AETC CASE NUMBER-2020-04

AIR FORCE FELLOWS

AIR UNIVERSITY (AU)

EW AND CYBER CONVERGENCE:

BEYOND INFORMATION WARFARE

by

Ryan J. Worrell, Lt Col, USAF

A Research Report Submitted to the Air Force Fellows
in Partial Fulfillment of the Graduation Requirements

Advisor:
Col Timothy Helfrich
Defense Advanced Research Projects Agency

Maxwell Air Force Base, Alabama

April 2020

Disclaimer

Contents

Illustrations

Acknowledgements

Thank you to Mooch and Fog, two men passionate about bringing the right people together to achieve results regardless of tribe, domain, and AFSC.

Abstract

Electromagnetic Spectrum Operations (EMSO) and Cyberspace Operations (CO) are on divergent organizational paths driven by historical mission applications. Although both operate in and through the electromagnetic spectrum (EMS), each organization views its use differently. EMSO focuses on exploiting, attacking, protecting, and managing the physical EMS, while CO is focused on the data driven human use of digital applications and the data contained within cyberspace and the EMS. Each community has a specialty developed over many years, but entrenched thought has created a divide between the two. Over time, doctrinal rhetoric or relabeling of terms may close the divide, but these efforts are cumbersome and often unsustainable. A more successful approach would be the assignment of common focus areas to unify applicable portions of each community. One such focus area should be building a coherent process within the Air Force to develop, test, and field relevant technology for embedded cyber applications in a timely manner. This focus area's mission would be fighting system to system with an initial Suppression of Enemy Air Defense (SEAD) type approach of a blue aircraft system versus a red Integrated Air Defense System (IADS). This approach could be further scoped to air centric with a focus on the blue aircraft network versus the red aircraft network. To do this many classification boundaries will need to be lowered to enable EWOs, COs, engineers, and pilots to work together to field a sustainable system approach within the Air Force.

Chapter 1

Foundational knowledge: Domains and Doctrine

> *Mission success in large-scale combat requires full spectrum superiority; the cumulative effect of achieving superiority in the air, land, maritime, and space domains; the information environment; and the EMS.*
>
> —JP 3-0

The increased complexity and interconnectedness of the operational environment has and will continue to drive the evolution of large-scale combat from domain specific to domain agnostic. AirLand Battle, Cross-Domain Integration (X-DI), Multi-Domain Operations (MDO), and today's Joint All-Domain Operations (JADO) are iterative evolutions that seek to increase Joint efficiency and effectiveness. Caught in these iterative evolutions, Electromagnetic Spectrum Operations (EMSO) and Cyberspace Operations (CO) have witnessed significant technological advancements in electromagnetic spectrum (EMS) access and computing effectiveness. These accelerations have both blurred the EMSO and CO lines and simultaneously created an artificial need to separate the two. In fact, doctrine will claim these are different domains with different plans for warfare and development. In truth, these advancements offer an integration opportunity to provide capabilities and increased capacity for the Joint Force Commander (JFC). Instead of focusing on doctrinal differences, both EMSO and CO should seek out the overlaps and identify future growth opportunities to develop, train, and fight together. Focused integration, in place of forced doctrinal rhetoric or relabeled terms, enables greater capabilities to the warfighter and combatant

commanders, specifically for the Air Force's Counterair mission. In order to clearly set a vector towards integrated operations we must begin with where we are now.

Domains: Two sides of the same coin

There are a few ways the word domain is interpreted. Each one carries a slightly different connotation and it is important that this report sets a foundation to start from.

Domain as defined by Merriam-Webster:

- a territory over which supreme authority is exercised
- a region distinctively marked by some physical feature
- an area or range of knowledge, influence, or activity[1]

In Joint Publication (JP) 3-0, the word domain is used to label the four physical aspects of the operational environment (OE): air, land, maritime and space, but domain is never defined. The OE is further defined to include the electromagnetic spectrum (EMS) and the information environment (which includes cyberspace), but neither are identified as domains.[2] In JP 3-12 cyberspace is identified as a global domain in the information environment (IE) and JP 3-13.1 reiterates that the EMS is the electromagnetic environment (EME) of the OE.[3] While overly convoluted, these joint doctrines collectively state that any OE consists of the air, land, maritime, and space domains; the EME (EMS in the OE); and the cyberspace domain (part of the IE in the OE), see Figure 1.

