

September 2008  
Vol. 31 • No. 9



The  
Electronic  
Warfare  
Publication  
[www.crows.org](http://www.crows.org)

# JED

*The Journal of Electronic Defense*

DOES

EW

+

CNO

= CYBER?

Also in this issue:

**EP-3: AIRBORNE SIGINT WORKHORSE**

# A (Pragmat Future for Joi Electronic Warfare

Does EW + CNO = Cy

ic)  
nt  
ber?

In the relatively short existence of the Joint Information Operations Warfare Command's Joint Electronic Warfare Center (JEWEC), we've enjoyed a very unique opportunity to observe and influence many contributing capabilities within the electronic warfare (EW) mission area. I'd like to offer some practical perspective on how we in the US EW community must reconsider our shared electromagnetic (EM) processes, paradigms and acquisition strategies in order to meet the current and projected threats awaiting us. But before you read any further, I ask you to reflect on the word "harmonization."

Right up front, I'd like to hit on three key points. First, the mission of Joint EW must never be relegated to the agenda of any single Armed Service as prime manager because this Service will ultimately appropriate Joint EW to serve only its own needs. Second, Joint EW must never be subsumed by the Cyber mission area because Cyber will appropriate Joint EW to serve only Cyber – and there are four other warfighting Domains still worthy of EW support. (For the purposes of this article, Cyber covers information technology infrastructures [ITI], as directed by the Joint Chiefs of Staff, and not the entire EM spectrum, as advocated by the Air Force.) Lastly, we have unwittingly evolved our shared EW processes to prevent the most capable and entitled organizations from managing them. As a result, we have built an incoherent EW organization across the DOD – a state we are rapidly losing the privilege to maintain.

### THE CROWDED EM SPECTRUM

Imagine a scenario in which we're in the middle of a large deployment of land forces in a faraway place. Several of the locals develop an inexplicable dislike for us over time and emplace RF-controlled "minefields" to deny our free access to the battlespace. To break the RF link in these improvised explosive systems, we rapidly build and deploy thousands of very clever road-portable jamming systems that sense and respond to RF threats (i.e., they feature a reactive architecture), ostensibly wasting finesse to cause minimal disturbance to an electromagnetic environment (EME)

that is arguably the most congested on the planet.

The problem is that when the "advanced" jammers arrive, they are met with in-band Blue Force communications; ISR conflicts; incompatible sister-Service active ground jammers; conflicts with proven, active airborne electronic attack (EA) capabilities; undeclared Gray (Allied) EA devices; and a wealth of legitimate in-band "White" civil-commercial traffic. The resultant EME is judged too complex to merit legitimate use of a brand new fifth-generation fighter. No coherent set of joint EM management processes awaited these deploying forces, just cool new toys, very good intentions and a ton of hard work to be done by a few talented warfighters trying to make sense of it all. What's the moral? Without senior advocacy, coherent joint oversight and adequate, proactive resourcing for joint EW, "EMI happens, with deadly consequences for Blue Forces."

### THE NEW STATUS QUO

There is now a battlespace-driven revolution in EW requirements. Joint EW's 21st-century challenge is to accept that, for the first time in the history of warfare, "tech peer" adversaries will intend, as their going-in position, to execute broad Spectrum denial against Blue Forces, exploiting known and systemic vulnerabilities and potentially denying physical battlespace access to those Blue Forces for some critical period of time. FACT: Spectrum is no longer an "unlimited resource." A concurrent migration (or expanding inclusion) in EM battlespace technologies is taking us from government-off-the-shelf (GOTS) to commercial-off-the-shelf (COTS) hardware, from high-power to low-power, from analog to digital and from airborne delivery to multi-Domain delivery (to include Land, Sea and Space), targeting accuracies and effects delivery from miles to meters in many cases, and certainly from RF-centric applications to multispectral effects.

In the massive, transformational "retooling" effort escorting the DOD involuntarily from a Major Combat Operation (MCO) posture to a more unsettling Counter-Insurgency (COIN) focus,

we must keep our eye on the long fight and appreciate that these shifts to meet the new asymmetric adversary (ideologically fueled and COTS-enabled in the current conflicts) in fact represent an expanding mission set for EW. This means that in addition to adapting EW to help fight the current adversary, we must not forfeit proficiency or capacity in the classical aspects of EW that are essential to defeating legacy threats. In other words, the list of things to do just got larger.

