AIR WAR COLLEGE

AIR UNIVERSITY

THE SHORELINE: WHERE CYBER AND ELECTRONIC WARFARE OPERATIONS COEXIST

by

John T. Arnold, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2009

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the 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 this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 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 a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **FEB 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **The Shoreline: Where Electronic Warfare and Cyberspace Meet**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air War College Air University**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**		
13. SUPPLEMENTARY NOTES **The original document contains color images.**		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**29**	

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Illustrations

Biography

Lieutenant Colonel Arnold was born in North Kingstown, Rhode Island on 19 December 1965, and graduated from Central Bucks East High School in Doylestown, Pennsylvania, in 1984. He received a Bachelor of Science in Electrical Engineering from the University of Virginia in 1988 and a Master of Science degree in Industrial Engineering from New Mexico State University in 1994. He is a graduate of Squadron Officer School, Air Command and Staff College, and Air War College.

After commissioning in 1988, Colonel Arnold was a distinguished graduate from F-111 FTU and served in the 492d Tactical Fighter Squadron, RAF Lakenheath as squadron electronic warfare officer. In June of 1992, Colonel Arnold served as operations analyst and test director for HQ Air Force Operational Test and Evaluation Center (AFOTEC), Kirtland AFB, NM.

In April 1994, Colonel Arnold returned to tactical aviation in the F-4G and flew 110 combat sorties in support of OPERATION SOUTHER WATCH. In April 1996, he transitioned to the EF-111 Raven and served as Flight Commander, Instructor EWO and, Functional Check Flight aircrew. During this time, Colonel Arnold flew 99 combat sorties in support of OPERATION NORTHER and SOUTHER WATCH. As Green Flag mission director, he led a composite wing of EW assets in support of Red Flag's first coalition EW exercise. In June of 1998, Colonel Arnold graduated with top honors from F-15E training. As 336 FS Chief of Readiness, he launched 24 aircraft in support of Operation Allied Force. He culminated his tour at Seymour-Johnson AFB as 4th FW Electronic Warfare Officer.

In December 2000, Colonel Arnold deployed to Osan AB, ROK serving as acting flight commander, 607th Combat Plans Flight, 607 Combat Plans Squadron, 7th AF. He was awarded the Field Grade Officer of the Year, 2001 for exceptional service during Ulchi-Focus Lens, the Air Force's largest joint/combined command and control exercise. In early 2003, Colonel Arnold moved to the Pentagon, Secretary of the Air Force (Acquisition) as EW Branch Chief. Leading a team of seven men and nine programs, he was responsible for $7.4B in EW research and development programs. In May 2005 he served as Director of Operations of the 36th Electronic Warfare Squadron and took command of the unit in May 2006. He is currently serving as a student at Air War College in Maxwell AFB, AL.

Col Arnold is a Master Navigator with over 1800 hours in the F-15E, EF-111A, F-4G, F-111F, and F-111D. He has served numerous tours in Air Operations Centers in CENTCOM and PACOM. His military decorations include the Meritorious Service Medal with five oak leaf clusters, The Air Medal with two oak leaf clusters, the Aerial Achievement Medal with two oak leaf clusters, the Air Force Commendation Medal, the Air Force Achievement Medal, and the Humanitarian Service Medal.

INTRODUCTION

"How did EW become part of the cyber portfolio? How did we expand the cyber portfolio beyond networks? Is cyberspace a place or a mission…" – Gen Norton A. Schwartz, 24 Aug 08

In the Department of Defense, and specifically during these trying times in the U.S. Air Force, words and their definitions are important. To this end, cyberspace has become the Air Forces' latest hot topic. Consequently, cyberspace is all over the media, being batted around within the most senior levels of the Pentagon, and has had resources thrown at it, all without a clear, nationally understood definition or concept of operations (CONOPs).

Electronic Warfare (EW) has been an enabling combat support mission for decades and on 1 Nov 2006 was subsumed into a new command (AFCYBER). "My intent [is] to redefine air power by extending… our global power into a new domain—the domain of electronics and the electromagnetic spectrum."[1] EW supports the land, air, sea, and space domains and similarly, can support operations in cyberspace. Should the classical mission set called EW, with clear doctrine and a mature legacy, fall underneath the umbrella of computers, networks, or information technologies? Many argue no. There is an area, which can be referred to as the "Shoreline", where EW and cyber can integrate to achieve synergistic effects on the battlefield.

In 1998, Information Operations (IO) was all the rage within the Air Force and before that, EW was subordinate to Command and Control Warfare (C2W), then Information Warfare (IW), and now to cyber. Entire officer and enlisted specialty codes were build, centers of excellence created, and millions of dollars spent to define and firmly establish this "new" mission type. While IO doctrine was still being drafted, EW as a whole was moved from its combat support role to become one of five pillars supporting the IO umbrella. Consequently,

[1] CSAF MFR to 8 AF/CC; Operational Cyberspace Command "Go Do" Letter; 1 Nov 06

EW resources and manpower were diverted to IO and traditional EW programs and projects declined.[2]

THE CYBER MOVEMENT

Similar to the actions taken when IO became the cornerstone of non-kinetic effects for the Air Force, during the summer of 2006 Dr. Lani Kass and her team of experts started a firestorm called cyberspace. Her efforts, backed by the Chief of Staff of the USAF, proposed the idea that operations with and through electronics and the electromagnetic spectrum occur in a very real and physical domain that exists across and connects the air, land, sea, and space domains.[3]

How EW became a part of the cyber portfolio is partially due to shared physical characteristics.

