AIR WAR COLLEGE

AIR UNIVERSITY

WARFARE IN THE ELECTROMAGNETIC SPECTRUM AND CYBERSPACE: UNITED STATES AIR FORCE CYBER/ELECTROMAGNETIC WARFARE COMMAND CONSTRUCT

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

by

Harold T. Cole, CDR, USN

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Col Thomas D. McCarthy

13 February 2014

DISTRIBUTION A. Approved for public release: distribution unlimited.

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, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Biography

CDR Harold Cole is an active duty Navy Information Warfare Officer. A graduate of Auburn University, he has served at sea and ashore conducting cryptologic, electronic warfare and cyberspace operations missions. Tours have included Deputy Information Warfare Commander for the NIMITZ Carrier Strike Group; Information and Electronic Warfare Officer onboard USS ENTERPRISE (CVN-65); Deputy Branch Chief for Cyberspace Warfare at OPNAV N2/N6; and multiple tours with the National Security Agency in both the Signals Intelligence Directorate and Information Assurance Directorate.

CDR Cole earned a Bachelor's Degree from Auburn University and a Master's Degree in Information Assurance from Capitol College. He earned JMPE Phase 1 from the Air Command and Staff College. He is working towards a Master's Degree in National Strategic Studies from the Air War College.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Abstract

The information revolution brought significant change to the world over the past thirty years. Similarly, that same revolution continues to play a significant role is shaping military organizational structures worldwide. The primary contributors to this revolution were the exploitation of the electromagnetic spectrum (EMS) and the rapid growth of information availability made possible by rapid advances in affordable digital computing power.

This paper seeks to examine current United States Air Force organizational constructs for electronic warfare (EW) and cyberspace operations to determine their effectiveness in preparing the Air Force for conflict over the next thirty years. A brief background of the EMS and cyberspace is provided to frame the discussion to follow. The relationship between cyberspace and the EMS is explained, with perceived and actual positions of the Army, Navy and Air Force discussed to show alternative thinking within the Department of Defense. The evolution of Air Force Electronic Warfare and Cyberspace Operations are both examined to provide context and frame discussion regarding why the Air Force chose to organize in its current manner. Future threats in cyberspace and the EMS are presented to show why these two environments will continue to grow in importance over the next three decades. Finally, recommendations offered focus on improving the state of EW in the Air Force, and strengthening the organizational relationship between cyberspace and EMS operations.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Introduction

Today and looking forward into the near future, the United States military should remain the world's preeminent fighting force. The greatest challenge to that dominance seen today is the asymmetric effect rapid technological development is having on traditional United States military capabilities. Many key enablers for the United States military are at risk for the first time due to these technical advances, often developed and fielded at a fraction of the cost of the threatened weapon system. Looking to the future, United States forces should expect to fight their way into a theater of operations, likely with degraded or denied communications and intelligence support. This reality, known today as anti-access, area denial (A2/AD) presents problems that must be overcome for the United States to retain its military strength in the world.

Looking forward three decades and predicting requirements for that timeframe is an enormous challenge. The Air Force does not definitively know what the next revolutionary technology is, but it does understand technology trends as it forecasts what the Air Force of 2040 needs to maintain sensor and weapons effects at range over time. Many of these important technologies deal closely with cyberspace and the electromagnetic spectrum (EMS)[1]. One thing the Air Force can do now is to organize in a way that takes full advantage of technological development in the coming decades. This paper argues that for the United States Air Force to maintain weapons and sensor density at range in an anti-access, area denial (A2/AD) scenario, it must think and act differently regarding its operations in and through cyberspace and the electromagnetic spectrum.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Thesis

Specifically, the United States Air Force Electronic Warfare and Cyberspace Operations force structure is not optimized to meet Combatant Commander requirements, and therefore must realign under a Cyber/Electromagnetic Operations Command construct to ensure effective access to and use of cyberspace and the electromagnetic spectrum in 2040.

Background

Today's world is in the early stages of a transformational revolution centered on information. Just as the agricultural and industrial revolutions changed the course of human civilization, the information revolution is changing the way people live, businesses operate, and governments interact. Information is available today to the average person in quantities and at speeds never imagined, and the secondary effects of availability are only now beginning to be understood. The term "cyberspace" emerged as a description of the environment encompassing the systems, infrastructure, links, and software that make this new information environment possible. United States military leaders doctrinally codified cyberspace as a domain alongside the air, land, sea, and space domains, and then further defined how to operate in this domain.

Information is not the only focal point of revolutionary growth. The EMS became increasingly important with development of new technologies and scientific disciplines. The radio frequency (RF) portion of the EMS was used extensively over the past one hundred and fifty years. Military application in communications, sensing and intelligence led the increasingly important utilization of the EMS in supporting military operations in

the traditional land, air, sea and space domains. Cyberspace is the newest operational domain, yet it does not function without the EMS. Further, new discoveries in power and directed energy are driving additional uses of the EMS that were not known or not feasible just a few decades ago. The EMS, which unlike cyberspace is a naturally occurring environment, is perhaps more critical than the narrowly defined cyberspace domain to warfighters today and in the future.

Cyberspace and the EMS – How They Relate

Today's Air Force has done a good job growing a cyberspace operations capability and integrating it into modern warfighting strategy and tactics. The Air Force also historically recognized the importance of Electronic Warfare (EW) and the EMS (though not always funded accordingly), both from its tactical application in airborne combat to its necessity in communications, sensing, intelligence and space operations. What the Air Force has not done well to date is align its efforts in cyberspace operations with its electronic warfare and EMS operations missions in a way that effectively and holistically leverages the EMS and cyberspace to their greatest potential.