Red Force EM targeting of our GPS, IADS, communications, Space, C2, ISR and Cyber (i.e., IT, telecoms and SCADA infrastructure controllers) networks should each or all be anticipated during future engagements, from contingencies to MCO. To expand on a previous point, we must also accept that EW is reaching well beyond its RF beginnings to include directed energy (DE), high-power microwave (HPM), lasers, IR, EO, acoustics, particle beam weapons and whatever other intentionally developed or adapted threats the EM weapons experts can fathom.

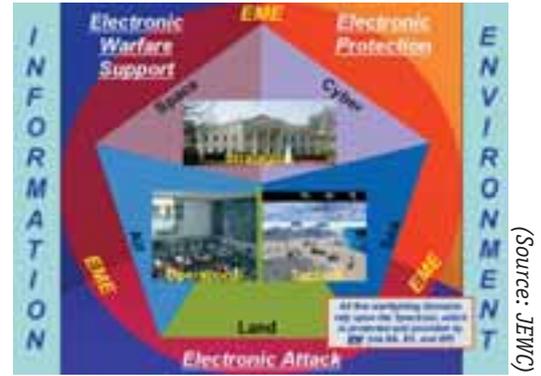
The following graphic is a simple, pragmatic and objective depiction of the new status quo. There are five warfighting Domains – Air, Land, Sea, Space and Cyber – and two warfighting environments – the EME and the information environment (IE). The EM Spectrum is present in every nook and cranny of the battlespace, save for the information environment, in practical terms. Further, the Spectrum is a continuum directly, completely and literally supporting the pentagon of military effort depicted. Conceptually subdividing responsibility for the Spectrum using the triad of EA, electronic warfare support (ES) and electronic protect (EP), decisive effects may be realized at all three levels of combat, and in every warfighting domain. As an example, we might throw EM energy at a “soft aperture” (i.e., one ready to receive and process in-band energy), such as a radar dish or an IEEE 802.11 wireless access point, delivering effects into the Land and Cyberspace Domains, respectively. Or we might direct high-energy malice, such as laser, HPM or other DE, instead at a “hard aperture” such as an unshielded circuit board with in-band

resonant characteristics or even a computer server unprotected by a Faraday cage. And because of EW’s maturity, proven history of operational-level execution and low potential for spillover of unintended effects, authorization to “fire” would not be as cumbersome or elevated as that of Cyber/CNO, itself dependent upon Spectrum Control as another customer of Joint EW.

The current evolution in EW demands a shift away from the comfortable old “EWO is a pod” or “EW equals EA” paradigms that have brought EW to its current state of broad process disarray and institutional atrophy. It’s also time to officially jettison the stale “EW equals Air” paradigm. Not only will EW and EM process effort be required from within the five Domains, these efforts will require new joint coherence to maintain a confident battlespace advantage over potential adversaries for the foreseeable future. This joint coherence will directly promote the process and capabilities development required to support our strategic missions. We can no longer enjoy the luxury of our previous “Air-centric, ELINT-specific” EW paradigm, either. Instead, EW is global Spectrum Control uniquely responsible for providing constant access to “contested” Spectrum and assisting in remediation and avoidance of “congested” Spectrum conditions as well. We comfortably recall the tested legacy mantra of strike aviation, “Steel on target.” Though this mantra will certainly enjoy continued utility for the foreseeable future, it’s time now to raise a new chant: “Energy on aperture.” Arguably, the latter includes the former. To the intrepid electronic warrior and the targeting experts who support him, the world is just one big collection of apertures.

The EW community can no longer afford to overlook EP’s contribution to the EW triad, nor its potential impact on EM capabilities, equipment and processes. Where EA and ES are typically “actions taken,” EP lives more as attributes that allow friendly missions and capabilities to continue operations in congested and contested (or denied) EM environments. Examples are the Joint Restricted Fre-

quencies List (JRFL) process; all low observables; SINGARS, HAVE QUICK and other spread-spectrum applications; electromagnetic pulse (EMP) hardening; etc. This framework represents a fundamental consistency in the language of JP 3-13.1, as well as US Strategic Command’s (USSTRATCOM’s) “Operational Concept for EW” (OCEW, 2006).