> "There is no organization or service capability in place with the express mission and responsibility to engage the adversary to ensure the sovereign ability to continuously operate and maneuver as required in and through the electromagnetic domain. This demands a consolidated electronic combat capability for the Joint Force and the Joint Force Commander. In this strategy, EW advances beyond using electro-magnetic energy to protect platforms or to project Radio Frequency (RF) energy against an adversary."[4]

Since the idea of forming an Air Force Cyber Command (AFCYBER), and more recently, a cyber Numbered Air Force (NAF) under Air Force Space Command (AFSPC), there have been misperceptions and confusion about cyberspace operations and apparently competing doctrines like IO. Cyberwar, cyber-craft, and cyber capabilities are inherently network-centric. "Resistance to the concept of cyber warfare seems to come from the misunderstanding of

[2] Lt Col Joseph Badalis e-mail; (HQ ACC/A8Z); 2 Oct 08
[3] Cyberspace Defined article, Lt Col David Fahrenkrug; Oct 2007
[4] AFRL e-mail; 24 Sept 08

cyberspace as a domain rather than an operation."[5] EW uses the electromagnetic spectrum to warn or defend as do specific computer-network operations. Since networks are created through the use of the electromagnetic spectrum, many activities in cyberspace are considered EW.[6] EW and cyber share many characteristics that, when used in concert, become a force multiplying enabler.

As the cyber movement gained momentum in 2006, the Air Force was moving with great speed to embrace this new concept. The publication of the classified *National Military Strategy for Cyberspace Operations* combined with Secretary Wynne's and General Mosley's establishment of AFCYBER (P) set the gears in motion for the service to become the Department of Defense's premier center for cyberspace capabilities. This is reflected in the earliest version of AFCYBER (P)'s mission statement: "To provide combat ready forces trained and equipped to conduct sustained combat operations through the electromagnetic spectrum and fully integrate these operations with air and space operations."

Many would argue and physical evidence supports that to fully integrate operations in and through the electromagnetic spectrum (from direct current to gamma rays) is an impossible task. This remains Gen William T. Lord's vision of AFCYBER to create a virtual command… to effect operations across the spectrum of conflict. [7] This is a lofty goal in such a fiscally constrained military climate. Words from the Joint EW Center make this point even more clear: "It is simply not realistic in practical terms to expect that we can dominate the spectrum, completely denying Red Force access to the entire spectrum at all times across an entire theater and simultaneously providing Blue Forces with free access across the Spectrum (in the presence

[5] Cyberspace Defined article; Lt Col David Fahrenkrug
[6] Ibid
[7] Strategic Studies Quarterly; Vol. 2, No. 3; Fall 2008; pg 13

of Red Force EA, congestion from White users and managing electromagnetic interference from Blue Forces."[8]

EW AND CYBER DEFINITIONS AND DOCTRINE

The Department of Defense's definition of cyberspace, not to be confused with cyber capabilities (to be discussed later), is a "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[9] To continue to muddy the waters, AFDD 2.5 (11 Jan 05) defines IO as those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare and information warfare and are conducted throughout all phases of an operation and across the range of military operations. Here we see definitions and doctrine crossing lines and blurring responsibilities once considered EW operations.

Gen Robert J. Elder, 8th Air Force Commander, was recently quoted calling cyberspace a part of a larger Air Force effort to gain the upper hand in network conflict. Upcoming Air Force doctrine calls for the service to have the freedom to attack online. New research efforts aim to gain access to any and all computers with a new division of information warriors under Air Force Space Command.[10] Air Force leadership charged with creating this new command make no mention of EW or the electromagnetic spectrum here. Cyber's net-centric doctrine is changing as quickly as the technology will allow.

[8] JED; Vol 31, No. 9 Sept 2008; Pg 32
[9] National Military Strategy for Cyberspace Operations; Sep 2006
[10] Wired Magazine; Vol. 42; Nov 2008

How EW operations became a subset of the cyber portfolio remains a matter of perspective. EW is an operational element of information operations. Additionally, influence operations and computer network operations (also known as network warfare operations) contribute to the integrated air, space, and land Operational Plans using information tactics to disrupt, corrupt, or change targeted human and automated decision making.[11] One level deeper in detail we learn from the latest version of the *Information Operations CONOPs* that EW operations are defined as military capabilities to achieve desired effects across the electromagnetic targeting domain.[12] EW uses Electronic Attack (EA or denial operations), Electronic Support (ES or exploitations operations), and Electronic Protect (EP or defensive operations) to achieve these effects. The lines of responsibility start to cross as stakeholders modify definitions and update doctrine. For example, Joint Publication 3-13 (13 Feb 06) expands EW operations and planning from traditional EA, ES, and EP (as well as Suppression of Enemy Air Defenses, SEAD) to effect operation-level measures of effectiveness, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), as well as including the complete electromagnetic energy spectrum. The publication goes on to ask military planners to consider EW's enabling effects on both open and closed electromagnetic environments.