The Army and Navy already recognized the need for cyberspace-EMS alignment and moved forward in organizationally aligning their services' cyberspace and EMS operations. Both services also recently published roadmaps/assessments detailing how they relate, the Army in the *Army Cyber-Electromagnetic Contest Capabilities Based Assessment*, and the Navy in the *U.S. Navy Information Dominance Roadmap 2013-2028*. Both services' publications highlight a future information environment dependent on the EMS. The Navy highlights three areas – Assured C2, Battlespace Awareness, and

Integrated Fires – as focal points demanding a holistic solution in cyberspace-EMS operations.[2] Both publications also highlight convergence of cyberspace and EMS capabilities, with the Army specifically stating:

> There is overwhelming evidence of convergence, but not to the point of absorption. Technological advances are increasingly dictating the interrelatedness and interdependence of cyber and EMS capabilities in order to maximize the full potential of both. Cyber is reliant on the EMS…Our analysis indicates that future capabilities will increasingly be unified single solutions with both cyber and EW aspects.[3]

As critical partners in any joint warfighting scenario, the Army and Navy understand the need to structure their cyberspace and EMS organizations so as to holistically operate and thrive in both cyberspace and the EMS.

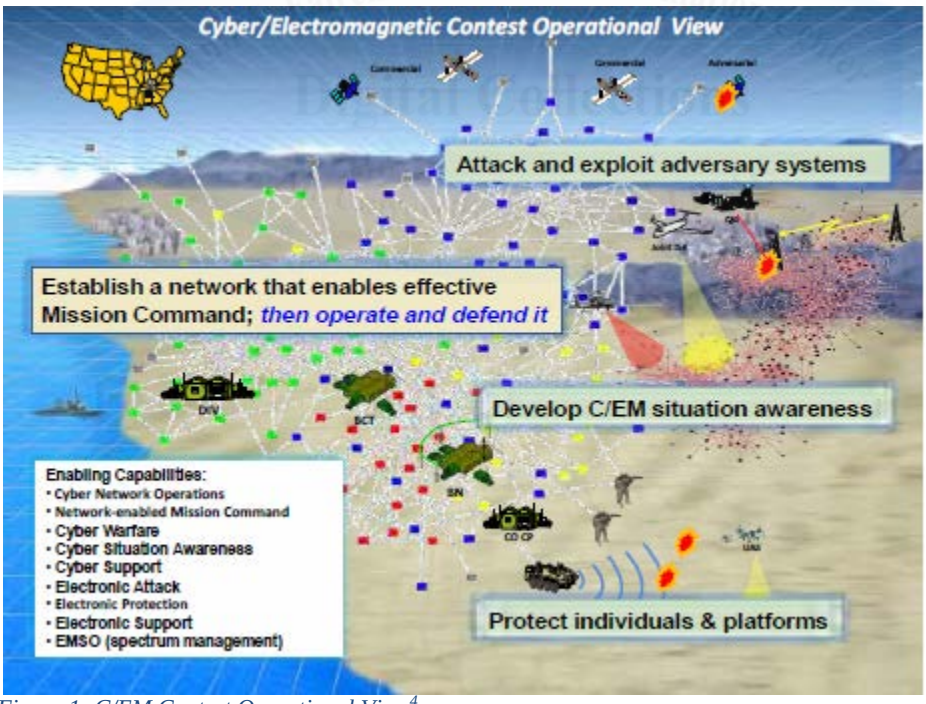

Figure 1: C/EM Contest Operational View[4]

USAF organization does not currently match what the Army and Navy are doing. A fundamental shift in thinking is necessary within the Air Force that strategically positions the service to leverage advances in both the information environment and

electromagnetic environment going forward. Today Air Force cyberspace operations forces organizationally belong to USAF Space Command. Air Force EW is not nearly as well aligned, with missions and forces scattered across Air Combat Command, Space Command, and the Air Force ISR Agency.

Throughout the Air Force, the term "cyber" is used to describe a capability or prescribe a solution. Unfortunately, the opposite appears true regarding EW and EMS operations. While there are pockets of support for EW throughout the Air Force, the synergy and excitement that exists regarding cyberspace operations is curiously absent when discussing EW. When voices are heard, it is too often comments dealing with "legacy" and "reestablishing" EW capabilities. A recent example is Lt Gen Herbert Carlisle's testimony in March 2011, to the House Armed Services Committee, Subcommittee on Readiness, when he described the USAF's future EW plans stating

> To keep our legacy platforms viable well into the future, the Air Force intends to reestablish itself as a leader in Electronic Warfare through modernization of legacy programs and increased capacity including acceleration of Active Electronically Scanned Array (AESA) radar modernization programs, electronic protect software upgrades and adding two additional EC-130H Compass Call aircraft authorizations over the FYDP.[5]

Focusing on modernizing legacy systems is not bad, but that strategy will not lead to a re-establishment of USAF primacy in EW. Lt Gen Carlisle did speak to USAF cyber capabilities in that same testimony, yet he did so in the context of traditional "support, defense and offense" in the information environment, with no mention of possible synergies in the EMS.[6]

