Future Electronic Attack: Coherent, Distributed and Cheap – JED, May 2019

– By Lt Col Jeff "Seed" Kassebaum –

Air and Space Superiority is impossible without Electromagnetic Superiority. For airpower missions, the first objective is usually "Gain and Maintain Air Superiority." However, the implied task is first to gain and maintain Electromagnetic Superiority…unless we concede that we can achieve our first objective by BFMing as singles while NORDO (impossible).

In August 2000, the Joint Chiefs of Staff established the Joint Airborne Electronic Attack (AEA) program as a temporary solution to establish a cadre of Airmen skilled in offensive electronic attack following the retirement of the USAF's EF-111A, and until a follow-on asset could be fielded. The Joint AEA program is executed in partnership between the US Navy's Electronic Attack Wing and a single USAF Squadron at Naval Air Station Whidbey Island, WA. In 2004, the USAF removed pilots from the program, and from 2004-2017, the USAF relied on a small group of second- and third-assignment Electronic Warfare Officers to maintain a skillset in offensive electronic attack for the Combat Air Force (CAF). To date, the USAF's 390th Electronic Combat Squadron at NAS Whidbey Island, a geographically-separated unit of the 366th Fighter Wing at Mountain Home AFB, Idaho, continues to be the sole source of Fighter Electronic Warfare Officers for the US Air Force, producing eight per fiscal year.

In 2015, Air Combat Command and Commander Naval Air Forces agreed to return USAF pilots to the Joint AEA program. With the support of the USAF Vice Chief of Staff, the first pilots

started to arrive in October 2017. One of the USAF's first Electronic Attack Fighter Pilots employed his weapons system in anger last November against ISIS. (No offense to the EF-111A community, but I'm defining an electronic attack fighter as possessing an air-to-air capability.)

The important questions for the USAF are, what will the understanding of Electromagnetic Superiority look like when those first pilots are leading Fighter Squadrons? How will the USAF evolve in how it executes Electronic Attack (EA), specifically?

CONCEPTUALIZING ELECTROMAGNETIC WARFARE

The intent of this article is to conceptualize how we, the USAF, should be thinking about Electromagnetic Warfare against the full scale of threat: from individual engagements to Integrated Air Defense Systems (IADS). I use the term "Electromagnetic Warfare" as a more accurate term than "Electronic Warfare," because it focuses on the domain in which we operate rather than the "electronic" devices used to fight in this domain. Additionally, I intend to refrain from buzzwords (i.e., family of systems, EW Battle Management, 3rd Offset, etc.), because they become meaningless after a few years when the novelty wears off.

See **Figure 1** to conceptualize Electromagnetic Warfare on a horizontal scale ranging from "offensive" to "defensive," against a vertical threat scale ranging from a single engagement to an Air Defense System.

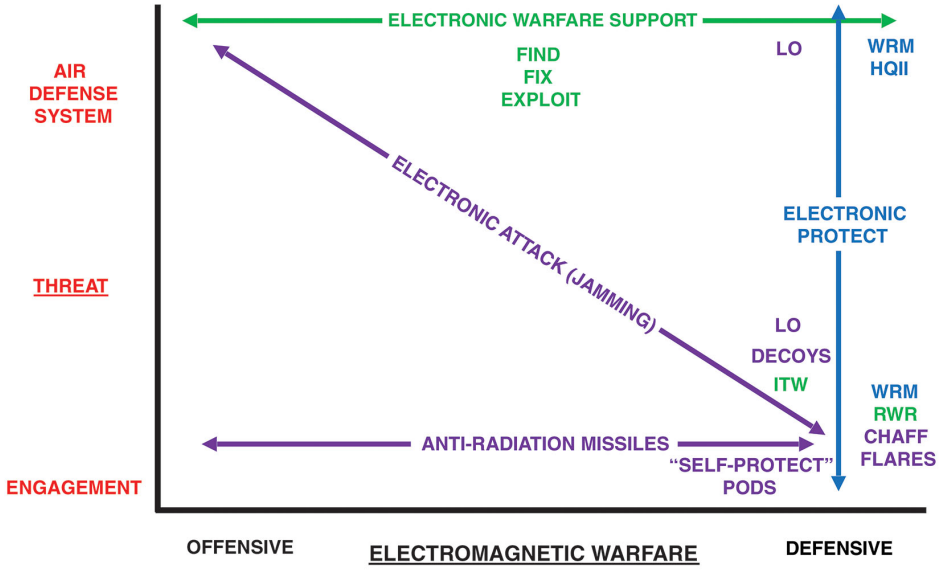

Figure 1: Electromagnetic Warfare versus Threat Scale.