According to an Air Force recognized cyber expert at AFRL, the main two reasons EW were included in the cyber portfolio was initially a resource grab to build a viable new command and the desperate need for a "Billy Mitchell moment"—something cyber operations needed which was an offensive effect that EW could deliver.[13]

[11] Influence Operations CONOPs; pg 2
[12] Ibid
[13] AFRL e-mail; 1 Oct 08

> *"Today, wars are of Intelligence, electronic warfare, and command & control… modern war can be won by information and that is now vital…"–Soviet Lt Gen S. Bogdanov*

SIMILARITIES THAT EW SHARES WITH CYBER

Just as EW supports IO, it can and should support cyber activities. The ever increasing pace of network technologies needs to be analyzed with respect to its relationship with traditional EW. Specifically, what mission types and enabling factors can coexist on the Shoreline: the area where EW and Cyber can mutually support the warfighter at the operational and tactical level of war? EW capabilities include directed energy, decoys, and Radio-Frequency (RF) jamming to deny, disrupt, or deceive an adversary's electromagnetic capability.[14] To be effective, EW planning and operations are dependent on accurate electronic support information and intelligence. Cyber planning and operations have the same information requirement. This small but significant requirement will form the basis of my conclusion discussed below. Doctrinally, here we see mutually supportive mission types that cross both boundaries. What was once called EW now has a more "social" definition where information technologies and EW operations enable decision making at the operational and tactical level for threat targeting, threat avoidance, or defensive measures. Unless this evolution of the definition of EW continues and EW assets are labeled as cyber capabilities, then a Venn diagram of EW and cyber will share a portion of overlap. This will also be discussed later in more detail as the "Shoreline area" where EW and cyber integrate.

[14] Influence Operations CONOPs; pg 11

According to the Department of Computer Science and Defense Analysis at the Naval Post Graduate School, cyberwar (defined as a cyberspace capability) is directed at information systems by means of software.[15] Similarly, traditional EA can be directed at information systems like early warning or acquisition radars using software (called mission data; see AFI 10-703) to create a desired effect. Cyber can use software (which can include malware, viruses, worms etc.) to have an effect on networks, computer servers, or automated information systems.

Additionally, the US Navy's new CYBERFORCOM *Talking Points* present linkages of EW activities with cyberspace. "Although we've been operating in cyberspace for a very long time—since the invention of telegraph, radio, and radar [classical EW target sets]—we now conduct the full range of military operations in this domain. This includes all energy that flows through commercial radio waves, micro-waves, and directed energy [new EW target sets]. If an electronic system emits, transmits or reflects, it's operating in cyberspace."[16] As a nation, we are more vulnerable in cyberspace than any other country because of its ubiquity.[17]

Furthermore, we learn from AFDD 2-5 that information warfare activities that fit comfortably into both cyber operations and EW operations is the enabling capability called military deception. A traditional form of EW used in tactical EA aircraft is synchronized false target jamming. This technique creates very realistic false targets and confusion by matching the jamming to the targeted radars electronic parameters or characteristics usually injected into the back lobes or side lobes of an adversary's air defense systems. The advanced jamming can pass through automated electronic countermeasures or filters and creates authentic looking targets that are not real (misinformation). Cyber capabilities exhibit some of the same traits with respect to military deception. The Defense Information Systems branch at the Naval Post Graduate School

[15] Defense of Information System: Analogies from Conventional Warfare; NPS Paper; Mar 2005
[16] Naval Network Warfare Command Renaming Communications Plan; LCDR Doug Gabos; Oct 2008
[17] Defense of Information System: Analogies from Conventional Warfare; NPS Paper; Mar 2005

is developing "software decoys" as a platform for implementing deceptive defensive tactics. The decoys are software modules that behave like normal software components but can recognize attack-like behavior and respond deceptively to it. Examples that have been explored to date include false error messages, deliberate delays, and the imposition of distracting tasks on the attacker.[18] The U.S. military depends on the Internet and since there are millions of computers and networks to protect, deception will be an important mission (both offensively and defensively) for the Air Force in cyberspace.

Like specialized jamming capabilities, deception in cyberspace can put an adversary in a position of weakness or confusion. There is military value to the practice of deception in both mission areas. Dr. Rowe and Dr. Rothstein, also from the Naval Post Graduate School, have been researching this very topic. First, deception in cyberspace increases one's freedom of action to carry out tasks by diverting the opponent's attention away from the real action being taken. Second, deceptive tactics may persuade an opponent to take a course of action that is to his disadvantage. Third, deception can create the element of surprise. Finally, deception can preserve resources.[19]

Another area of the shoreline where EW and cyber coexist is in the area of influence operations. This ties doctrinally into both information operations and military deception. Col Richard Szafranski (USAF retired) defines information as "Any difference that makes a difference." Therefore, attacking information systems at a much larger and integrated effort can be labeled netwar in cyber war. Linking multiple EW and cyber capabilities in a unique manner can create quite an enabling effect. For example, if an agency was created that combined offensive jamming with the complete tool kit of a modern network operations center and added a

[18] Defense of Information System: Analogies from Conventional Warfare; NPS Paper; Mar 2005
[19] Ibid

small subset of influence operations, it would generate a significant capability to affect many aspects of the battle space.

This agency would generate effects, expressed by Maj George Orr who wrote *Combat Operations C3I: Fundamentals and Interactions*, that would interrupt or destroy the communication between people and their equipment in all types of networked systems resulting in chaos and failure. With respect to the military arena, when commanders are unable to communicate, their decisions within the realm of combat become unstable. This idea has great significance with regard to how the command element should consider the effect of influence at the personal, public and executive levels during conflict.