(Source: JEWIC)

## THE NOBLE QUEST FOR SPECTRUM DOMINANCE

The concept of Spectrum Dominance has gotten a lot of mileage over recent years, and Spectrum Dominance represents a fine conceptual target for harmonizing our warfighting focus. Recalling the simple vignette at the beginning of the discussion, however, 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 of Red Force EA, congestion from White users and managing electromagnetic interference from Blue Forces). Dominance in any play space arguably seeks to convey the owner’s ability to move freely throughout completely unimpeded, uninfluenced and unchallenged. From a logistical standpoint alone, the effort expended to attain such an absolute state would place us squarely within the “diminishing marginal gains” region. We are not equipped to achieve Spectrum Dominance even if the warfighter required it, which he does not.

If we weave no other common thread throughout future military DOTMLPF (Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities) considerations,



# WERLATONE

## **SOPHISTICATED APPLICATIONS**

- JAMMING
- COMMUNICATIONS
- CO-SITE MANAGEMENT

REQUIRE,

## **SOPHISTICATED SOLUTIONS**

- MORE POWER
  - GREATER BANDWIDTH
  - LESS LOSS
  - SMALLER PACKAGES
- 
- POWER COMBINERS/DIVIDERS
  - 90° HYBRID COUPLERS
  - 0°/180° HYBRID JUNCTIONS
  - DIRECTIONAL COUPLERS

DESIGNED TO MEET THE MOST STRINGENT OPERATING CONDITIONS.

Werlatone, Inc.  
2095 Route 22  
PO Box 47  
Brewster, NY 10509  
T. 845.279.6187  
F. 845.279.7404  
[sales@werlatone.com](mailto:sales@werlatone.com)

[www.werlatone.com](http://www.werlatone.com)

we must plan to capture efficiencies, not excesses. But on the path to this conceptual target, we must instead be contented to engage jointly in Spectrum Control actions, controlling the required portions of the Spectrum at the required time in the required location(s). This provides reliable access to enough Spectrum to conduct required operations and meet anticipated contingencies. Adversaries can pretend to own the rest if it suits them to think so. Instead, we must commit to constant pursuit of Spectrum Control – not “omnipotence,” just what it takes to get the job done reliably for our Joint Force Commanders.

### TYING IT ALL TOGETHER

When we integrate and synchronize operational-level EW and coherent EM capabilities development all together into one coherent package, the results have unavoidable strategic significance. While major regional “OPLANS” protect strategic national interests, USSTRATCOM’s OPLANS protect our nation. It is the coherent joint aggregation of regional and operational-level EW effort by an empowered repository of joint expertise that creates the durable foundation of strategic EW to achieve Global Spectrum Control. By engaging and neutralizing Red Force access to the Spectrum, as well as protecting Spectrum access from Blue EM process mismanagement and equipment incompatibility, Gray equipment “declaration” protocols and White expansion and encroachment, we can create spectral freedom of maneuver, which is critical to our strategic lines of operation. We will not get there by any real measure until we designate and empower one joint authority – an “Expert Advocate” to harmonize Service efforts in EM capabilities development, process development, compatibility, interoperability and operational execution.

### EW AND CYBER

As we look at what effects EW is delivering in the battlespace and how it provides Spectrum Control to the warfighter, it is also worth mentioning what EW is not. Simply stated, EW is not part of Cyberspace. Cyber is a customer of EW. It certainly uses limited aspects of EW, but EW serves

four other Domains – Land, Sea, Air and Space – that also need to achieve Spectrum Control (see “Why EW Is Not Part of Cyberspace,” p 38).