All purple references are electronic attack, whether lethal (anti-radiation missiles), non-lethal (jamming), active (jamming, decoys, flares), or passive (LO, chaff)1. Electronic Attack (probably should be Electromagnetic Attack, but one step at a time) must attack the threat using offense and defense. Offensive electronic attack focuses on the threat system, the IADS – whether it uses organic cueing or non-organic cueing – to allow Blue (friendly) forces access to what Red (enemy) holds valuable. Defensive electronic attack focuses on defeating the threat in the end game, after the IADS has been able to develop and engage a track. These defensive electronic attack capabilities are often poorly termed “self-protect” pods, but are inherently defensive in nature.

Electronic warfare support (ES, green) largely focuses at the threat system level, except when performing Imminent Threat Warning (ITW), which is at engagement level. Radar warning receivers (RWR) are also purely at engagement level…no RWR gear cares if a NEBO is looking at it, for example.

Electronic protect (blue) is our capability to prevent the threat from using electronic attack against us by using War

Reserve Modes and frequency/waveform agility in radar and communications (Have Quick II).
The USAF has been successful in Low Observable technology (passive electronic attack) and anti-radiation missiles (lethal electronic attack). Where we have ceded capability for our strike packages is in offensive electronic attack against the threat system, relying on a sister service (the US Navy) to execute much of the requirements in Combatant Command Operational Plans. When the USAF does use offensive electronic attack, it means either the too few EC-130H (EC-37B sometime in the future) or Aggressor EA pods at training exercises.

So, the status of things in 2019: offensive EA for Aggressors, defensive EA for Blue strikers. We are not only missing a capability to be sufficiently "Offensive Electromagnetically," but we are looking at only a small portion of the Electromagnetic (EM) Spectrum.

WE ARE BEHIND

We cannot continue to execute airpower while being defensive. We must move beyond our 1980s mentality of hiding in the EM Spectrum – we have run out of places to hide. Additionally, we must not rely solely on defensive electronic attack; why wait for an engagement and then defend against it? Why surrender that decision making space (or time) to Red? (Boyd). As an analogy, imagine a strike package without Offensive Counter Air; we would not plan for our strikers to ingress to the target area and just keep dodging air-to-air missiles on the way, then drop and egress. We need an offensive counter to the air threat for the same reason we need an offensive counter to the electromagnetic threat (the IADS Kill Chain is the threat). Today's US Air Force, with its limited offensive electronic attack capabilities, expects our strike package to ingress while the IADS processes plot returns, sends plots through filter centers, develops tracks, then engages the tracks while our defensive electronic attack capability defends in the end game. Defining "limited" with specifics is

more appropriate in another venue. However, the fight in the Electromagnetic domain extends from below VHF all the way up to Millimeter Wave frequencies.

Further, when prioritization is given to defensive over offensive systems, we put ourselves in reactive instead of proactive situations. Tactically, this means we have added variables we cannot accurately account for in mission planning. Additionally, we are, in essence, planning to be engaged and relying on "faith" that defensive electronic attack – coupled with maneuvers, chaff and flares – will defeat an engagement.

We should conceptualize non-lethal electronic attack (jamming) the same way as lethal electronic attack (ARM) – there are three types: reactive, pre-emptive and proactive. Reactive employment of ARM is a defensive tactic, whereas pre-emptive and proactive ARM employment are inherently offensive. In short, the difference between the two offensive types: pre-emptively targeting a known threat versus targeting a previously unknown threat that has become known and will be factor in the future (but is not a threat upon discovery).

Pre-emptive targeting: Strategic SAM near target area hasn't moved in weeks; in mission planning, we develop a gameplan to target with offensive electronic attack and ARM, and we execute this plan after mission planning is complete.

Reactive targeting: There are tactical SAMs roaming around in vicinity of the target area; while the strike package is attacking, a tactical SAM pops up and targets strikers within its missile engagement zone (MEZ). Those strikers are now being defensive – reactively targeting the SAM to protect the defending strikers.

Proactive targeting: There are tactical SAMs roaming around in vicinity of the target area; before strikers have ingressed, a previously unlocated SAM pops up near the target area, which

will be a threat to strikers *in the near future*, so that SAM is targeted offensively, before strikers are defending, because the threat *will* be a factor if not proactively targeted.

So Figure 1 should be modified. See **Figure 2** to conceptualize both non-lethal and lethal electronic attack in offense and defense.