Regardless of how much a commander studies theory or understands the adaptation of Col John Boyd's OODA loop to get into the mind of the enemy, personnel may fail to be able to act during combat or the stresses during combat training. This happened during Ulchi Focus Lens, the Air Forces largest command and control exercise conducted in PACAF. The Integrated Tasking Order (ITO) must be complete and distributed to all combat units by 1800 hours each day. Every tactical level commander was well very sharp, each with a cool and calm demeanor. After just one day of the exercise in full swing, the network links were cut and everyone from up and down the 7th Air Force chain stopped working; they were completely overwhelmed and unable to finish the war exercise (normally a ten day event).[20]

The ultimate aim of this agency would focus on attacks on the mind of the enemy commander and render him powerless through disorganization or confusion. This is the precise effect that takes place in the orientation piece of the OODA loop. Once intelligence gathers certain cultural, emotional (value), and intellectual information, one can use this to move an adversary to a position that creates doubt or confusion. Through the controlled use of

[20] Ulchi Focus Lens outbrief; Osan AB; Feb 2002

information, this agency will be able to disrupt the orientation process of an adversary, thus moving him in to a position of disadvantage.

As technology and information is passed on and through the modern battle space, opportunities will arrive with shorter and shorter time to react that can be used to affect an adversary. Consequently, the enemy could inject overwhelming or just barely noticeable packages of misinformation at certain levels to create devastating effects. Again, focusing on John Boyd's orientation piece of the OODA loop; to affect the cognitive realm of an adversary, this agency would be able to psychologically attack an opponent and achieve victory without actual fighting.

> *"Never in history have so many people found themselves intimately tied to—cyberspace—that is limited only be the human imagination." –Lt Col David A. Umphress, USAFR*

DIFFERENCES OF EW AND CYBER

As Gen Elder noted in his Global Cyber Operations briefing at the First Annual Cyber Symposium, cyber capabilities included efforts that overload information servers (denial of service), data loss or manipulation, or destruction of information system integrity. Here we see again the net-centric identity of cyberspace. Although wireless networks can be affected by operations in the electromagnetic spectrum, the preponderance of information networks and associated computer equipment fall outside of traditional EW target sets.

Similarly, Gen Elder's cyber "Digital Attack Defense Initiatives" include application code vulnerability analysis, centralized system configuration management, software diversity, database clustering, cyber side-arms or self-defensive tools, and cyber armor or system hardening to describe areas of focus for the Air Force with respect to cyber. None of these “core” initiatives come close to the latest doctrine or definition of EW. Air Force doctrine states that EW creates effects across the range of the IO operating environment. Consequently, cyber or networks operations are focused on the information domain, which is composed of a dynamic combination of hardware, software, and data components.[21]

Additionally, cyber capabilities are directed to achieve desired effects across the analog and digital network portion of the battle space. Networks are defined as any collection of systems that transmit or store information.[22] Doctrinal examples of networks include digital track files, telecommunications, and information systems. The difference between cyber and EW are clear, each enable the warfighter the capability to operate in the revolution in military affairs known as the information age. The figure below lists threats to information warfare and only three are traditional EW: Military Deception, RF Jamming, and Directed Energy Weapons.[23]

Information Warfare Threats			
Compromise	**Deception/ Corruption**	**Denial/ Loss**	**Destruction**
Malicious Code System Intrusion Psychological Ops Intel Collection Technology Transfer Software Bugs	Malicious Code System Intrusion Military Deception Spoofing Imitation	Malicious Code System Intrusion Lasers Physical Attack Nuclear & Non-nuclear EMP Virus Insertion System Overload Radio Frequency Jamming	Bombs Directed Energy Weapons Lasers Physical Attack Nuclear & Non-nuclear EMP Chemical/ Biological Warfare

Figure 1 (AFDD 2-5)

[21] AFDD 2-5; pg 3
[22] Ibid; pg 5
[23] Ibid; pg 6

While the Chief of Staff directed a cyber command back in 2006, his vision was to many "a bridge too far." He directed the integration and consolidation of all command and control functions, EW, Network operations, Intelligence, Surveillance, and Reconnaissance (ISR) across the spectrum of conflict. Ultimately, the Chief ordered the development of the capability to produce cyber strikes that could produce full-scale global effects.[24] Understandably, the aim is to provide the warfighter with more capability however, an order of this magnitude would take the resources of an entire new service. Specifically, combining command and control units into one agency or command is militarily unsound. Attempting to integrate all ISR missions is logistically impossible and financially devastating. Consequently, the DoD recently released the latest approved cyberspace definition which down scopes and refines cyber operations to its computer and net-centric area of military effect. "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[25] Similarly, Secretary Wynne in his *Letter to Airman* (dated 7 May 07), asked all to ensure the freedom of action across the electromagnetic spectrum which would allow us to operate freely in all other domains. To operate across the entire spectrum is not only physically impossible but, is too contested to completely dominate this domain. To their credit, in many ways the Chief and the Secretary are like Gen Billy Mitchell; both staunch advocates for the latest in technology to advance the ideals and capability of the U. S. Air Force regardless of any obstacles.