There are detractors to joining cyberspace operations and EW/EMS Operations. Usually their concerns revolve around two ideas: either EW being absorbed into cyberspace operations, or cyberspace operations becoming part of EW or EMS operations. Lt Col Jesse Bourque, USAF, makes a strong case for separation when he states "It remains essential to the 21st-century fighting force to understand that the requirement to control the EM Spectrum extends well beyond the needs of IT management or Operations in Cyberspace."[7] Lt Col Bourque is exactly right in arguing for separation, but his argument is based on the idea of absorption. The better argument focuses on *dependency*, specifically the dependency of cyberspace operations on the EMS. In this context, the call is not to merge or join, but rather organize around the concept of cyberspace dependency on the EMS. Captain Mickey Batson and Lieutenant Commander Matthew Labert, USN, address dependency of cyberspace on the EMS in their paper describing non-kinetic warfare concepts, focused primarily on offensive cyberspace operations (OCO) and electronic attack (EA) similarities. While not calling for joining the two disciplines, they do advocate for integration, saying "The underlying physics of OCO and EA drive toward a natural convergence of capabilities."[8]

Both now and in the future, operations in the information environment will not be possible without understanding and controlling applicable portions of the electromagnetic environment. Based on its reliance on operations in the air, space, *electromagnetic* and cyberspace domains, the Air Force is well positioned physically and logically to dominate these realms when and where necessary, but it must first organize and align its forces better to enable the cohesion necessary to man, train and equip the Air Force properly for operations in these domains.

USAF Electronic Warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic Warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support (JP 3-13.1).

While historians point to the beginning of the 20th Century and the Battle of Tsushima during the Russo-Japanese War in 1904 as the birth of electronic warfare, USAF EW history really does not begin until World War II.[9] Throughout that war, and in each conflict since, EW played a critical, though often unheralded, part in the fight. World War II demonstrated the importance of radio communications, as well as the ability to intercept, deny and deceive the enemy through electronic means. Equally important was the growth of radar, on the ground, at sea and in the air. The capability to defeat radar and communications also developed in parallel with their rise in operational use; jamming and deception being the two applications most frequently seen throughout the war. When World War II ended, kinetic fighting stopped, but electronic warfare accelerated throughout the Cold War with the Soviet Union.

From its formation in 1947, the USAF recognized EW's importance in warfare, yet it always remained a fringe capability that supported air operations. Air Force EW development continued in parallel to development of Soviet air defense systems in the 1950s and 1960s, leading into the Vietnam War and the challenges presented and overcome (with varying success) in the air domain and EMS. The Vietnam War taught the USAF a lot about operating in the air and electromagnetic environments. While airborne technologies matured with evolving engine and aerodynamic advances (including

development of stealth technologies), electromagnetic spectrum understanding and utilization moved at a much greater pace. Radar and communication advances led the race militarily, setting the stage for a post-Vietnam Air Force that was smaller but more technologically advanced, and dependent at the same time.

The early 1980's saw a resurgence in Air Force EW capabilities, largely due to recognition by leaders that the increasingly technical nature of air warfare required understanding how to operate in the EMS, as well as the ability to exploit an adversary's weaknesses in it.[10] USAF senior leaders openly discussed and wrote about the necessity to operate in, deny and exploit adversaries in the EMS. A generation of capabilities were developed and fielded after recognizing the need to keep pace with ever more sophisticated integrated air defense systems being sold by the Soviet Union around the world.[11] Unfortunately for the Air Force EW community, the early 1980s also meant a push to focus on stealth technologies. Stealth advocates promised to make aircraft "invisible" to radars, greatly reducing the need for separate active EW capabilities. This point was (and still is) widely debated, nevertheless by the early 1990s the Berlin Wall fell and the Air Force's first stealth platform, the F-117, performed even better than expected. Despite positive accolades for EW capabilities (including those used in concert with stealth aircraft) coming out of Operation Desert Storm, USAF EW stayed at the capability development fringe while stealth focused programs accelerated with the B-2, F-22 and F-35. If there is any future airborne EW capability, it will likely be packaged with the F-35. According to Lockheed Martin Vice President Stephen O'Bryan, the F-35A (USAF variant) EW capability "is as good as, or better than, [that of the] fourth generation airplanes specifically built for that purpose."[12] Accepting Mr. O'Bryan at his word (he