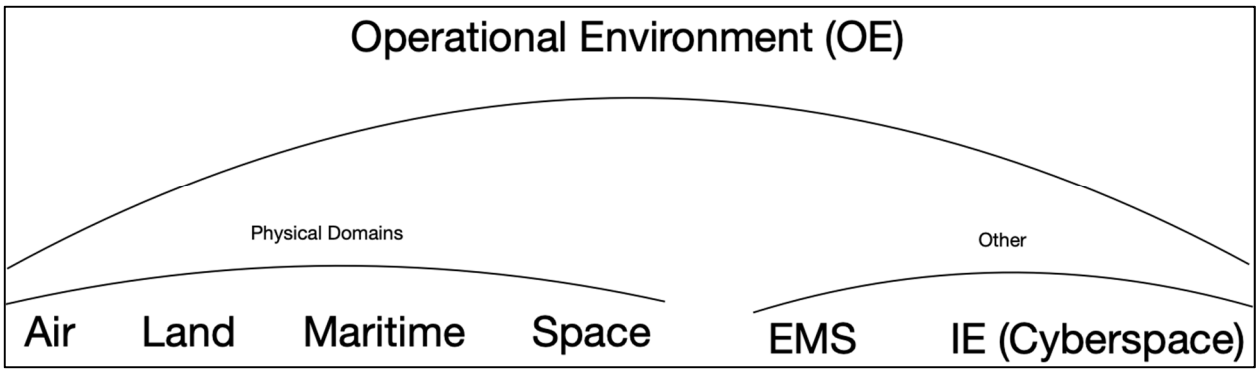

Figure 1: Joint Doctrine – Operational Environment

Conversely, Air Force Doctrine Note (AFDN) 1-20 does define the word domain and identifies Cyberspace and EMS as independent domains, see Figure 2. Succinctly defined as, "a sphere of activity or influence with common and distinct characteristics in which a force can conduct joint functions", the USAF's role in JADO is to support operations in the Air, Space, Cyberspace, and EMS domains.[4] The purpose of Air Force operations in and through all four domains listed is to enable convergence of effects in all domains. This "convergence of effects" is a fundamental idea that will be revisited.

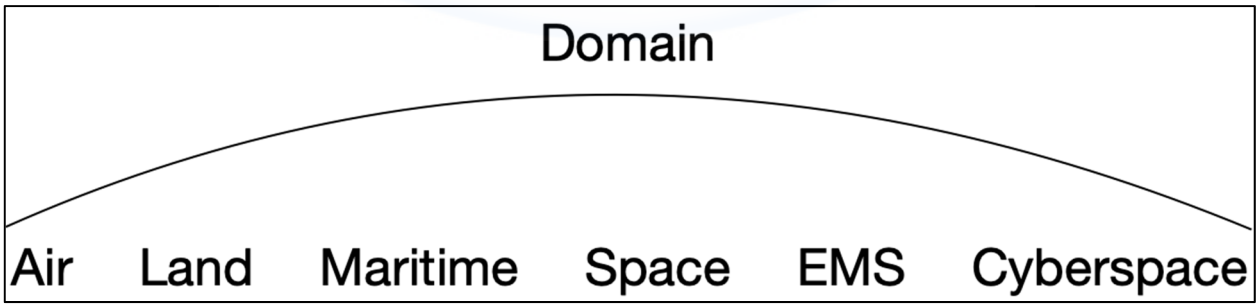

Figure 2: Air Force domains

Cyberspace as previously mentioned, is defined as a global domain in Joint Publication 13-2 Cyberspace Operations.[5] The cyberspace domain is the interdependent network of information technology infrastructures and their associated data within the Information Environment. It includes the "Internet, telecommunications networks, computer systems, and embedded processors

and controllers."[6] Any cyberspace operation aims to achieve some effect in and/or through this interdependent and interconnected domain that weaves through every aspect of modern conflict. For example, IADS are interdependent and interconnected networks reliant on computer systems and embedded processors for increasing functionality. Further, individual weapon systems, from aircraft to Surface-Air-Missile (SAM) systems, continue to incorporate computer systems and embedded processors to perform specific data integration and dissemination functions.

Cyberspace operations seek to achieve effects in and/or across three layers: physical, logical, and persona. Each layer encapsulates a unique portion of the cyberspace environment and requires different levels of intelligence information to effectively exploit or attack. The physical layer is the actual hardware, components, and nodes of the wired and/or wireless network. Logical includes the processes, algorithms, and functions that manipulate data within the network. Finally, persona includes the digital identity of users, procedures, and activities in or on a network.[7] These three layers can be complicated within the IP based networks of the Internet, however their protocols are documented and available to any Internet user.

Within a closed military network, such as an IADS and airborne networks, the information controls are more regulated, thus less complex. An IADS' physical nodes may leverage wireless datalink connections to increase mobility and survivability of individual systems. The IADS' infrastructure may be simpler from a logic perspective but can include different protocols and processes for handling information compared to normal Internet protocols. The persona layer may align perfectly with the logic layer, if the persona of each aircraft and weapon system is assigned to enable network participation in a prescriptive manner. Airborne networks rely exclusively on datalinks and voice communications in the EMS for their data applications and should be considered part of cyberspace. The increased use of datalink connections and a reliance on

integrated processors across military networks provides a convergence opportunity for operations within cyberspace and the EMS.

