenal." United States Naval Institute. Proceedings 138, no. 1 (2012): 40-44, http://search.proquest.com/docview/921024415?accountid=322 (accessed April 21, 2012)
[xl] Filipowski, Sean. Rear Admiral U.S. Navy. "Looking Forward for Maritime Spectrum Warfare" Phoenix Challenge Conferences 2011, as quoted in Mickey Batson and Matthew Labert, "Expanding the Non-Kinetic Warfare Arsenal," *United States Naval Institute. Proceedings* 138, no. 1 (2012), http://search.proquest.com/docview/921024415?accountid=322 (accessed 14 April 2012)

[xli] Chairman of the Joint Chiefs of Staff. *Universal Joint Task List* (Washington, DC: SECDEF) http://www.dtic.mil/doctrine/training/ujtl_tasks.htm (accessed 10 April 2012)
[xlii] Sun Tzu, *The Art of War*, trans. Samuel Griffith (New York: Oxford University Press, 1963), Kindle edition, 42.
[xliii] VADM Jack Dorsett, "Information Dominance and the U.S. Navy's Cyber Warfare Vision", http://www.dtic.mil/ndia/2010SET/Dorsett.pdf, Slide 6.
[xliv] Joint Pub 3-13, *Information Operations*, (13 February 2006), xiii.
[xlv] Fleet Training Management and data Pull System data pull of all 1810, IWOs on COCOM staffs, 12 April 2012
[xlvi] CAPT Roy Petty (Professor, Joint Maritime Operations, U.S. Naval War College), in discussion with the author, 23 April 2012

BIBLIOGRAPHY

Association of Old Crows. *Electronic Warfare: The Changing Face of Combat* http://www.myaoc.org/EWEB/images/aoc_library/Government_Affairs/AOC%20report.pdf (accessed April 14, 2012).

Batson, Mickey and Matthew Labert. "Expanding the Non-Kinetic Warfare Arsenal." *United States Naval Institute. Proceedings* 138, no. 1 (2012): 40-44. http://search.proquest.com/docview/921024415?accountid=322 (accessed April 21, 2012).

Clausewitz, Carl von. *On War.* Translated and edited by Michael Howard and Peter Paret. New Jersey: Princeton University Press, 1989. Kindle Edition.

Filipowski, Sean. Rear Admiral U.S. Navy. "Looking Forward for Maritime Spectrum Warfare" Phoenix Challenge Conferences 2011. Quoted in Mickey Batson and Matthew Labert, "Expanding the Non-Kinetic Warfare Arsenal," *United States Naval Institute. Proceedings* 138, no. 1 (2012): 40-44, http://search.proquest.com/docview/921024415?accountid=322 (accessed 14 April 2012)

Hinkley, CAPT Brian E., "Fleet Electronic Warfare Center: Changing the Face of Combat." *InfoDomain Decision Superiority for the Warfighter* Summer 2009 Issue (2009): 3-4, 25.

Leigher, Rear Admiral William E. "Learning to Operate in Cyberspace." *United States Naval Institute Proceedings* 137, no. 2 (2011): 32-37, http://search.proquest.com/docview/850462363?accountid=322 (accessed 2 April 2012).

Parshall, Jonathan and Tully, Anthony. *Shattered Sword.* Washington, DC: Potomac Books, 2005.

Targeted News Service. "Navy Information Warfare/Cryptology Community Celebrates 77th Anniversary." 09 March 2012. http://search.proquest.com/docview/926976827?accountid=322 (accessed 12 April 2012).

Tzu, Sun. *The Art of War*. Translated by Samuel Griffith. New York: Oxford University Press, 1963. Kindle edition

U.S. Army. *Cyberspace Operations Concept Capability Plan 2016-2028*. Training and Doctrine Command (TRADOC) Pamphlet 525-7-8. Washington, DC: 22 February 2010.

U.S. Army. *Operations*. Field Manual (FM) 3-0. Washington, DC: Headquarters

Department of the Army, 14 June 2001.

U.S. Navy. "Battle of Midway." http://www.navy.mil/midway/how.html (accessed 16 April 2012).

U.S. Navy. Office of the Chief of Naval Operations to Naval Administration. Message: NAVADMIN 233/05 151308Z SEP 05. 15 September 2005. http://www.public.navy.mil/bupers-npc/reference/messages/documents/navadmins/nav2005/nav05233.txt (accessed March 12, 2012).

U.S. Navy. Office of the Chief of Naval Operations. *Naval Intelligence*. Naval Doctrine Publication (NDP) 2. Washington, DC: Department of the Navy, CNO, 30 September 1994.

U.S. Navy. Naval Network Warfare Command. *History*. http://www.netwarcom.navy.mil/ (accessed April 20, 2012)

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, 08 November 2010, as amended through 15 March 2012.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint and National Intelligence Support to Military Operations*. Joint Publication (JP) 2-01. Washington, DC: CJCS, 05 January 2012.

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.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Electronic Warfare*. Joint Publication (JP) 3-13.1. Washington, DC: CJCS, 08 February 2012.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Military Deception*. Joint Publication (JP) 3-13.4. Washington, DC: CJCS, 26 January 2012.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy of the United States of America 2011: Redefining America's Leadership*. Washington, DC: CJCS, 08 February 2011.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Memorandum of Policy (MOP) 30: Command and Control Warfare*. Washington, DC: CJCS 1993.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Universal Joint Task List.* Washington, DC: SECDEF, http://www.dtic.mil/doctrine/training/ujtl_tasks.htm (accessed 10 April 2012).

U.S. Office of the Secretary of Defense. *Quadrennial Defense Review(QDR) Report.* Washington, DC: SECDEF, 2001.

U.S. Office of the Secretary of Defense. *Quadrennial Defense Review (QDR) Report.* Washington, DC: SECDEF, 2010.

U.S. Office of the Secretary of Defense. *Quadrennial Roles and Missions Review Report,* January 2009, http://purl.access.gpo.gov/GPO/LPS108437 (accessed April 12 2012).

U.S. Navy. Office of the Chief of Naval Operations. "The Information Dominance Corps." OPNAVINST 5300.12. Washington, DC: Department of the Navy, CNO, 06 October 2009.

United States Fleet Cyber Command/United States TENTH Fleet. http://www.fcc.navy.mil/ (accessed 10 April 2012).

United States Fleet Cyber Command/TENTH Fleet, Press Release, #10-01, June 29, 2010. http://www.fcc.navy.mil/ (accessed 10 April 2012).

Roughead, Admiral Gary, Chief of Naval Operations. "Testimony" Before the House Armed Services Committee on FY10 Department of Navy Posture 14 May 2009, http://www.au.af.mil/au/awc/awcgate/navy/navyposture2009.pdf (accessed 21 April 2012).

Vego, Milan N. *Joint Operational Warfare: Theory and Practice*. 2007. Reprint, Newport, RI: Naval War College, 2009.

Vego, Milan. "Technological Superiority is NOT a Panacea." *United States Naval Institute. Proceedings* 136, no. 10 (2010): 28-32 http://search.proquest.com/docview/815414790?accountid=322 (accessed April 17, 2012).

Dorsett, VADM Jack, "Information Dominance and the U.S. Navy's Cyber Warfare Vision" (14 April 2010) http://www.dtic.mil/ndia/2010SET/Dorsett.pdf (accessed 20 April 2012).