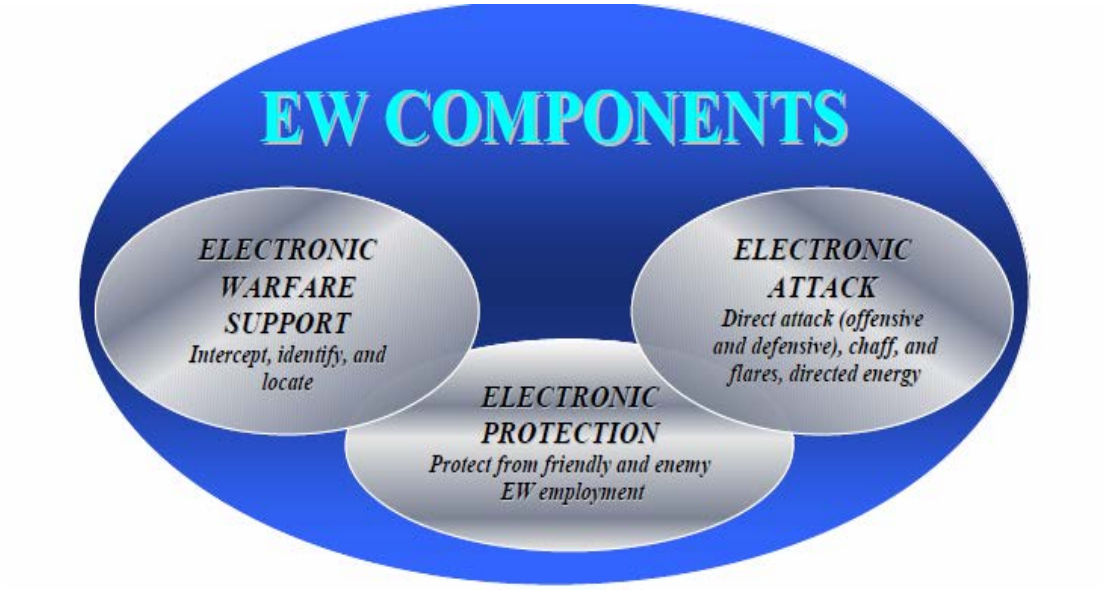

Figure 2: EW Components – from AFDD 3-13.1

was a former Navy F/A-18 pilot), even such a robust EW capability as the one described does not demonstrate that the Air Force is organizationally putting EW and EMS Operations at the front of its operational priorities. Instead, it validates the traditional thinking that EW is necessary to support air operations. Current DOD and USAF EW doctrine and definitions are codified in Joint Publication 3-13.1, and AFDD 3-13.1. These definitions, while exhaustively vetted for applicability, are ultimately viewed as a "battle for control of the electromagnetic (EM) spectrum."[13] In this context, EW becomes more than just a type of warfare. Instead, offensive, defensive and control/use aspects of the electromagnetic environment are better represented and understood operationally, similar to the current definition of cyberspace operations as it relates to the information environment.

Today, the Air Force continues to see the need for EW, yet the lack organizationally of a strong EW advocate means it will continue to struggle to fund development in an austere budget environment, let alone develop more advanced and innovative applications for

employment of force in and through the EMS. The F-35 EW capabilities are a step in the right direction, and plans to incorporate similar capabilities into the proposed Long-Range Strike Bomber (LRS-B) demonstrate an appreciation for EW as well. Recently, a senior defense aerospace industry official was quoted saying

> In the past, EW was essentially about defending a single platform…but in the future it will be all about exploiting the EM spectrum – integrated and effective across the full spectrum of operations, systems and domains… The Air Force sees the LRS-B as a central platform… to deliver both broad electronic attack as well as traditional kinetic attack.[14]

Unfortunately, it is not clear that the Air Force is *organizationally* prepared to optimally harness these capabilities and employ them in an integrated manner with their cyberspace operations capabilities.

Muir S. Fairchild Research Information Center
Digital Collections
AU University–Maxwell AFB, AL

USAF Cyberspace Operations

Cyberspace is a new term used to describe the intersection of people, technology and information. DOD went through several revisions of the definition, settling currently on the definition listed below in its recently published Joint Publication 3-12, Cyberspace Operations.

- **Cyberspace is "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." Cyberspace Operations (JP 3-12).**

In calling cyberspace a domain, DOD put it on par with the more commonly accepted domains of air, land, sea and space. While these four domains all describe something that physically exists, cyberspace is not a physically similar "place." Instead, cyberspace transcends traditional

boundaries as we know them, whether geographic, national, institutional or logical. Therefore, defining cyberspace as a domain, as DOD does, greatly limits military strategic thinking to the relatively narrow definition of a domain.[15]

- **Cyberspace Operations is "The employment of cyberspace capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace" Cyberspace Operations (JP 3-12).**

Similar to the origins of EW, cyberspace operations were secretive, behind the scenes efforts to support greater warfighting objectives in conflicts dating back to the 1980s. The USAF was much more assertive as this warfare area emerged by staking an early claim to cyberspace operations, first by including the term *cyberspace* in the Air Force mission statement in 2005, and then laying the groundwork for an operational cyberspace command structure.[16] Contemporary cyberspace operations evolved from command control and communications counter-measures (C3CM) concepts[17], Network Centric Warfare, Information Warfare and Computer Network Operations. Similar to EW, ties to the national intelligence community restricted many cyberspace operations capabilities to compartmented channels, limiting traditional warfighters' understanding of this emerging warfare environment until recently.

USAF cyberspace operations was formally established with the initial announcement by Secretary of the Air Force Michael Wynne in November 2006, and provisional activation of Air Force Cyber Command (AFCYBER) in late 2008. That decision was quickly reversed though, and instead the 24th Air Force and Air Forces Cyber was established under Air Force Space Command as the USAF cyber component to United States Cyber Command (USCYBERCOM).

One interesting omission from the final Air Force Cyber construct was that it left out the previously included missions in EW from the current organization. Regardless of the reason why EW was left out, it means that EW and other EMS operations are not viewed at the same level organizationally as cyberspace and cyberspace operations. While this alignment does not significantly affect the force presentation to USCYBERCOM (which also has no EW/EMS authorities; those are still with USSTRATCOM), it does affect how USAF cyberspace and EMS forces support geographic combatant commanders. An interconnected cyberspace AND EMS focused organization is needed to maximize the Air Force's ability to operate in both areas now and in the future.

EMS and Cyberspace Future Threats

Looking thirty years into the future, it is safe to assume that both the EMS and cyberspace will become increasingly integrated and critical to warfighting. What is not clear is what cyberspace and its dependency of the EMS will look like, nor how it will be protected or attacked. Rapid technological advancement over the last thirty years demonstrates how difficult it will be to identify specific capabilities relevant in that timeframe, yet technology trends point to broad capabilities in the following areas.