Electromagnetic spectrum (EMS) is a domain defined as all frequencies of electromagnetic radiation and consists of oscillating electric and magnetic fields. Unlike the cyberspace domain, the EMS exists without human interaction and is a domain with both physical and temporal units.[8] While different, the EMS and cyberspace are both pervasive domains critical to many cross-domain effects. The EMS ranges in frequency from zero to infinity and is subdivided into 26 lettered categories from radio waves to gamma rays. The most prolific EMS access for civilian and military applications is the radio frequency (RF) spectrum between 30 Hertz and 300 Gigahertz.[9] In this contested and congested spectrum, all platforms, weapons, and their associated kill chains must balance accessing, exploiting, protecting, and contesting an adversary's EMS use; this is the essence of EMS operations.[10]

Whereas, CO seeks effects in and/or across three layers, EMS operations seek to exploit, attack, protect, and manage the physical layer of the EMS. This physical layer is the external RF of the hardware, component, or node in a wireless network. This is not to imply that EMSO lacks internal layers similar to CO's logical and persona layers, but for EMSO these internal layers are simply data carried by the external physical layer (RF). For example, an aircraft receiver can exploit the internals (voice or data) of a link by tuning to a specific physical RF. Similarly, a radar transmits and receives on a specific RF, but uses an waveforms with embedded information to process radar returns. Finally, a jammer may use internals to identify a threat, but to effectively jam the threat signal the physical RF must be engaged. While there are subtle nuances in CO and EMSO layers, their strengths lie more in their commonalities and can be leveraged through cross domain (cyberspace and EMS) applications.

The original definitions that divided these domains is inaccurate and grew out of a misunderstanding that there are two domains. The technology is developed in parallel using the EMS to convey digital information of various forms. While the internet is met with much exuberance and opportunity for military exploits, this exuberance misdirects attention that could be focused on exploitation of digital information on military weapon systems and networks. The United States Navy and Army have already incorporated cyberspace into their EW function; however, the USAF has myopically focused on internet-based applications of CO.[11]

Cross Domain Applications

Domains are a way to help describe the physical environment being used for a function but should not unnecessarily bound a warfighting action. In reality many warfighting actions cross domains on a regular basis. Some are more significant crossings than others thus drawing attention as a unique action or warfighting development. An example of a clear cross-domain application is an aircraft releasing a munition against a surface target. The aircraft, operating in the air domain, causes an effect on the land domain. If a cyber-effect uses the Internet (cyberspace domain) to create an effect on a node within a space network, then that action effects the space domain. If an airborne electromagnetic attack uses the EMS domain to create an effect on another airplane or surface target that action is using both the air and EMS domains. Finally, when a cyber-effect crosses the wireless EMS domain to create an effect on a node within an IADS network that action is using both the cyberspace and EMS domains.

In general, doctrine and theory use the primary domain in which the function is occurring to denote the type of military power. This traditional concept does not hold true for cyber or EW. For cyber we have defined the cyberspace domain as a man-made information domain agnostic of a physical medium. Cyber is reliant on influencing the data within the medium, but the medium

itself is considered irrelevant. EW is reliant on affecting data flow by influencing the medium in both the physical world (physics-based RF wave) and digital world (data encoded in physical space). If tactical aircraft data are manipulated through the EMS from another aircraft using cyber techniques…what is it? It is Airpower enabled through the EMS/Cyberspace/Air domain. This is a very different cross-domain effect requiring a multi-disciplinary approach to understand this integrated process (desired effect, timing, and follow-on action or decision) from start to finish.

Doctrines

In order to understand how this integrated cross-domain process should work it is important to review both relevant Joint and Air Force doctrine. Doctrine provides best practices and guidance for warfare applications. This study consulted the following doctrine and will provide a short review to determine alignment and misalignment between Cyber Operations (CO) and EW.

Cyber Operations and EW doctrine:

JP 3-12: Cyberspace Operations
AF Annex 3-12: Cyberspace Operations
JP 3-13: Information Operations
JP 3-13.1: Electronic Warfare
JP 6-01: Joint Electromagnetic Spectrum Management Operations
JDN 3-16: Joint Electromagnetic Spectrum Operations
AF Annex 3-51 EW – EMSO
AF Doctrine Note 1-20: USAF Role in Joint All-Domain Operations

Cyberspace doctrine through EMS

Joint doctrine contains a section for how cyberspace attacks should be integrated with other fires. The example presented is EMS-enabled cyber-attacks against an enemy IADS.[12] The remainder of the cyberspace examples in Joint Doctrine are associated with normal network operations through the Internet or phone lines. This explains why the majority of cyberspace

operations focus on defense of Department of Defense Information Network (DODIN) and offensive use of the Internet.