Another clear distinction where EW and cyber diverge comes from the AFCYBER CONOPs. Here we read that the scope of cyber capabilities involves effects across the entire

[24] CSAF MFR to 8 AF/CC; Operational Cyberspace Command "Go Do" Letter; 1 Nov 06
[25] Action Memo from Gen James E. Cartwright; Definition of Cyberspace Operation; 29 Sept 08

electromagnetic spectrum but, then quickly limits cyber operations to include only Internet Protocol (IP) based networks and computers, control systems (SCADA devices), and data links.[26] In this document, cyber appears to include many traditional Air Force missions that have no relation to cyber. Offensive counter cyber operations are targeted at an adversary's cyber capability but, cites EA and EW as examples; they are distinct yet supportive enabling capabilities. To define cyber operations with a clearly EW mission type is academically unsound and confusing to the individual trying to execute the CONOPs. The document goes on to mention interdiction, close cyber support (synonymous with close air support), and state that offensive cyber operations will deny an enemy access to the electromagnetic spectrum. Arguably, this concept and its supporting mission types need to be refined and better articulated.

To consider EW as a physical layer component of cyber operations is simple and appealing. What it misses are those aspects of cyber that are neither EW nor network operations, such as computer security, software/hardware protection, information assurance (albeit a supporting capability of IO), and trust.

It is understandable why the AFCYBER proponents insisted on including EW into cyber operations with our current budget situation. What gets difficult to understand is the expanse of cyberspace itself. Cyber-power is delivered through the effective mastery of three principal elements: the science of electro-magnetism, the technology of electronics, and the infrastructure which may include the interdependent network of information technology. This replicates the trinity of air power articulated by Gen Hap Arnold as he advanced air power: air as the domain, airplane as the technology, and navigation as the infrastructure. Our cyber forefather's intent was to deny all adversaries electromagnetic awareness, transportability, maneuverability, or

[26] AFCYBER CONOPs; Version 4; 21 Dec 06; pg 6

effects-generating capability and is a grand vision but, pragmatically very difficult.[27] Because the Air Force hasn't completely resolved what or if AFCYBER will look like, Gen Norton Schwartz has put a halt to further activities relating to the establishment of this new command. Announced as the "Strategic Pause", the Air Force is rethinking all cyber requirements to better synchronize with other key Air Force mission areas (read EW).

Another area where EW and cyber differ is how information and control are passed using the Seven Layers of the Open Source Interconnection Model (see figure 2). This model defines a networking framework for implementing information sharing protocols in seven layers. Users working on the network pass control from one layer to the next starting with the application layer, proceeding down the stack over a communication channel and then back up the stack to the end user or recipient. The application layer supports end-user processes and provides application services for the transfer of information on a net. The next layer down is the presentation layer which provides independence from differences in data representation or encryption. Here information is put into the correct format for the application layer to accept. Below this is the fifth layer or session layer. This is where connections are established, managed, and terminated between applications. Layers four through two concentrate on the transportation of data, creating virtual circuits, and encoding/decoding of data into digital bits. So far the model has dealt only with information handling. The lowest and last layer, the level where EW can target, is the physical layer. This level provides the hardware means of sending and receiving data on a network. Physical layer components can be jammed or disrupted using modern EW techniques like Digital Radio Frequency Modulation (DRFM) jamming, high power microwaves, or directed energy (High energy lasers). Targeting the physical infrastructure of the network stack will undermine the upper layers. In contrast, cyber operations target layer two

[27] AFRL email; 23 Sept 08

(data links) and above. The seven layer model creates a graphical or hierarchical image to better understand the difference in target sets if considering an effect using traditional EW vice cyber operations.