Muir S. Fairchild Research Information Center
Digital Collections
Air University – Maxwell AFB, AL

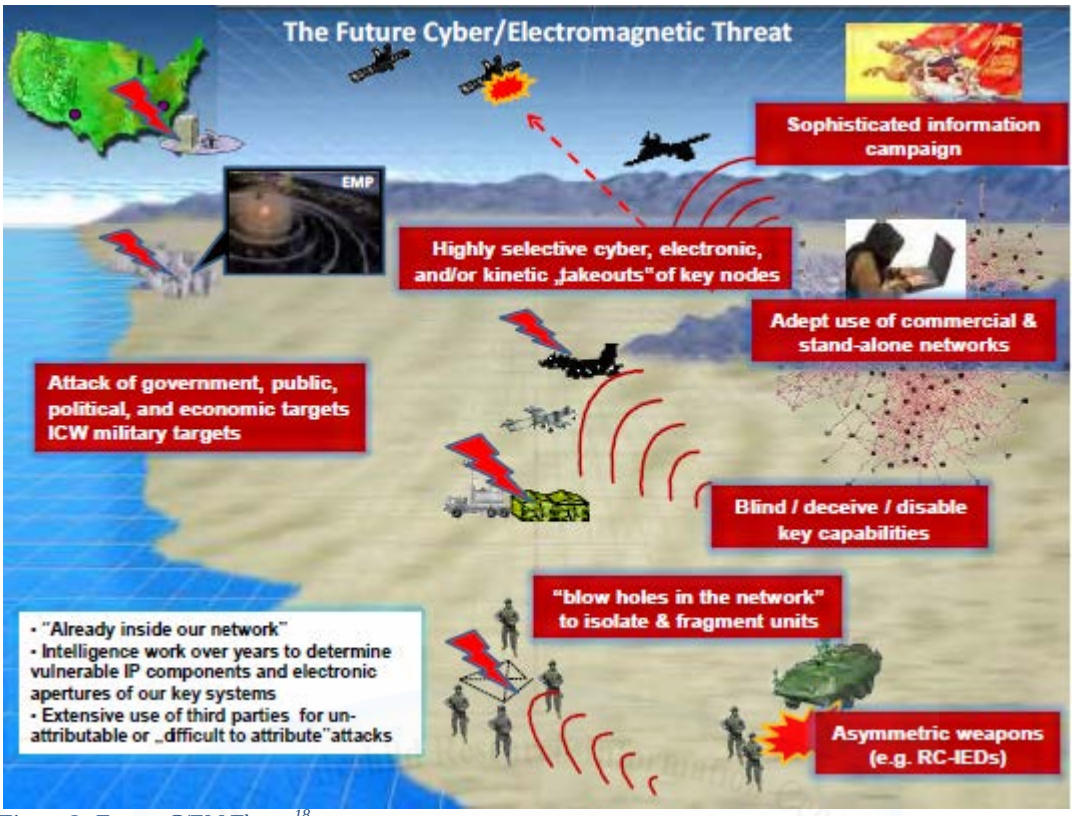

Figure 3: Future C/EM Threat[18]

Spectrum warfare and agility/maneuver in the EMS are key concepts that will continue to develop in the coming years. Based on current trends, by 2040 today's fixed frequency communications and radar systems should be replaced by systems that dynamically maneuver across EMS to achieve desired results while minimizing an adversary's ability to deny or degrade those capabilities. The coordination necessary to achieve these results will be largely autonomous within the systems themselves, yet the human operators will still need to assert some levels of control to focus on desired end goals. These future systems will blur the conventional lines between today's traditional computer networks under the purview of cyber operators and traditional radio networks administered by EMS operators.

Directed energy weapons, often discussed in science fiction yet never quite ready for operational use, will be operationally relevant by 2040. The family of technologies collectively known as directed energy weapons will begin with local defensive capabilities and eventually mature into offensive weapons. Already today, laser based point defense systems are being operationally fielded. Earlier this year, the Navy announced testing a fiber based solid-state laser capable of shooting down a UAV. This system will be deployed in the summer of 2014 operationally onboard the USS Ponce.[19] The Air Force also evaluated directed energy weapons and is actively pursuing future capabilities through the Air Force Research Lab (AFRL).

At AFRL "The Directed Energy Directorate focuses in four core technical competencies: Laser Systems, High Power Electromagnetics, Weapons Modeling and Simulation, and Directed Energy and Electro-Optics for Space Superiority."[20] The Air Force recently publicized a directed energy test of the Boeing Counter Electronics High Powered Microwave Advanced Missile Project (CHAMP). CHAMP is a cruise missile capable of releasing an electromagnetic pulse (EMP) against a target to electrically destroy unshielded electronics. This highly useful capability was highlighted by USAF Deputy Assistant Secretary (ST&E) Dr. David Walker in his testimony to the House Armed Services Committee in April 2013.[21] In the future, CHAMP-like capabilities will deliver different payloads to include cyber munitions or directed energy effects. Current USAF cyberspace and EW organizations does not holistically support this integration in development, procurement and operations however, and is another reason to align cyber and EW efforts organizationally.