Within the Joint Service (and the strata above), the prevailing sentiment would indicate that EW will indeed remain an articulated mission area to exercise the critical care for and protection of the Spectrum, and not to be assimilated by any new peer mission area, such as Cyber. To contrast, operational and tactical EW are forms of non-kinetic fires, which are simply about denying, degrading, disrupting or destroying any and all adversary EM-susceptible networks or their use of relevant parts of the Spectrum. Computer network operations (CNO – now, Cyber) can hit many of these networks through wired coupling and a few unwired hops (such that national authorities will even allow). But EW is a very mature mission area that can make targeted apertures of them all, and it has been capable of doing so for quite a bit longer than Cyber. EW has massed capabilities to attack most, if not all, EM-susceptible adversary network apertures (“soft” and “hard”), protecting friendly networks for more than six decades. In contemporary terms, examples of these adversary EM-susceptible networks include Space, communications, C2, ISR, IADS, Air-to-Air, UAVs, SCADA, computers, IEDs and so on.

Operationally, EW and CNO/Cyber can and should collaborate to generate very desirable effects. For example, an airborne EA platform can deliver a computer network attack that can take down a radar for a very long time without having to find and revisit this target every day (as would be done with EW working alone). But most of the time, the warfighter just needs EW or he just needs CNO. Just because EW and CNO can and do collaborate some of the time, it does not mean they need to be collocated within the same Cyber organization where they will compete for budget and resources. Simply put, EW supports Cyber the same way it supports other Domains – by providing Spectrum Control. But EW (that is, the broad and enduring requirement for Spectrum Control) is not part of Cyber.

In the final analysis, Joint EW will remain an articulated mission area if it is to provide its maximum warfighting value (in the form of Spectrum Control), evolve and truly adapt to battlespace demands. 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 information technology infrastructure (ITI) management, or Operations in Cyberspace. The simple logic follows: All military activities require reliable access to the Spectrum; friendly Spectrum access is provided and protected uniquely by Joint EW; and effective Joint EW can derive only from undistracted, undiluted joint advocacy and expertise.

### WHERE ARE OUR “EFFECTS-BASED CAPABILITIES”?

EW has landed in its current disorganized and weak situation in large part because the Services, legitimately pursuing their individual mission statements and visions, have been allowed too much freedom to conceive EM capabilities and processes that they have built to meet their own individual needs, visualizing the “next fight” from their specific perspectives. The Services then push these EM capabilities and processes into the “joint” battlespace with the best of intentions, and with the secret hope that their EM solutions and processes become the warfighter’s favorites. Expressed plainly, joint warfighters require effects, as opposed to capabilities; Joint EW effects are delivered as a function of capability and capacity, and one magic box in the STO (special technical operations) closet is not enough. Achieving Spectrum Control is more complex than this in terms of technology, process coherence and human skill.

There has been a historical shortfall in joint harmonization of EW, beginning at “effects required” and traveling backward to EM-compatible and interoperable EW systems developed by the Services. So what formally chartered and appropriately resourced joint agency is able to meet these expectations for persistently bridging this gap? An expert agent with operationally current and durable joint EW perspective is essential to marshal

shared EM processes from the top, determining joint warfighting effects requirements and then translating them down to the Services through JMETLs (joint mission-essential task lists) and resulting METLs to cause a systemic upward "pull" for fully compatible and interoperable EM capabilities and processes. This is supposed to be happening now, but due to a lack of dedicated joint EW advocacy, the DOD isn't achieving this, practically speaking. Under objective scrutiny, we will continue to find that ad hoc, periodic and/or Domain-, Service- or platform-centric solutions are counterproductive, due to the false executive expectations of remedy they invariably create.

### PROGRESS AND SUCCESS IN THE EW COMMUNITY

Our shortfall in achieving joint harmonization does not mean EW has not made progress in recent years. Here are a few leading examples of recent EW successes within the DOD.

- Army commitment to EW as a new core competency
- USN investment in Army EW (JCCS-1, NAVEODTECHDIV, etc.)
- EM RED TEAM Growth and EW Spiral to IO Range
- Advocacy: PACOM EW Ops Assessment and the JCS "EW Tank"
- Electronic Target Folders (ETFs) and EW JMEM development
- OSD (AT&L) EW Joint Analysis Team (JAT) establishment
- USN "Next-Generation Jammer" Program
- Joint EW Planners Course and the "Joint EW Training Summit" serial
- Next-Generation EW Integrated Reprogramming System (NGES) Database, replacing legacy EWIR Database
- OSD (AT&L) EW Roadmap
- Vice Chairman Joint Chiefs of Staff EW Capabilities-Based Assessment task to USSTRATCOM

True success in the future will be based not only on our ability to characterize joint warfighting effects and work backward to harmonize the Services' efforts, but also to take these and other very promising opportunities and weave them together into a new cultural baseline of joint coherence.