Since CO will utilize EMS for some activities in the wireless medium there is coordination that must go through Joint electromagnetic spectrum operations (JEMSO). JEMSO doctrine focuses on managing the EMS with regard to EW and deconflicts any other fires/communications that plan to exploit, attack, or protect resources in the EMS.[13] Within JEMSO, each service component coordinates EMS usage differently. The Air force uses a communications staff officer in coordination with Intel and operations to plan and coordinate JEMSO.[14] The communications officer is neither cyber nor EW trained. Computer Network Operations (CNO) conduct effects focused on electronic information and infrastructure in the digital domain of Cyberspace. While EW focuses on the use of the radiated energy, CNO is oriented about the information (data) on the networks or the network structure itself. Any CNO mission that requires EMS support must then coordinate use through JEMSO in a similar fashion to traditional EW missions.[15]

The Navy takes a different direction by delegating management of the RF spectrum to Navy Cyber Forces. This delegation inherently links the two components of EW and CO together and can enable better integration. JEMSO and network operations (NETOPS) only overlap where frequencies are used to conduct NETOPS. NETOPS will place a request for frequency utilization to the spectrum manager at the CCMD and subordinate unified command level. Typically, this will be handled by the Joint Electronic Warfare Cell (EWC) in the J-3.[16]

EW doctrine to Cyberspace

Electromagnetic Warfare is composed of three primary divisions; electromagnetic attack (EA), electromagnetic protection (EP), and electromagnetic warfare support (ES). EA is the "use of EM energy, [directed energy], or anti-radiation weapons to attack personnel, facilities, or

equipment with the intent of degrading, neutralizing, or destroying enemy combat capability."[17] EP is focused on protecting personnel, facilities, and equipment from any phenomena (friendly, neutral, enemy, and natural) that would prevent use of a friendly combat capability. ES is any action tasked by an operational commander to "search for, intercept, identify, and located or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat reaction, targeting, planning and conduct of future operations."[18]

Wired and wireless links are portions of EMS used to carry information (cyberspace). Since EW focuses on disrupting enemy use of the EMS through EA while protecting friendly use through EP, it is natural that EW and CO should be coordinated. If not coordinated, there is a high risk of fratricide from either EW or CO.[19]

These concepts consider EW and CO as two separate exclusive operations in the same medium, the EMS. However, an enemy IADS operates as a computer network across the EMS. It treats the physical medium of EMS and the data carried across it as one coherent system. Thus, the airpower system of CO and EW should not only synchronize separate efforts, but they must work in unison to achieve a singular effect. EW could open the door through the medium (EMS) to enable CO to conduct data operations within the closed network. Thereby "Causing an enemy radar to think it's a washing machine and go into the rinse cycle," as an example.[20] The conceptual pairing of EW and CO is easily applied to any enemy embedded military system that uses computer processors and any wired or wireless connection to another computer system. This application would be evident in any SEAD or IO mission area.[21]

CO may be conducted through EW and EW may be conducted through CO. The attack surface in the OE is increasing daily as new signals are used to propagate information across the planet. Even if wired access is not available to a computer network, EMS access might be the link to a

successful computer attack. If an aircraft was used to deliver malicious code into cyberspace through a wireless aperture that would be considered "EW-delivered computer network attack (CNA)."[22] Additionally, EW could be used to destroy a physical node in a computer network using and electromagnetic pulse (EMP) or high-powered microwave (HPM) weapon, which would then be a cyberspace effect caused by EW. EW operations are critical to setting proper conditions for CO against enemy military networks due to their inherent closed architectures isolated from the commercial Internet.[23]

Counterair aligns both EW and CO to a single mission set comprised of clear targets to address. The CO mission is allocated airfields, operating bases, and other support infrastructure reliant on IP based networks. EW suppresses C2 and the networked IADS wireless links (voice or data) and nodes (radars or radios). The overlap in mission is targeting C2 and the networked IADS links and nodes. Counterair provides two focus areas, C2 and SEAD, to narrow application vignettes for EW and Cyber convergence.[24] These focus areas are represented by enemy aircraft networks or IADS networks. Today these may be separate networks, but in the very near future technology advancements will enable many countries to connect these two digital wired and wireless networks. Thus it is incredibly important for EW and CO operations to be integrated in a tactical manner applied to Counterair missions.

Summary

A majority of EW doctrine discusses how to use EA, ES, and EP to conduct Information Operations and SEAD mission sets. The majority of CO doctrine covers network operations to support Information Operations and Intelligence. Both EW and CO doctrine clearly state a means of integration between EW and CO to conduct fires through the EMS into cyberspace and cause effects in cyberspace through EW. In the following chapter the organizational structure described

will show how a portion of EW and CO doctrines are fulfilled but still miss an important convergence in the SEAD mission set.