Future Offensive and Defensive Cyberspace Operations capabilities will evolve from today's manually crafted computer code into much more sophisticated capabilities that will likely be written by both human and autonomous machine programmers alike. The concept of computers writing their own code might seem far-fetched, yet the basis for this concept already exists and is being researched and developed today. These concepts form the basis for self-healing networks that can recognize cyber-attacks and defend themselves, along with offensive tools that can change their code structure to avoid or defeat a network defense system. These capabilities will not exist only inside today's traditional computer networks but will be used tactically against RF based communications, radars, satellite constellations, and any additional system or network that depends on electronic input or output to function.

USAF Cyber-EM Warfare Way-Ahead

With the previous scenarios in mind, the USAF should recognize the need to prepare for future operations and conflict in and through the EMS. If the logic presented previously, that cyberspace is wholly dependent on the EMS, is accepted, then the following thoughts emerge as ways to organize and fight in and through the electromagnetic and cyberspace environment.

The most immediate problem the Air Force must address is its lack of any real vision in Electronic Warfare. As previously discussed, Air Force leadership still does not demonstrate its belief in EW as a core mission capability. Service leadership's words (recent Congressional testimony) and actions (funding for EW systems outside of the F-35 is not a priority) reflect the historic norm previously highlighted that EW is a peripheral

capability of the USAF. This is in stark contrast to the Army and Navy, which have both placed a renewed emphasis on EW capabilities.

The Army, after abandoning EW for many years, re-engaged in EW. "The Army's new EW emphasis emerged from its fight against IEDs in Iraq. But, important as that fight is, EW's importance quickly spread beyond it."[22] Spurred on by its realization of EW's importance on the modern battlefield, Army leadership implemented changes to the service that affected tactics, manning and organizational structures.[23] The stark reality of the need to operate both offensively and defensively in and through the EMS, plus the explosion of wireless RF-based C4ISR technologies that its field commanders depended on spurred the Army to organizationally wake up and understand the significance of the EMS and Cyberspace. The Army is now actively championing EW and "cyberelectromagnetic activities" in its recently published FM 3-36 Electronic Warfare,[24] and the previously mentioned Army C/EM Contest Capabilities Based Assessment.[25]

The Navy, like the Air Force, reorganized its cyber forces several years ago into an operational command structure to command and control those forces. Unlike the Air Force though, the Navy's Fleet Cyber Command / US 10th Fleet consolidates the Navy's cyber and EW missions under one operational commander. While not perfect, it does enable the Navy to organize, command, and control its cyber and electromagnetic forces from one operational command. The Chief of Naval Operations has also enthusiastically promoted cyber-electromagnetic discussion, recently personally publishing several articles on the subject, including one for AOL Defense in which he states "future conflicts will not be won simply by using the EM spectrum and cyberspace, they will be won within the EM

spectrum and cyberspace."[26] In contrast, all Air Force senior leadership language seems to focus on all the disparate parts as individual problems and not one that should be dealt with holistically. Regarding cyberspace-EMS operations convergence, the Navy placed a high level of importance on shipboard and airborne EW capabilities for the fleet that in the near future will fulfill both cyberspace and EW mission requirements, increasing funding in this area even through recent budget cuts. The CNO recognizes that his ships and aircraft cannot survive in a current or future contested theater of operations without integrated cyberspace - EW capabilities.

The greatest challenge the Air Force faces is to redefine its relationship between cyberspace and EMS operations. Though cyberspace operations is the newer of the disciplines, the momentum gained from establishing the initial AFCYBER and later the 24th Air Force**,** provides the USAF with a construct to build its Cyber-EM Warfare force around. The Air Force previously explored this option, with the initial plans for the 8th Air Force / USAFCYBER including both cyberspace operations and electronic warfare capabilities and forces.[27] Unfortunately, neither the EW mission nor forces converted to the 24th Air Force.

Currently EW organizations are nested under Air Combat Command, while the 24th Air Force has cyberspace operations, communications (deemed "cyber" by the Air Force) and Information Operations (which includes EW historically) organizations under its command. Finally, the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA) conducts both cyberspace operations and EMS Operations missions, from an intelligence collection and production perspective. In this context, current Air Force

cyberspace operations and EMS operations are aligned in three vertical stovepipes – ACC, SPACECOM and AFISRA – making integration and coordination of capabilities a bureaucratic challenge. In order to optimally address future combatant requirements in these two areas, the Air Force should look at restructuring how its EMS operations are organizationally spread across the service.

The Navy Strategic Studies Group recently completed and published its SSG XXXI report titled "EM Maneuver Warfare" which provides some useful options for the USAF to consider when looking at organization constructs for cyberspace and EMS operations. As defined by the SSG, "**EM Maneuver Warfare** uses EM energy to shape the battlespace, enhance awareness, affect the enemy's perception, and achieve decisive results."[28] The concept of maneuver in and through the EMS and cyberspace is something the Air Force is already familiar with, and it should leverage this work (USAF participated in the study) to build its own holistic cyberspace-EMS operations vision and organizational structures from these thoughts and concepts.

Conclusion

Today's Air Force goes forward without a cohesive strategy clearly organizing cyberspace and EMS operations holistically. It is apparent that the Air Force invested considerable resources into its cyberspace operations mission, and it built a robust organizational structure around the mission. Unlike cyberspace operations, missions involving EMS operations are scattered across the Air Force, with no apparent organizational glue to pull them together as with cyberspace operations. Air Force efforts in communications are critical to all the DOD, and its communications forces execute this mission well.