### THE WAY AHEAD FOR JOINT EW

Our new EW processes must be adaptive, focused and anticipate the realities of change and resistance. They must take into account not only COTS evolution, weaponization and availability, but also the potential for hybrid COTS and GOTS adaptations to employment. We must commit to deconstruct, redesign and streamline existing joint EW and EM processes to make them adaptable and maintain our increasingly challenged lead in the battlespace.

The chairman of the Joint Chiefs of Staff needs one empowered, globally aware but operationally-focused joint EW executive agent who can inspire Service and Combatant Commander (CO-COM) process coherence and organically provide informed and operationally sound acquisition recommendations. Ultimately, threat trends and warfighting trends in the EM battlespace dictate that this consolidation of expert joint EW authority must occur. With the impending US administration change and the near

When so much is on the line...

**RELIABILITY** is the **only** deliverable

**At Comtech PST, we know what's at stake.**

That's why we build the best Solid State, High Power Amplifier Systems in the business...reliable power that leads to mission success, no matter what the odds. And we deliver it whether on the ground, at sea, or in the air.

- ▲ More effective jamming through Comtech PST/Hill Engineering's fast switching technology
- ▲ Frequencies from 1 MHz to 6 GHz
- ▲ Output power from 5 watts to 30 kW
- ▲ Meets MIL environmental specs

**Find out more about customized solutions you can rely on at:**

**COMTECH PST** TM

**Reliability, Proven Under Fire**  
105 Baylis Road, Melville, NY 11747  
Tel: 631.777.8900 • Fax: 631.777.8877  
E-mail: info@comtechpst.com  
Web: www.comtechpst.com

Comtech PST/Hill Engineering  
417 Boston St., Topsfield, MA 01983  
Tel: 978.887.5754 • Fax: 978.887.7244



ISO 9001:2000 / AS9100:2004 - 01

1.5 MHz-3GHz  
1 kW Power Amplifier System



## Joint Electronic Warfare...

Attack, Exploit, & Defend the Spectrum in Five Warfighting Domains



EW as Global Spectrum Control do it for us. Borrowing words from perhaps our first and certainly most renowned electronic warfare officer, Albert Einstein, "We can't solve problems by using the same kind of thinking we used when we created them." Amen. ✈

*\* Author's Note: The following article represents the views of the author only and is not meant to represent those of US Strategic Command, the US Air Force or the Joint Information Operations Warfare Command (JIOWC).*

*Lt Col Jesse "Judge" Bourque is the director of operations for the Joint EW Center (Lackland AFB, TX). He served for 15 years as an Electronic Warfare Officer in and associated with Air Force Special Operations Command through 2005, amassing 300 hours of combat time in the AC-130H Spectre Gunship and the MC-130H Combat Talon II. Prior to assuming his current position at the JEWCC, he served as Director of Electronic Warfare in the Iraq Theater of Operations, Multi-National Corps Iraq.*

certainty of increased budgetary scrutiny and restraint, we must, as the joint EW community, optimize our shared processes, capture any efficiencies we can and dictate our own recapitaliza-

tion from within. These efforts must be undertaken among EW experts to ensure duplication is minimized across the Joint Force, lest "others" less wise in the true requirements of coherently applied

## WHY EW IS NOT PART OF CYBERSPACE

The ability to defend Cyberspace is critical to our nation and Cyberspace itself carries intrinsic significance. However, the sense of importance bestowed on Cyberspace has also led to the potentially damaging misconception that Cyberspace might also include the whole of the Electromagnetic (EM) Spectrum. In truth, Cyberspace traverses infinitesimally small portions of the EM Spectrum and does not incorporate the electronic warfare (EW) mission area charged with protection of this Spectrum.