Notes

[1] (Merriam-Webster 2020)
[2] (Joint Publication 3-0 2018)
[3] (Joint Publication 3-12: Cyberspace Operations 2018) (Joint Publication 3-13.1: Electronic Warfare 2012)
[4] (U.S. Air Force Doctrine 2020)
[5] (Joint Publication 3-12: Cyberspace Operations 2018)
[6] Ibid
[7] Ibid
[8] (Curtis E. LeMay Center for Doctrine Development and Education 2019)
[9] Ibid
[10] (Joint Doctrine Note 3-16: Joint Electromagnetic Spectrum Operations 2016)
[11] (Joint Publication 3-12: Cyberspace Operations 2018)
[12] Ibid
[13] (Joint Publication 6-01: Joint Electromagnetic Spectrum Operations 2012)
[14] Ibid
[15] Ibid
[16] Ibid
[17] (Joint Publication 3-13.1: Electronic Warfare 2012)
[18] Ibid
[19] Ibid
[20] (Jumper 2006)
[21] (Joint Publication 3-13.1: Electronic Warfare 2012)
[22] Ibid
[23] Ibid
[24] (Curtis E. LeMay Center for Doctrine Development and Education 2019)

Chapter 2

Organizational Application

Definitions are neither true nor false. They are chosen for convenience.

—Colin S. Gray

All organizations in our modern military access the electromagnetic spectrum or use cyberspace in some form or fashion. The following chapter will show how the Air Force has chosen to establish its forces for organizing and equipping specifically to electromagnetic warfare and cyberspace operations. There will be some reference to the overarching structure of cyber and EW, but the intent is to focus on how specific integration for offensive operations is currently enabled and identify where shortfalls may occur. In general, defensive and management operations for both CO and EMSO consume a large portion of our Air Force's time and resources to facilitate daily peacetime operations and help prepare for wartime operations.

Organizations

The two primary organizations in the Air Force for conducting EW and Cyber are very separate and distinct teams, under Air Combat Command (ACC). The 16th AF is primarily focused on Intelligence Surveillance Reconnaissance (ISR) and network cyber operations and the 53 WG is focused on airborne EW and Operational Test (OT).

Sixteenth Air Forces (Air Forces Cyber) is the numbered command with primary responsibility for organizing, training, and equipping forces for Information Warfare (IW) operations. 16th AF manages intelligence, reconnaissance, cyber warfare, electronic warfare, and information warfare.[1] Additionally, the 16th is the Service Cryptologic Component and is responsible to the National Security Agency/Central Security Service for Air Force matters involving the conduct of cryptologic activities. Reactivated in October 2019, the 16th AF merged the 24th AF (AFCYBER) and 25th AF (known as Air Force Intelligence).[2] The IW NAF is steadily increasing integration between organizations and includes the merger of the 625th Operations Center and 624th Operations Center into a newly formed 616th Operations Center as "a warfighting unit that will be responsible for the convergence of Air Force Information Warfare."[3] However, historic precedent leans toward its ISR and cyber foundations as evident in its subordinate units.[4] The 55th Wing, 668th Cyberspace Wing, and the Air Force's newest combat wing, the 67th Cyberspace Wing comprise 16th AF's EMSO and CO units and provide some burgeoning offensive integration. The 55th Wing operates all variants of the RC-135 and the EC-130H, focusing on reconnaissance and electronic warfare.[5] The 668th Cyberspace Wing focuses on defensive cyber operations, actionable intelligence, engineering and installation of capabilities.[6] 67th Cyberspace Wing rounds out the cyber operation focused on "generating, projecting, and sustaining combat power through the Cyberspace Vulnerability Assessment/Hunter weapon system."[7]

The 53 Wing produces most of the EW software and mission data files for aircraft in the AF for fighters, bombers and specialized electronic warfare aircraft.[8] Hardware for aircraft is developed by aircraft manufacturers at initial aircraft design and acquired through program offices during sustainment. Software is modular but generally produced by the original maker and

published in updates on an annual or more frequent basis. The 53 WG takes collected intelligence and uses those databases to program mission data files for each aircraft. The 53rd Wing does not currently conduct EW development for the EC-130H units who are managed by Big Safari and assigned to the 55 Wing under 16th AF. With the projected activation of the Spectrum Warfare Wing (SWW), the Air Force may have an additional opportunity to align EW and CO efforts, however further details are not available on how the SWW will be organized and which authorities it will control.

Equipping

Some specialized units are beginning to investigate Cyber through EW applications, but the funding / manning scale or classification has prevented them from progressing beyond initial technology development. Some very limited fielding efforts have succeeded through individual program offices. A matured EMS Superiority Directorate (newly established at HAF/A5L) may provide a more unified approach. As such, the Air Force currently lacks a robust architecture to develop, test, and field EMS enabled cyber effects to a broad range of assets and mission sets.