Additionally, directed energy research and testing continues to show promise, and the USAF is a leader in developing new capabilities that utilize the EMS. Electronic Warfare is the one piece of USAF EMS Operations that does not demonstrate the same type of forward looking vision needed in projected future conflicts to fight and operate effectively in and through the cyberspace – EMS environments. Current EW efforts in the tactical air arena are notable, but these forces are buried deep in the Air Combat Command organization, with no apparent organizational connections to the 24th Air Force's cyberspace operations organization.

When the USAF successfully aligns its cyber and EMS operations, it can expect to achieve greater effects in not just these two domains, but in every domain in which it operates.

---

[1] The EMS is defined in JP 1-02 as "The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands."
[2] United States Navy, *U.S. Navy Information Dominance Roadmap 2013-2028*, publication (2013), ii.
[3] *Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA)*, report (Fort Leavenworth, KS: Combined Arms Center - Capability Development Integration Directorate, 30 March 2011), EXSUM p.5.
[4] Ibid, 24.
[5] *Are We Ready? The President's Fiscal Year 2012 Budget Request and Global Challenges to Readiness*, House Armed Services Committee, Subcommittee on Readiness Cong., 7 (2011) (testimony of Lt Gen Herbert J. Carlisle).
[6] Ibid, 5.
[7] Bourque, Jesse. 2008. "Why EW Is Not Part Of Cyberspace." *Journal of Electronic Defense* 31, no. 9: 40.
[8] Batson, Mickey, and Labert, Matthew. 2012. "Expanding the Non-Kinetic Warfare Arsenal." *U.S. Naval Institute Proceedings* 138, no. 1: 44.
[9] Arcangelis Mario. De, *Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts* (Poole, Dorset: Blandford Press, 1985), 11-12.
[10] Larson, Doyle E. "Exploiting Electronic Warfare" Air Force Magazine, July 1981, 1.
[11] Skantze, Lawrence A. "The Challenge of Electronic Warfare" Air Force Magazine, July 1982, 1-3.
[12] John A. Tirpak, "Electronic Warfare, Economy Style," Air Force Magazine, November 2012, 55, www.airforcemag.com.

[13] D. Curtis Schleher, *Electronic Warfare in the Information Age* (Boston: Artech House, 1999), xi.
[14] Haystead, John. "Enabling Global Strike: EW Upgrades for the USAF's Bomber Fleet" Journal of Electronic Defense, March 2013, 37.
[15] Chris Demchak, "Cybered Conflict vs. Cyber War," *Atlantic Council*, October 20, 2010, accessed February 6, 2014, www.atlanticcouncil.org/blogs/new-atlanticist/cybered-conflict-vs-cyber-war.
[16] John C.K. Daly, "US Air Force Prepares For Cyber Warfare," Space War, October 09, 2006, accessed December 17, 2013, http://www.spacewar.com/reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html
[17] Larson, Doyle E. "Exploiting Electronic Warfare" Air Force Magazine, July 1981, 1.
[18] *Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA)*, report (Fort Leavenworth, KS: Combined Arms Center - Capability Development Integration Directorate, 30 March 2011), 26.
[19] Office of Naval Research, "Navy Leaders Announce Plans for Deploying Cost-Saving Laser Technology," Navy.mil, April 08, 2013, accessed December 17, 2013, http://www.navy.mil/submit/display.asp?story_id=73234.
[20] "Kirtland Air Force Base - AFRL Directed Energy Directorate," Kirtland Air Force Base - AFRL Directed Energy Directorate, accessed December 17, 2013, http://www.kirtland.af.mil/afrl_de/.
[21] *Fiscal Year 2014 Air Force Science and Technology*, PRESENTATION TO THE HOUSE ARMED SERVICES COMMITTEE Cong., 13 (16 April, 2013) (testimony of Dr. David E. Walker).
[22] Robert K. Ackerman, "Iraq Hones Army Electronic Warfare," SIGNAL Magazine, June 2007, article body, accessed February 02, 2014, http://www.afcea.org/content/?q=node/1328.
[23] Ibid.
[24] Army Field Manual (FM) 3-36. *Electronic Warfare*, November 2012. E-1.
[25] *Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA)*, report (Fort Leavenworth, KS: Combined Arms Center - Capability Development Integration Directorate, 30 March 2011), EXSUM 1.
[26] Jonathan Greenert, "Adm. Greenert: Wireless Cyberwar, The EM Spectrum, And The Changing Navy," Breaking Defense, April 03, 2013, accessed December 18, 2013, http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy/.
[27] "Air Force Secretary Announces Provisional Cyber Command," Air Force Secretary Announces Provisional Cyber Command Article Display, September 19, 2007, accessed February 8, 2014, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/125683/air-force-secretary-announces-provisional-cyber-command.aspx.
[28] Chief of Naval Operations Strategic Studies Group XXXI, *EM Maneuver Warfare*, report (Chief of Naval Operations Strategic Studies Group, January 2013), 1-3.

BIBLIOGRAPHY

Academic Papers

Dobbs, William F., “Reclaiming Lost Ground: The Future of Electronic Warfare in the USAF” SAASS Thesis, Air University, Maxwell AFB, June 2008.

Articles

Ackerman, Robert K. "Iraq Hones Army Electronic Warfare." SIGNAL Magazine. June 2007. Accessed February 02, 2014. http://www.afcea.org/content/?q=node/1328.

Air Force Secretary Announces Provisional Cyber Command." Air Force Secretary Announces Provisional Cyber Command Article Display. September 19, 2007. Accessed February 8, 2014. http://www.af.mil/News/ArticleDisplay/tabid/223/Article/125683/air-force-secretary-announces-provisional-cyber-command.aspx.