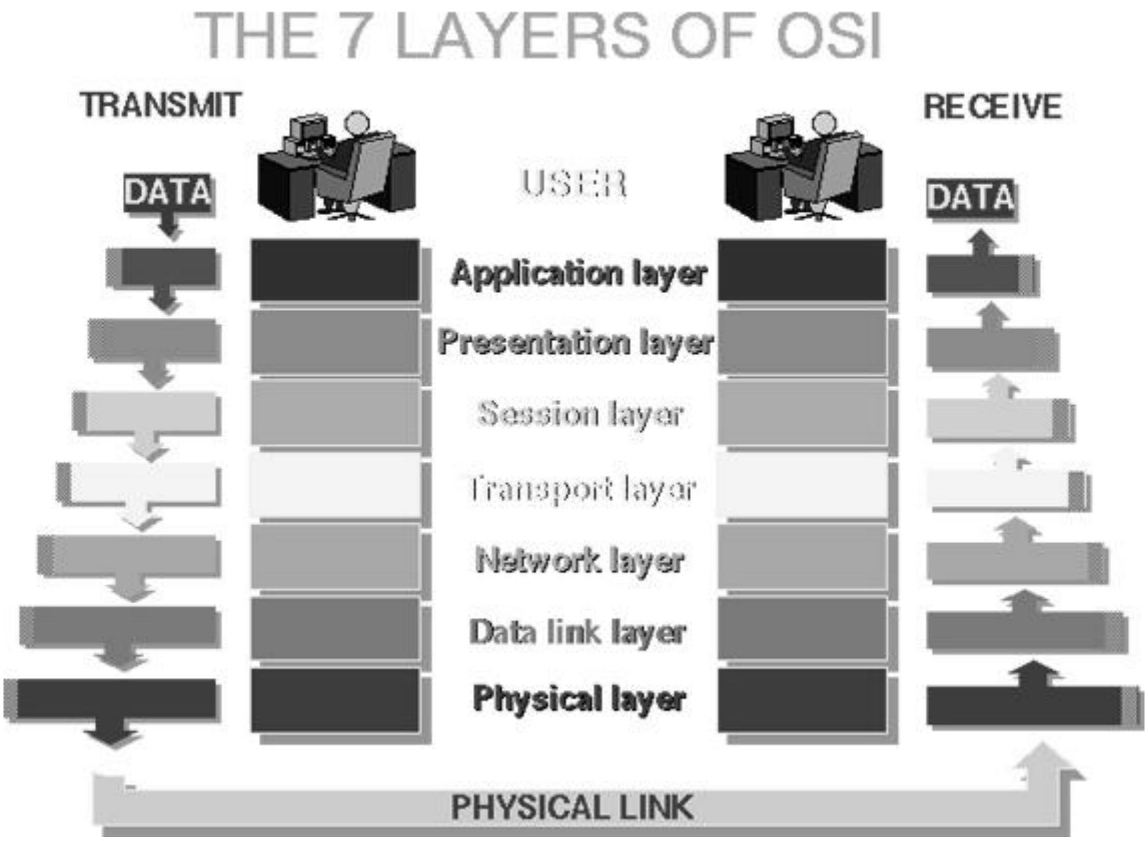

Figure 2 (Image from *The Abdus Salam International Centre for Theoretical Physics*)

The September 2008 volume of *The Journal of Electronic Defense* suggests the combination of computer network operations and EW equals cyber capabilities. Lt Col Jesse Bourque, Director of Operations of the Joint EW Center, is very clear on the boundaries of EW and cyber. "The electromagnetic spectrum is not part of cyberspace (except in very small portions) and, more specifically, EW should not form any part of Cyber command." He continues, control of the electromagnetic spectrum is a requirement for achieving military objectives. With the ever increasing demands in this warfighting domain, many agree with Lt Col Bourque's assessment that a quick resource grab of EW into a broad cyber CONOPs has serious and detrimental ramifications for EW. "It is time to reject this broad definition of cyberspace [as originally directed by the Joint Chiefs of Staff] and restore the accepted definition that cyberspace describes information technology infrastructures."[28] It is also understood that EW is in the midst of serious change, well beyond its humble beginnings of chaff, flares, and RF detection. There is no doubt that new technology and weapons are expanding into and overlapping the domain where EW traditionally applied.

Lt Col Bourque's clear delineation between cyber and EW hits at the root of the two peer yet distinct mission areas. "Within the Joint services, EW will need to remain an articulated mission area to exercise the care and protection of the [electromagnetic] spectrum, and not be assimilated by a new mission area like cyber. To contrast, tactical EW is a form of non-kinetic fires, which is about denying, degrading, disrupting, or destroying any and all adversary EM-susceptible networks or relevant parts of the spectrum [radars, SCADA systems, etc.]. Cyber can hit many of these networks… but, EW is a very mature mission area that can make targeted apertures of them all."[29] Strategically, operationally, and tactically EW and cyber can share the spectrum to deliver desired effects across the battle space. "Just because EW and CNO can and do collaborate, it does not mean they need to be collaborated within the same cyber organization where they will compete for budget and resources. Simply put, EW supports cyber the same way

[28] JED; Vol. 31; No. 9; Sep 08; Pg 6
[29] JED; Vol. 31, No. 9; Sep 08; Pg 34

it support the [air, land, space, and sea] domains—by providing spectrum control. EW, that is the broad and enduring requirement for spectrum control, is not part of cyber."[30]

Two clear yet dissimilar definitions of EW and cyber come from the very highest levels inside the National Capital Region. "Cyberspace means the interdependent network of information technology infrastructures and includes the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries."[31] Furthermore, "Operations in cyber space are digitally-based operations designed to attack, defend, exploit and maintain cyberspace and the data within it. Other military operations (such as EW, PSYOP, physical attack, etc.) may create effects in or through cyberspace but, are not operations in cyberspace per se, merely due to their use of the domain."[32]

A final example professing the difference between cyber and EW is the three tiered triangle domain model, see figure 2.