Summary

Two organizations are primarily responsible for EW and Cyber operations in the USAF. Each organization has a separate mission focus with very little overlap. As a result, requirements are not being submitted to create cross-domain effects integrating the two. Additionally, there is no codified integration or development pipeline to identify gaps, partner with research labs, and deliver capabilities or capacity to the primary operators (CO, EWO, or pilot). Lacking a steady state capability pipeline, there is no training environment and testing events to provide the only

"one-time" opportunity to develop tactics, techniques, or procedures for integrated EW and cyber solutions.

Notes

[1] (US CYBERCOM 2020)
[2] (16th AF 2020)
[3] (LtGen Haugh 2020)
[4] (Air Force News 2020)
[5] (55 WG Factsheet 2017)
[6] (688CW Factsheet 2020)
[7] (67WG Factsheet 2020)
[8] (53 WG Factsheet 2020)

Chapter 3

Discussion

The evolution of the IADS net has made communication and information the key elements of its structure.

—Lt Col James Brungess, USAF

Change is a difficult process to approach when many organizations are fighting for resources to do their assigned duty. To imply there is another duty more relevant than their given task may cause upheaval or resistance. However, when faced with modern warfare there is a relevance in preserving human life by increasing effectiveness of the warfighter. EW and Cyber must converge in some activities but not all. Convergence needs to happen to support airpower applications against enemy military networks: surface, air, and space networks. All three networks rely heavily on the EMS to transmit data that operates in closed networks based on modern computing processes. In order to conduct embedded cyber effects within these networks a convergence of EW and CO is required to fully grasp and solve the problem set.

Convergence

From Merriam-Webster, convergence is defined as "the merging of distinct technologies, industries, or devices into a unified whole."[1] While the Air Force speaks to EW and Cyber

convergence its EW/EMSO and CO doctrines are overlapped, its organizations are unaligned, and its mission authorities are divergent.

Doctrine. Clearly defining the cyberspace and the electromagnetic spectrum as two separate domains creates unnecessary division and stove-piping between the two communities. Initially Cyber grew as a mission solely focused on use of the interconnected network of computers around the world, rather than military equipment due to the stand-alone nature of most aircraft, tanks, and ships. However as military equipment grew into network centric warfare there was a new set of networks available for cyber operations. During that time of growth, the EW community continued to focus on detecting and disrupting individual portions of the EMS, specifically focusing in radars, communications, and datalinks.

These CO and EW concepts are both sides of the same coin, but our doctrine ineffectively draws succinct lines in the sand with only tangential mention to "cross-domain" support options. Further, these lines have established small fiefdoms that are unable to integrate with each other. There is no impetus for cyberspace to integrate with EW, because CO are mostly focused on the global commons of computers in an Information Warfare (IW) fight. Cyberspace doctrine is missing implications for all airpower applications, except for IW. Cyberspace doctrine should be adjusted to include clear applications during full scale conflict. Offensive Cyber applications against enemy military embedded systems and networks would help delineate roles and drive modernization for a portion of cyber units across our Air Force organizations.

Organizations. The new 16th AF does not promote convergence between cyber operations and electromagnetic warfare. Their primary focus is still intelligence and information warfare. Using cyber to gain additional intelligence is simpler and less cost imposing, so it makes sense as the easiest first change to implement. However, it would be more important to specifically enable

cyber and EW forces to operate together to target enemy embedded systems and networks that are closed off from 'traditional' cyberspace. The Air Force has many responsibilities across the full spectrum of conflict, but ultimately, it is a warfighting organization and should remember to maintain that focus in preparation for any future conflict.

The last reason cyber and EW forces need to converge and act in union is primarily driven by how military systems interact. The easiest point to access a closed network enemy IADS or aircraft network is through the friendly aircraft with line of sight to the network and proximity to detect the EMS portions of the network. After insertion of a cyber-effect is complete, it could then use the closed wired medium for further nefarious applications.[2] If organizations are not aligned to train for this type of activity it will never go beyond small back shop experiments. Line crews will not have proficiency to dynamically respond to changes in the network and EMS when conflict begins.

Our future force needs to be able to fight system warfare against adversary systems. Our blue assets will be networked through closed weapon system datalinks, supported by beyond line of sight (BLOS) communications, and must be enabled to systematically dismantle an opposing forces network. Dominance against an enemy network of the future will require access to both the physical domain of the EMS and the logical domain of cyberspace. Both the waveforms being transmitted, and the data contained within must be exploited, disrupted, and used for destruction to enable airpower and achieve our national objectives in any military conflict. This requires a convergence of our organizations and our authorities.