Batson, Mickey, and Matthew Labert. 2012. "Expanding the Non-Kinetic Warfare Arsenal." *U.S. Naval Institute Proceedings* 138, no. 1: 40-44. *Academic Search Complete*, EBSCO*host*(accessed December 17, 2013).

Bourque, Jesse. 2008. "Why EW Is Not Part Of Cyberspace." *Journal of Electronic Defense* 31, no. 9: 38-40. *Academic Search Complete*, EBSCO*host*(accessed December 17, 2013).

Bourque, Jesse, “Does EW + CNO = Cyber?” Journal of Electronic Defense. Gainesville: September 2008. Vol. 31, Iss. 9; pp 30-35.

Congressional Research Service. "Electronic Warfare Is Dragging." *Air Force Magazine*, April 2001. Accessed October 07, 2013. http://www.airforcemag.com/.

Daly, John C.K. "US Air Force Prepares For Cyber Warfare." Space War. October 09, 2006. Accessed December 17, 2013. http://www.spacewar.com/reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html .

Demchak, Chris. "Cybered Conflict vs. Cyber War." *Atlantic Council*, October 20, 2010. Accessed February 6, 2014. www.atlanticcouncil.org/blogs/new-atlanticist/cybered-conflict-vs-cyber-war.

Greenert, Jonathan W. "Imminent Domain." *Proceedings*, December 2012. Accessed October 3, 2013. www.usni.org.

Greenert, Jonathan. "Adm. Greenert: Wireless Cyberwar, The EM Spectrum, And The Changing Navy." Breaking Defense. April 03, 2013. Accessed December 18,

2013. http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy/.

"Kirtland Air Force Base - AFRL Directed Energy Directorate." Kirtland Air Force Base - AFRL Directed Energy Directorate. Accessed December 17, 2013. http://www.kirtland.af.mil/afrl_de/.

Knowles, John. "Why Two Domains Are Better Than One." Journal of Electronic Defense, Gainesville: May 2013. Vol. 36, No. 5; 48-51.

Larson, Doyle E. "Exploiting Electronic Warfare." *Air Force Magazine*, July 1981. Accessed October 07, 2013. http://www.airforcemag.com/.

Office of Naval Research. "Navy Leaders Announce Plans for Deploying Cost-Saving Laser Technology." Navy.mil. April 08, 2013. Accessed December 17, 2013. http://www.navy.mil/submit/display.asp?story_id=73234.

Skantze, Lawrence A. "The Challenge of Electronic Warfare." *Air Force Magazine*, July 1982. Accessed October 07, 2013. http://www.airforcemag.com/.

Tirpak, John A. "Electronic Warfare, Economy Style." *Air Force Magazine*, November 1995. Accessed October 07, 2013. http://www.airforcemag.com/.

Tirpak, John A. "The F-35's Race Against Time." *Air Force Magazine* 95, no. 11 (November 2012): 52-55. Accessed January 25, 2014. http://www.airforcemag.com/MagazineArchive/Pages/2012/November%202012/1112fighter.aspx

Congressional Research Service. "Electronic Warfare Is Dragging." *Air Force Magazine*, April 2001. Accessed October 07, 2013. http://www.airforcemag.com/.

Books

Adamy, David. *Electronic Warfare: Pocket Guide*. Raleigh: SciTech Publishing, 2011.

Adamy, David L. *EW 101: A First Course in Electronic Warfare*. Boston: Artech House, 2001.

Adamy, David L. *EW 102: A Second Course in Electronic Warfare*. Boston: Artech House, 2004.

Browne, J. P. R., and M. T. Thurbon. *Electronic Warfare*. Vol. 4. London: Brassey's, 1998.

De, Arcangelis Mario. *Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts*. Poole, Dorset: Blandford Press, 1985.

Elsworth, Adam T., ed. *Electronic Warfare*. New York: Nova Science Publishers, 2010.

Price, Alfred. *The History of US Electronic Warfare.* 1st ed. Vol. 3. United States: Association of Old Crows, 2000.

Price, Alfred. *War in the Fourth Dimension: US Electronic Warfare, from the Vietnam War to the Present*. London: Greenhill, 2001.

Schleher, D. Curtis. *Electronic Warfare in the Information Age*. Boston: Artech House, 1999.

Schleher, D. Curtis. *Introduction to Electronic Warfare*. Dedham, MA: Artech House, 1986.

Wong, Wilson. *Emerging Military Technologies: A Guide To The Issues*. Santa Barbara, CA: Praeger, 2013.

Government Documents

Air Force Doctrine Document (AFDD) 3-13.1. *Electronic Warfare*, 28 July 2011.

Air Force Doctrine Document (AFDD) 3-12. *Cyberspace Operations*, 15 July 2010.

Chief of Naval Operations Strategic Studies Group XXXI. *EM Maneuver Warfare*. Report. Chief of Naval Operations Strategic Studies Group, January 2013.

Joint Publication (JP) 3-13.1. *Electronic Warfare*, 08 February 2012.

Fiscal Year 2014 Air Force Science and Technology, PRESENTATION TO THE HOUSE ARMED SERVICES COMMITTEE Cong., 13 (16 April, 2013) (testimony of Dr. David E. Walker).

Army Field Manual (FM) 3-36. *Electronic Warfare*, November 2012.

Muir S. Fairchild Research Information Center
Digital Collections
Air University-Maxwell AFB, AL