*"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." (National Security Policy Directive 54)*

*"Operations in Cyberspace 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 and support operations in Cyberspace, but are not operations in Cyberspace per se, merely due to their use of the Domain." (Principal Undersecretary of Defense)*

The message defined by our most senior leaders that resonates quite well outside the confines of the US Air Force community rightly characterizes Cyberspace as "information technology infrastructures" (ITI), plain and simple. In this authorized Cyberspace definition, note the conspicuous ab-

sence of any mention of the EM Spectrum. Cyberspace is simply the ITI upon which ours and other nations depend.

Here are some broad substantiating points to consider in recognizing that Joint EW as Spectrum Control transcends the needs and bounds of Cyberspace.

**Spectrum Control is increasingly crucial to all military efforts across all Services and within all five Domains.** If any one customer (or Domain) is allowed to exercise ownership of Spectrum Control, a bastardized version of it will be grown to ultimately favor only that Domain. EW, as the foundation of Spectrum Control, does not belong solely to the Air, Sea, Space, Ground or Cyber Domains. EW supports all of them and must remain fully available to each of them.

**All military activity depends directly or indirectly on EM Spectrum availability.** We can either coherently provide for it in all Domains or just hope it's there when we need it. If we resort to hope, Spectrum won't be there; adversaries are now planning to take it away. Cyber, with its focus on ITI, is not inherently concerned with the entire EM Spectrum or Spectrum Control.

**Joint EW is Global Spectrum Control.** Joint EW is the DOD-coherent formation of shared EM/EW capability and process development. EW is not just a CREW box or an airborne jamming pod; it is a global effects requirement. Joint EW is "actions taken" to exploit (ES), harden (EP) or deny (EA) the Spectrum for our use.

**EW is (absolutely) not Cyber, but it can support Cyberspace Operations.** Cyber is computer network operations (CNO) expanded to encompass military/government/commercial computer networks. EW guards the Spectrum and is employed in a variety of roles across all Domains. The majority of Cyber is outside of EW operations, just as the majority of EW does not support Cyber. EW operators have operational context and experience. "Net warriors" have "tools."

**Cyber (CNO) is not a replacement for IO.** The two are completely different. Cyberspace operations exert control over ITI, whereas IO is a cross-capability integrating strategy for optimized cognitive effects.

**Some EW and Cyber target sets may overlap, but key attributes differ sharply.** Authorities required for CNO are stratospheric and cannot be levied on EW. Spillover and probability of unintended effects from CNO are considerably higher than from EW. The maturity of these two mission areas is very different. Cyber is still finding its legs, while EW is 60 years old. The skill set for Cyber/CNO is still formally undefined, while EW has its own joint planning and manpower base. The pipeline for Cyber manpower is not yet established, while EW schools exist for all four Services.

**Cyber is "meta-CNO" is "network warfare" is NSA is Title 50.** This is a simplified depiction of Cyber traced back to its apparent roots. As an operational mission area (within USC Title 10) that directly supports the warfighter, responsibility for EW as Spectrum Control cannot be permanently subordinated to an organization that is funded for and focused on intelligence collection and analysis (within USC Title 50). Although both activities (i.e., "camps") are fundamental to mission accomplishment, their aims are often diametrically opposite – the Title 50-funded requirement "to collect" within the Spectrum versus the Title 10-funded operational requirement "to deceive, degrade, deny or destroy" within the Spectrum and its supporting infrastructure. These two camps must be continually reconciled via balanced exchange and collaboration, not assimilation. If the Cyber camp is given control of EW, EA and ES will be institutionally subordinated to the national collection mission at the highest levels, and funding (or lack thereof) will quickly follow suit.

**EW previously was subordinated to C2W, then IW, then IO and now Cyber (within the Air Force).** Who will make the grab for EW next? How many iterations of the same drama should Joint warfighters expected to endure? Clearly, it is time to allow EW, as Spectrum Control, to evolve and flourish based on its decades of proven merit and strong future relevance.

Another important distinction is the difference between operations *in* Cyberspace and operations *into* or *through* Cyberspace. An EW operation, such as locating and disabling (with jamming or HPM) a cell phone used to trigger an IED, generates an effect against a target within Cyberspace. However, this does not make it a Cyber operation. It is an EW operation into Cyberspace. This example is no more a Cyber attack than if the cell phone were disabled by dropping a 500-lb. "dumb" bomb on it.