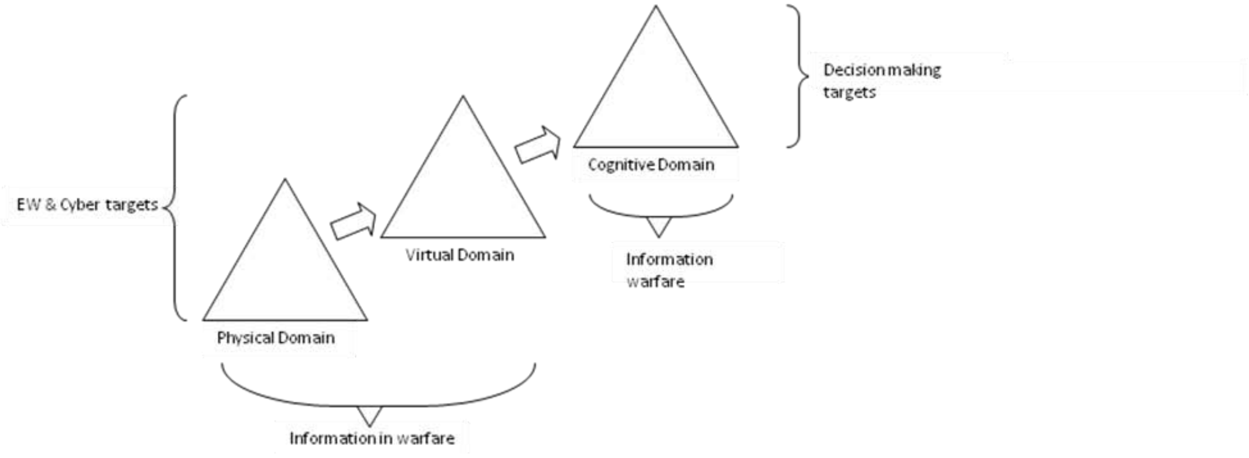

Figure 3 (Gen Elder's AFCYBER brief, n.d.)

[30] Ibid
[31] National Security Policy Directive 54, 2006
[32] Principal Undersecretary of Defense definition; 2007

The lowest level is the physical domain where the infrastructure resides. Computers, networks, and cables establish the hardware that information control and transmission can occur. The next level up is the virtual domain where data is stored, managed, and processed to "handle" information. These two domains, by the very nature of the physical characteristics create opportunities for both EW and cyber to exploit. Also within these two domains a potential adversary can wage information in warfare operations. Said another way, the information itself is the target set where data manipulation and information loss can create very desirable military effects. Lastly, and most importantly, is the cognitive domain. This is where information becomes knowledge, where command and control is executed, and the human or social aspect of information warfare can be applied. Of note, the cognitive domain is usually considered above the target set of cyber or EW operations. However, here is another opportunity to examine the concept of trust and reliability with respect to our information systems. As mentioned, EW can generate misinformation effects at the cognitive level which could influence an adversary and place him in a position of disadvantage. The influence agency mentioned above would focus their efforts on this target set.

> *"IO should be separated into three areas: manipulation of public perception, computer network attack, and electronic warfare. Only the latter should be assigned to the warfighter." – Gen Hal Hornberg, 3 Mar 03*

CONCLUSION: THE SHORLINE: WHERE EW AND CYBER COEXIST

From differences in definitions, doctrine, and information user models to similarities between EW and cyber; the shoreline between the two mission types clearly exists. Either recognized as a customer, peer capability, or operation passing through, EW shares one area of overlap or shoreline: acquisition of critical and pertinent information.

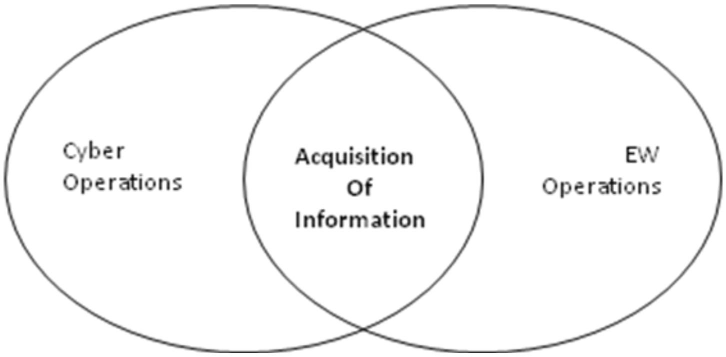

Figure 4 (Cyber/EW Venn Diagram)

Acquisition of accurate information (i.e. Intelligence) is a necessity to successfully execute either EW or cyber missions. Without the right information at the right time would spell disaster for either mission task. It is imperative for cyber and EW to acquire information, in the proper format and context, to be effective regardless of the conflict or crisis. Acquiring this information will take active steps to seek out and collect as well as ensuring defenses are fortified to prevent a potential adversary from doing the same. “The solder-operator behind a computer monitor (cyber) or radar screen (EW) is usually the front line of defense in the battle to detect and understand electronic intent. Electronic intent is easy to mask, as skilled computer programmers and [double-digit SAM operators] are demonstrating.”[33] Acquisition of information is key to seizing command of the cyber and electromagnetic high ground.

To produce combined power in cyberspace, EW and computer network operations need to effectively integrate to disrupt an adversary’s information system while protecting our own, with the objective of gaining information superiority. Net-centric

[33] Cyber Silhouettes; pg 204

operations disrupt the processing and use of information while EW disrupts the acquisition and forwarding of information.[34] The focus of cyber is to acquire precise information to manipulate information sharing (as mentioned above in the 7 Layer OSI Model). Acquiring the Intelligence information of a networked air defense system would allow EW to deny or degrade radars and communications to take control of a specific battle field situation. This combined with an offensive cyber attack would substantially increase the combat effectiveness of an operation.

An example of this is the Chinese concept of IO. Their efforts would focus on controlling the flow of information (after they've acquired Intelligence and access) in both the electromagnetic sphere and cyberspace. A successful Chinese EW and cyber operation would manipulate information processing while disrupting command and control capability.[35]

It is not surprising that both EW and cyber have acquisition "systems" to focus operators on approaching threats. For traditional EW, the Russians use many variants like the P-35 Barlock acquisition radar for the SA-5 or the 76N6 Clam Shell acquisition radar for the SA-10. The US Army uses the EQ-36 Counterfire Target acquisition radar and the U.S. and German Air Forces use the AN/TPS-117 acquisition radar for base defense. Similarly, cyber sensing payloads (cybercraft) exist to monitor data traffic that looks for unusual patterns or signals that match signatures on the network. Other active cybercraft gather timely information about its local environment and integrates this information with time synchronized data to build a complete picture of the digital

[34] Ibid; pg 91
[35] Ibid; pg 92

environment. There are many tools and physical systems that EW and Cyber share to acquire critical and timely Intelligence.