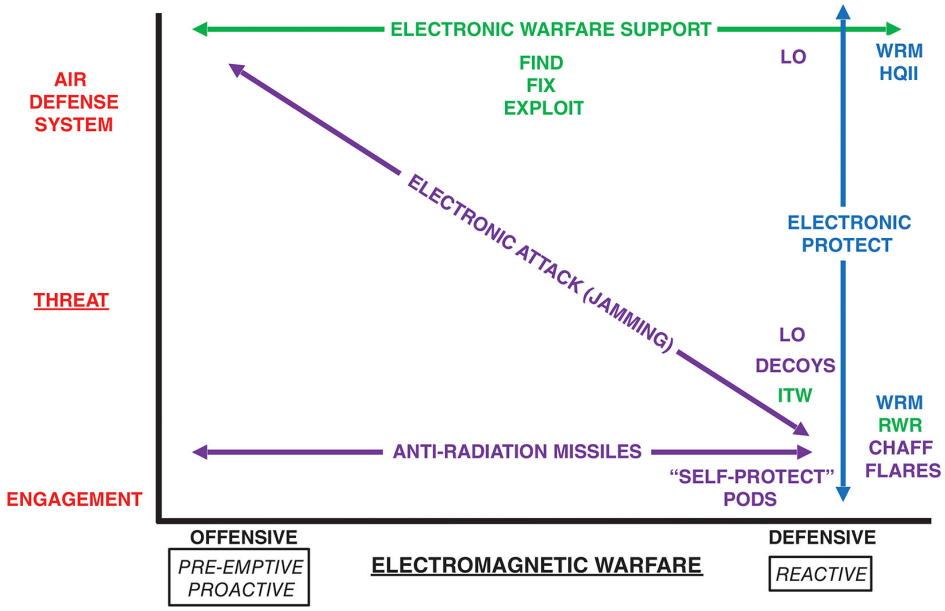

Figure 2: Electromagnetic Warfare Targeting versus Threat Scale.

What is our plan to counter and attack Red when the IADS moves to bi-static, multistatic, and passive detect track management and millimeter wave track engagement? These are not physics problems. These are solvable technological problems that are complimentary to the fundamental principles of multi-axis attack and saturation.

Anyone can point out where we are deficient. How we focus on addressing our deficiencies is far more important. What should the USAF look like in Electromagnetic Warfare when our first electronic attack fighter pilots lead squadrons (~2032-2035)? How do we make Red use greater resources to counter our effects in an IADS?

If we shift from reliance on dedicated offensive electronic attack platforms to distributed, linked and coherent electronic attack among our strike package, we can force the threat to increase their investment in track management and track validation. Distributed systems across a strike package also imply the inherent power advantage of proximity to threat receivers – reduced dissipation from free space path loss. We could use bistatic, multistatic and passive detect capabilities to our advantage; overwhelm the system with coherent targets and cripple the system's processing and decision-making capacities. A new kind of saturation. The key piece is focusing earlier in the adversary Kill Chain before the threat can get to the engage stage. Coherent waveforms designed to get past the filter center are a superior system-level attack and reduce the effectiveness of engagements later in the Kill Chain.

Further, we need to shed the concept of electronic attack as the job of a dedicated weapons system. The Electromagnetic Spectrum is an expansive domain, and electronic attack must be distributed throughout the strike package. We do not have a singular, dedicated jet that carries the AMRAAM; they are distributed across multiple weapons systems. The same should hold for electronic attack, and for the same reason, the threat.

LONG(ER) RANGES

The reach of current and near-future surface-to-air threats must push our thinking about electronic attack away from brute force, largely due to power dissipation rates. We *could* focus on technologically advancing a way to make amplifiers/transmitters lighter, smaller and more powerful – a cost-prohibitive evolution. Instead, we should resist fighting the threat with brute force by putting development effort into coherent waveform strategies and techniques. By doing so, we mitigate the reach of Surface-to-Air Missile (SAM) *complexes*; we only need the threat to receive coherent pulses, not raise

an ambient noise threshold – a cost effective revolution.

What does distributed, linked and coherent EA even look like? Attributes we need are cheap, linked devices with a thinking human in the loop somewhere, and augmented with algorithmic predictive targeting. In turn, force the threat into developing more complicated pulses to discern targets – a technological and cost imposition. Force an oversaturation of machine and human, and force Red to divide resources and defend against a distributed, multi-axis attack across the strike package.

If we view Electronic Attack as a Triple Constraint Venn diagram, where we want cheap, coherent and distributed, it would look like **Figure 3**.