## AOC Professional Development Courses

Obtain the knowledge that can help you advance your career.

### Upcoming courses

**Intercept of Stealth Radar Signals**  
September 16-19

**ELINT and Modern Signals**  
September 23-26

**Interpretation and Use of Real-Time UAV Video**  
October 1-3

**Wideband Digital Receivers**  
October 7-9

**Fundamental Principles of EW**  
October 14-17  
Reno, NV

**EW Project Management**  
October 19  
Reno, NV

**Radar for EW Engineers**  
October 19  
Reno, NV

**Angle Jamming**  
October 24  
Reno, NV

**Introduction to Radar and EW**  
November 4-7

**Writing Solid CONOPS for US Government Programs and Projects**  
November 18-20

**Multi-Sensor Data Fusion**  
December 2-5

All courses offered at AOC Headquarters in Alexandria, VA unless otherwise noted. Onsite classes available.

Visit [www.crows.org](http://www.crows.org) for more information.

## VISIT THE NEW AOC JOB BOARD at

  
[www.jobs.crows.org](http://www.jobs.crows.org)

With its focus on companies and professionals in the fields of electronic warfare and information operations, the AOC Career Center offers its members, non-members and the industry at large an easy-to-use and highly targeted resource for online employment connections.

### ***For Job Seekers:***

- FREE and confidential résumé posting
- Job search control
- Easy job application
- Saved jobs capability

### ***For Employers:***

- Unmatched exposure for job listings
- Easy online job management
- Résumé searching access
- Build better company awareness

**BOXWOOD**  
REAL REVENUE. REAL RELATIONSHIPS. REAL RESULTS.

***Begin shaping your  
professional future  
now at [www.jobs.crows.org](http://www.jobs.crows.org)***

Here is a suggested definition of Cyber that distinguishes between operations in Cyberspace and operations into or through Cyberspace:

“Operations in Cyberspace” are computer-based actions taken to attack and exploit adversary information technology infrastructures (ITI) while defending and maintaining friendly ITI and the data within them. These operations may include disabling, corrupting or destroying adversary ITI or employing friendly ITI to convey cognitive content intended to influence, corrupt, disrupt or usurp adversary human and automated decision-making processes while protecting our own. These operations do not include “Operations into Cyberspace,” consisting of military operations (such as EW, PSYOP, physical attack, etc.) that may create and deliver informational, kinetic or spectral effects into or through Cyberspace and support operations in Cyberspace, but are not “Operations in Cyberspace” merely due to their application within or support to the domain.

The reasoning behind the distinction drawn in the above definition is to separate that which is a truly intra-Cyberspace operation from that which is a different mission but overlaps, targets or traverses the Cyberspace area of responsibility. Additionally conveyed within the same DEPSECDEF memo referenced earlier, “Other military operations (such as EW, PSYOP, physical attack, etc.) may create effects within or through cyberspace and support operations in cyberspace, but are not operations in cyberspace per se merely due to their use of the domain.” This was arguably the DEPSECDEF’s vote to maintain the enduring soundness of pre-existing military operations launched from within the other four warfighting domains, the EM environment and the information environment to prevent them from being erroneously grouped by the temporary effects they realize. Though effects are critical, they are transient and it is the capabilities and mission areas (i.e., EW, PSYOP, etc.) that deliver them that are enduring and must convey their enduring identity for DOTMLPF purposes.

Using the above definition, a computer-delivered CNA against a telecommunications router to intercept a telephone call would clearly fall within the bounds of “Operations in Cyberspace.” However, EA-6B jamming attacks against an SA-15 tracking radar, EA suppression of adversary C2 networks, directed energy attacks intended to “fry” critical server circuit boards or laser attacks against a satellite’s IR/EO apertures would clearly fall outside of Operations in Cyberspace, although effects could or would be registered within friendly or adversary Cyberspace (“operations into Cyberspace”).

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 ITI management or Operations in Cyberspace. Joint EW must never be subsumed by the Cyber mission area or EW will only evolve in those areas (EA, for example) that support attacks against the ITI, while many other EW areas (ES, EP and IRCM, for example) will languish. All of these areas of EW are needed to serve our five warfighting domains, including Cyberspace.

– Lt Col Jesse Bourque