Authorities and enablers. Critical timing and effects must be delegated well below the Joint Force Air Component Commander (JFACC) level to the mission and package commanders. In either case of EMS enabled cyber or cyber enabled EW, the timing and tempo are critical to the

airborne assets exposed in the threat environment. Authority to operate and change tasking must be executed in clear communication with the protected assets. In order to do that in a timely manner it is evident we need to have properly educated EMS and Cyberspace operators forward deployed within manned platforms and with the right equipment.

Those authorities must be acting with a purpose for technology application. The goal is to change the adversary's course of action to comply with US interests.[3] By weaving EW and CO together, such doubt in the integrity of their systems will naturally coerce an enemy to slow or doubt their current ability to proceed. The capability to cause a hesitation in the pace of conflict will be critical to JADO and can be enabled by proper technology derived from a convergence of EMS and CO. Finally, these actions must be carried out with proper rules of engagement (ROE) to enable timely decisions at the forefront of the battlespace.

Equipping

Requirements / Acquisitions cannot take 15 years to design well enough hardware to field and iterate with software applications in a modular architecture. The combat air forces need cyber effects rapidly produced against military networks, such as IADS and airborne aircraft. Actionable capabilities against embedded systems would enable light-speed effects in an environment normally constrained by friction of air against missiles and bombs in flight. Alignment from development through fielding will be critical for the future of airpower. Development can focus on generating possible capabilities and effects rather than platform centric iterations.[4]

There does not need to be one place that is doing all of the RF-enabled Cyber, or Cyber enabled RF for that matter. It should be woven throughout both the EW and OCO communities. EWOs should understand that their effects are using the open-air medium and accesses inherent in the broad EMS to influence a computer processor. In order to understand the implications of EMS

actions effecting the computer processor, the operational or acquisition team requires both a computer engineer and EE engineer. In Cyber operations and development the opposite is also true, any good cyber technique should be using every access vector open to attack. This goes much beyond the traditional wired applications and begins to consider every input vector on a platform as a possible access vector. In order to properly close that loop the cyber team would benefit from an EW approach to using the EMS.

There is no clear delineation whether CO should support EW or EW should support CO. It is however clear that the two should support each other and it will depend on the mission and environment to decide who is supported and who is supporting. The same is true with all Air Force mission sets. It is rare to be able to truly say one type of power or domain will always be the supported force, but force must be dynamic and agile in order to defeat the adversary's integrated systems. Designing options that easily use both EW and CO give asymmetric options during future conflicts to quickly end or deescalate conflict by instilling military doubt in the adversary.[5]

Conclusion

In conclusion there should be one domain, EMS, comprised of a physical structure and an information structure. Within the EMS, the USAF conducts cyberspace operations and electromagnetic warfare. These two warfighting communities must develop in unison or the Air Force will be unable to conduct Joint All Domain Operations and all communities will find themselves without an ability to integrate due to ineffective development across multiple classifications, domains and doctrines.

In order to develop in unison, a single mission set should be used to focus efforts. A team of OCO and EWOs should be given access to any common work being done to address access to IADS through EMS. Their primary objective should not be to determine tactical applications for

this technology. Instead the team should make a deliberate effort to create a process in the Air Force where Cyber and EMS enabled technology can grow from basic development to operational application. It should consolidate requirements, enable feedback from operators, and provide direction connections to program offices with airborne weapon systems. This process should be similar to how any basic weapon or EA technique used by an aircraft is produced. After production the training environment must be enabled to facilitate tactical development.

Training ranges must enable Cyber and EMS enabled technologies to be used on a sortie to sortie basis. This frequency is required to suitably train individual operators to understand timing, tempo and effectiveness of their individual choices during a mission. Clear debrief information is crucial to that learning environment. Thus, ranges need to have a means to present exactly what happened during the mission, and how the cyber-attack or EMS attack caused a change in the enemy network. It will take years of practice and learning before the instructors in both OCO and EWO communities are able to build enough common knowledge to keep the community developing in a coherent tactical sense. After this point, an update to doctrine will help record valuable lessons learned in the use of the EMS to conduct cyber-attacks.

The final stage in any military development is an update to doctrine. As OCO and EWOs practice, provide feedback to acquisitions, and test new technology many lessons will be learned. Some will be niche lessons, but the overarching concepts will endure. These enduring lessons must drive a rewrite of doctrine. The rewrite should be approached with intent to identify ways to unify Cyber and EMS operations. Many warfighting mission sets will overlap and should be rewritten to clearly inform the next generation of warfighters how to use the EMS to create an asymmetric advantage for the United States of America in the Counterair mission.