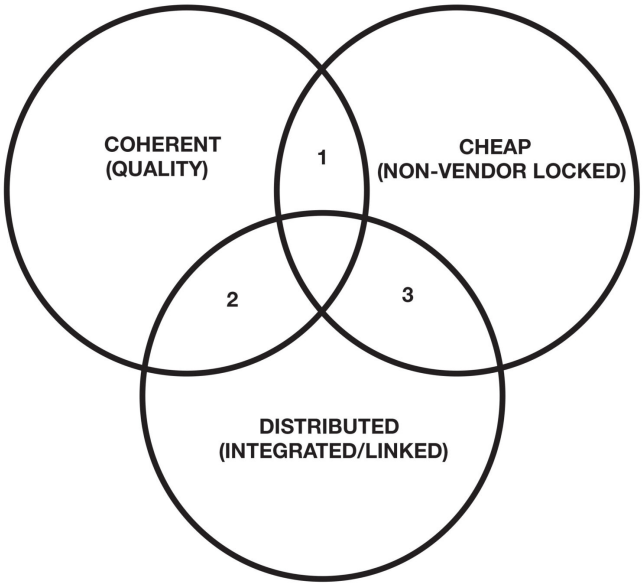

Figure 3: Electronic Attack Triple Constraint.

And, like a Triple Constraint, reality and budget means we get two of the three, but unlikely, all three with finite time and finite resources. The numbers in the overlapping circles signify priority. Best to have cheap and coherent, but above all, coherent. Waveforms that fail to make it through a filter center will not affect the system. Non-coherent waveforms could be successful at the individual threat engagement level, but that works only once those individual threats are isolated

from above-echelon information. We should not anticipate future threat capabilities to have less redundancy in information sharing than they have today.

Further, Figure 3 doesn't just apply to EA; it also applies to ES. Distributed sensors that can discern coherently among assets, flights and packages are necessary to find, fix and exploit the threat. But this discussion is outside the scope of this article.

CHEAP, LINKED, MANNED & UNMANNED

Future electronic attack, even if we use distributed and coherent capabilities, should still not remove decision making from a thinking human (aviator?) in the loop. However, the array of offensive electronic attack must be scalable in order to execute quickly enough to suppress a dynamic IADS effectively.

Day One of a war, we will not have Electromagnetic Superiority – we will have to take it. Exactly where the human is "in the loop" must be based on Red system capability versus Blue capacity. A system with a robust, mobile, redundant threat capability is likely to drive our use of more unmanned assets forward first with a reliance on ES to exploit. As system capability deteriorates, Blue capacity to move the human forward in the battlespace increases. Manned and unmanned is not a "versus" equation, it's a question of scale and capacity.

President Eisenhower's charge against the "acquisition of unwarranted influence," loosely applied to electronic attack, must be weapons system-agnostic, especially in acquisition procurement pipelines. Cheap means the taxpayer must own the software, or the hardware, or both, while still incentivizing industry to compete to meet tomorrow's threat requirements before being overcome by events. Ideally, to best support the warfighter, we need non-vendor locked and open architecture materiel, or we risk losing ground to a more rapidly

developing adversary.

THE FUTURE FOR ELECTRONIC ATTACK

To gain and maintain Air Superiority now, and increasingly so against future peer threats, the Combat Air Force needs Airmen who understand that electronic attack spans offense and defense and must be used against the threat ranging from Air Defense Systems to single engagements. For the last several decades, we have become relatively proficient at the bottom and right side of Figure 1. However, our expertise has atrophied USAF-wide on the upper left of the figure. To be effective, we must execute in a manner wholly different than our previous concept of airpower. Future electronic attack must encompass both offense and defense coherently across a system's processing capability and capacity before engagement.

The good news, however, is the US Air Force's investment in creating more Airmen for the Joint AEA program, who will become experts in electronic attack. No longer is the Joint AEA program only for second- or third-assignment airmen. Now, pilots direct from pilot training and Combat Systems Officers (CSOs) direct from CSO school spend their first three operational years learning electronic attack in the 390th Electronic Combat Squadron. Upon assignment completion, they will go to a USAF weapons system and bring that skillset to more communities in the CAF than ever before. The first cadre of initial assignment airmen include five pilots and two CSOs. Multiple communities in the CAF will benefit from greater and more detailed integrated planning and execution, as well as appreciate the valid dissatisfaction with lack of offensive electronic attack across the CAF. Longer term, as the USAF develops a distributed and coherent way to attack the threat electromagnetically, this cadre of EA experts will inform decision makers. The key point is that future electronic attack is not just about buying a new device or upgrading an old one; it is about building and developing the people with the skillset and background to accurately conceptualize

Electromagnetic Warfare to achieve success in gaining and maintaining Electromagnetic, Air and Space Superiority. ♦

About the author: *Lt Col Jeff "Seed" Kassebaum is the Commander, 390th Electronic Combat Squadron at NAS Whidbey Island, WA, where he flies the EA-18G Growler. He has deployed eight times and fought in three wars. He is an EA-18G Instructor Electronic Warfare Officer, EC-130H Weapons Officer, and has flown over 2,000 hours in the EC-130H, EA-6B and EA-18G.*