EW and cyber operations need to be able to operate at the tactical, operational, and strategic levels both for offensive and defensive activities. EW and cyber require very detailed and specific information to protect information and information systems. This will allow operations by ensuring availability, integrity and confidentiality; in short, information assurance.[36] Offensively, acquiring delicate information would allow operations that would permit cyber and EW to target telecommunications, electrical power grids, banking, transportation, and a host of military links, nodes, and apertures. These two mission types provide offensive and defensive capabilities, with the right information, to the warfighter.

The shoreline between EW and cyberspace is the acquisition of specific, timely, and reliable Intelligence. EW and cyber capabilities are expanding and warfighters are now required to address a wealth of new aspects of a revolutionary complex and contested arena. Operation in cyberspace and in traditional EW mission areas is becoming an unconstrained global interaction of humans and machines. This develops relationships where data, information, and cognition are created and exchanged.[37] With the acquisition of critical information, EW and cyber can create effects where information and knowledge can be misrepresented, compromised, denied or destroyed to gain military advantage.

[36] Information Operations CONOPs; Pg 72

[37] Office of Naval Research; Broad agency Announcement No. 09-002; 27 Oct 2008

SUMMARY

It is only a matter of time before the Air Force develops the CONOPs and definitions for cyber as it matures within the service. Regardless of who “owns” EW or cyber in the future, these combat enablers will continue to support the warfighter for any and all conflicts. Gathering timely Intelligence that results in actionable information for commanders will determine victory or failure on the battlefield, over networks, or in cyberspace. Information dominance is possessed by no single nation-state or individual. The collective enabling effects of cyber and EW will shift the balance of power to the one who understands the need for and control of the “right” information.

Bibliography

Articles

Alexander, Keith B., Lieutenant General. “Warfighting in Cyberspace”. *Joint Forces Quarterly* iss 46 (3d Qtr 2007)

Borque, Jesse “Judge”, Lt Col. “A (Pragmatic) Future of Joint Electronic Warfare”. *IO Sphere.* Summer 2008

Fahrenkrug, David T., Lt Col. “Cyberspace Defined”. Air University Press. Reprinted 27 Aug 2008

Szafranski, Richard, Col. “A Theory of Information Warfare: Preparing for 2020”. *Air Power Journal* (Spring 1995)

Umphress, David A., Lt Col. “Cyberspace: The New Air and Space?”. *Pireps* vol 55 no 4 (2007)

Books

Armistead, Leigh. *Information Operations: Warfare and the Hard Reality of Soft Power*. Dulles Virginia: Brassey’s Inc, 2004

Thomas, Timothy L., Cyber Silhouettes: Shadows Over Information Operations. Foreign Military Studies Office. Fort Leavenworth, Kansas, 2005

Periodicals

Bourque, Jesse “Judge”, Lt Col. “Why EW is not Part of Cyberspace”. *Journal of Electronic Defense* vol 31 no 9 (Sept 2008)

Lord, William T., Major General. “USAF Cyberspace Command: To Fly and Fight in Cyberspace”. *Strategic Studies Quarterly* vol. 2 no 3 (Fall 2008)

Personal Communications – Interviews/E-Mails

Badalis, Joseph V., Lt Col. Email. 2 Oct 2008

Caudle, Daryl L., CAPT, Email. 7 Oct 2008

Elder, Robert J., Major General. Email. 19 Oct 2008

Jabbour, Kamal T., Dr. Email. 23 Sep 2008

Schwarz, Norton A., General. Email. 24 Aug 2008

Briefings/White Papers/Messages

7 Layers of the OSI Model. Abdus Salam International Centre for Theoretical Physics. 3 Mar 2008

Elder, Robert J., “Briefing: Air Force Global Cyber Ops”. 1st Annual Cyber Symposium. 28 Nov 2007

Lord, William T., “Briefing: CAF/MAF AFCYBER Command Status Update.” 27 Jul 2008

Kass, Lani, Dr. “Briefing: A Warfighting Domain”. 26 Sep 2006

Moseley, T. Michael. CSAF White Paper. “The Nation’s Guardians America’s 21st Century Air Force. 29 Dec 2007

Rowe, Neil C., “Defense of Information Systems: Analogies from Conventional Warfare”. Departments of Computer Science and Defense Analysis. U.S. Naval Post Graduate School. Reprinted 22 Sept 2008

Government Documents

Air Force CONOPS for Influence Operations, (Draft), 2005

Air Force CONOPS for Information Operations, 6 Feb 2004

Air Force CONOPs for Cyber, ver 4.0. 21 Dec 2006

Air Force Doctrine Document 2-5, *Electronic Warfare*, 2005

Cartwright, James E., General. Action Memo: Definition of Cyberspace Operations. 29 Sep 2008

Moseley, T. Michael, General. Memo for Record. *Operational Cyberspace Command “Go Do” Letter*. 1 Nov 2006

Naval Network Warfare Command: Command Renaming Communications Plan. (Draft) 3 Oct 2008