Notes

[1] (Merriam Webster 2020)
[2] (Theohary and Hoehn 2019)
[3] (LtCol Sick 2019)
[4] (Maj Delloiacono 2019)
[5] (Gen O'Shaughnessy, LtCol Strohmeyer and LtCol Forrest 2018)

Glossary

ACC	Air Combat Command
C2	Command & Control
CNA	Computer Network Attack
CNO	Computer Network Operations
CO	Cyberspace Operations
DE	Directed Energy
DODIN	Department of Defense Information Network
EA	Electromagnetic Attack
EME	Electromagnetic Environment
EMP	Electromagnetic Pulse
EMS	Electromagnetic Spectrum
EMSO	Electromagnetic Spectrum Operations
EP	Electromagnetic Protection
ES	Electromagnetic Support
EWO	Electromagnetic Warfare Officer
EWC	Electronic Warfare Cell
HPM	High-Powered Microwave
JADO	Joint All-Domain Operations
JEMSO	Joint Electromagnetic Spectrum Operations
JFACC	Joint Force Air Component Commander
JFC	Joint Force Commander
IADS	Integrated Air Defense System
IE	Information Environment
IO	Information Operations
ISR	Intelligence Surveillance Reconnaissance
NETOPS	Network Operations
OCO	Offensive Cyber Operations
OE	Operational Environment
OT	Operational Test
RF	Radio Frequency
ROE	Rules of Engagement
SAM	Surface to Air Missile system
SEAD	Suppression of Enemy Air Defenses

Bibliography

2020. *16th AF.* April 15. https://www.16af.af.mil/About-Us/Fact-Sheets/Display/Article/1957318/sixteenth-air-force-air-forces-cyber/.

2020. *53 WG Factsheet.* April 14. https://www.eglin.af.mil/About-Us/Fact-Sheets/Display/Article/390946/53rd-wing/.

2017. *55 WG Factsheet.* 08 21. Accessed April 15, 2020. https://www.offutt.af.mil/Portals/97/55th%20Wing%20Fact%20Sheet2.pdf?ver=2017-08-21-102734-797.

2020. *67WG Factsheet.* April 14. https://www.16af.af.mil/Units/67CW/.

2020. *688CW Factsheet.* April 14. https://www.16af.af.mil/Units/688CW/.

2020. *Air Force News.* April 15. https://www.af.mil/News/Article-Display/Article/1987970/air-force-integrates-missions-strengthens-information-warfare-capabilities/.

2019. "Curtis E. LeMay Center for Doctrine Development and Education." *Annex 3-01 Counter Air Operations.* September 6. https://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-01-Counterair-Ops/.

2019. "Curtis E. LeMay Center for Doctrine Development and Education." *Annex 3-51 Electromagnetic Warfare and Electromagnetic Spectrum Operations.* July 30. https://www.doctrine.af.mil/Operational-Level-Doctrine/Annex-3-51-EW-and-EMS-Ops/.

Gen O'Shaughnessy, TJ O, Matthew LtCol Strohmeyer, and Christopher LtCol Forrest. 2018. *Strategic Shaping: Expanding the Competitive Space to Deter Great Powers during Crisis and Gain Advantage in Conflict.* Pacific Air Forces - Strategic Thinking White Papers.

2016. "Joint Doctrine Note 3-16: Joint Electromagnetic Spectrum Operations." *Joint Chiefs of Staff.* Oct 20. https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn3_16.pdf?ver=2017-12-28-144149-910.

2018. "Joint Publication 3-0." *Joint Operations.* Oct 22. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.

2018. "Joint Publication 3-12: Cyberspace Operations." June 8. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

2012. "Joint Publication 3-13.1: Electronic Warfare." February 08.

2012. "Joint Publication 6-01: Joint Electromagnetic Spectrum Operations." Mar 20.

Jumper, Gen John P. 2006. "Future Standoff Jamming." *AF Magazine* 31-32.

LtCol Sick, Kellen D. 2019. *Coercing the Mind: Using Non-Violent Actions To Achieve Politcal Outcomes.* SAASS Thesis, Maxwell AFB: Air University.

LtGen Haugh, Timothy D. 2020. *16th AF News.* Mar 18. https://www.16af.af.mil/News/Article/2116154/air-force-information-warfares-new-warfighting-unit-activates/.

Maj Delloiacono, Brad M. 2019. *Game Changing Technologies: Rapid on Ramps and Normalization.* Research, Air University.

2020. *Merriam Webster.* April. Accessed April 14, 2020. https://www.merriam-webster.com/dictionary/convergence.

2020. *Merriam-Webster.* Accessed April 10, 2020. https://www.merriam-webster.com/dictionary/domain.

Theohary, Catherine A., and John R. Hoehn. 2019. "Convergence of Cyberspace Operations and Electronic Warfare." Congressional Research Service, Washington D.C.

2020. "U.S. Air Force Doctrine." *Air Force Doctrine Note 1-20: USAF Role in Joint All-Domain Operations.* Mar 5. https://www.doctrine.af.mil/Portals/61/documents/Notes/Joint%20All-Domain%20Operations%20Doctrine--CSAF%20signed.pdf.

2020. *US CYBERCOM.* April 14. https://www.cybercom.mil/Components/.