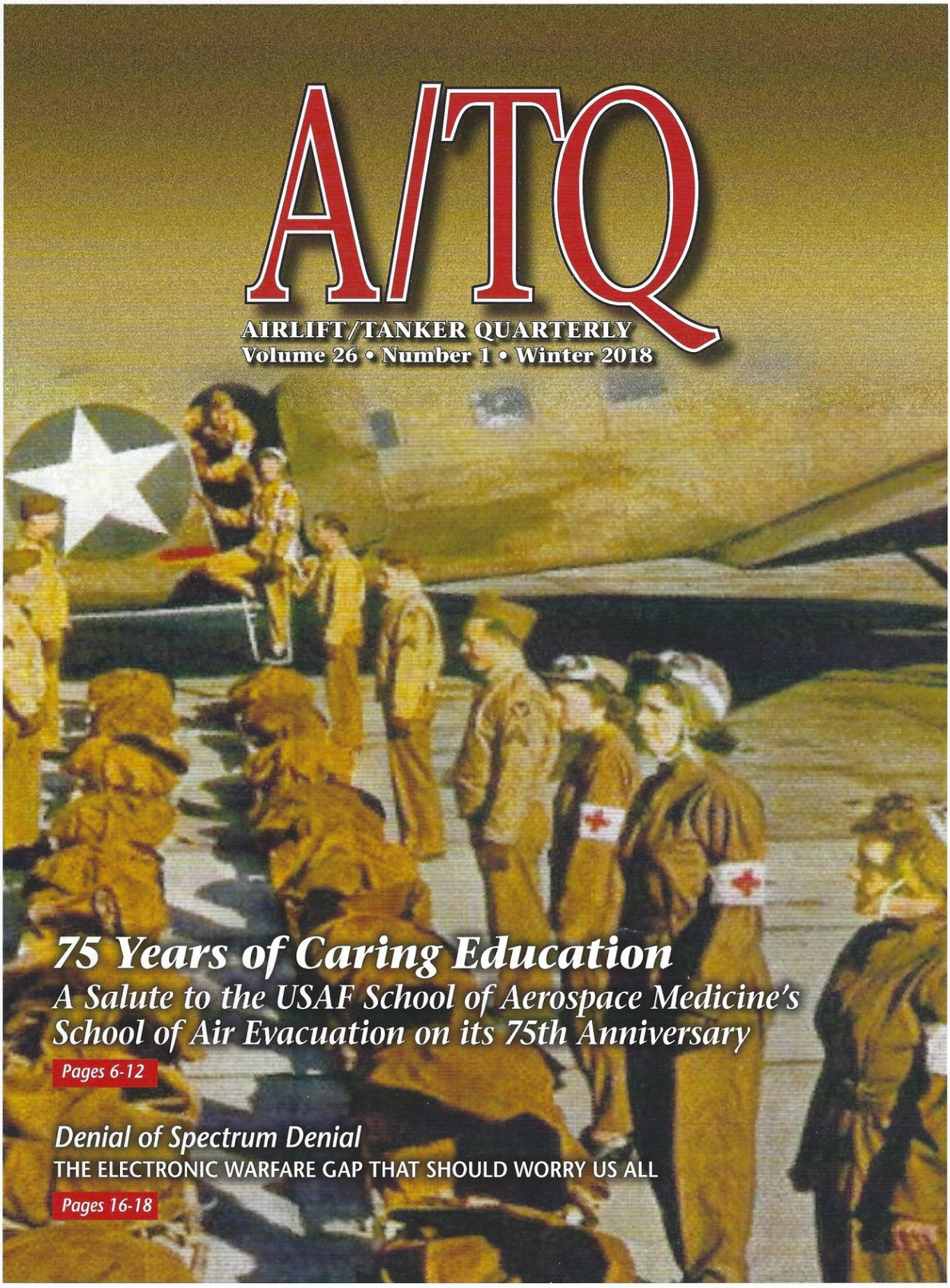
A/TQ

AIRLIFT/TANKER QUARTERLY
Volume 26 • Number 1 • Winter 2018



75 Years of Caring Education

A Salute to the USAF School of Aerospace Medicine's School of Air Evacuation on its 75th Anniversary

Pages 6-12

Denial of Spectrum Denial

THE ELECTRONIC WARFARE GAP THAT SHOULD WORRY US ALL

Pages 16-18

Denial of Spectrum Denial

THE ELECTRONIC WARFARE GAP THAT SHOULD WORRY US ALL

by Steve "Tango" Tourangeau, Lt Col USAF (Retired) and President of Warrior Support Solutions, LLC

The swordsman stepped into the market square and brandished his weapon with swift and impressive maneuvers. He then took his stance, waiting to strike. Indiana Jones took one look at the situation, pulled out his gun, and shot him down before he could strike a single blow. While this is an entertaining scene from a favorite movie, the truth is it will play out for real with the United States and its adversaries in the next engagement; the U.S. thinks it is Indiana Jones with big guns supported by all powerful electronic warfare (EW) and electromagnetic spectrum operations (EMSO). The problem is that when our warriors enter the next fight (supported by our airlift and tankers), we are likely to discover that our adversaries have outpaced us in everything EW/EMSO and that *we* have become that ill-prepared swordsman.

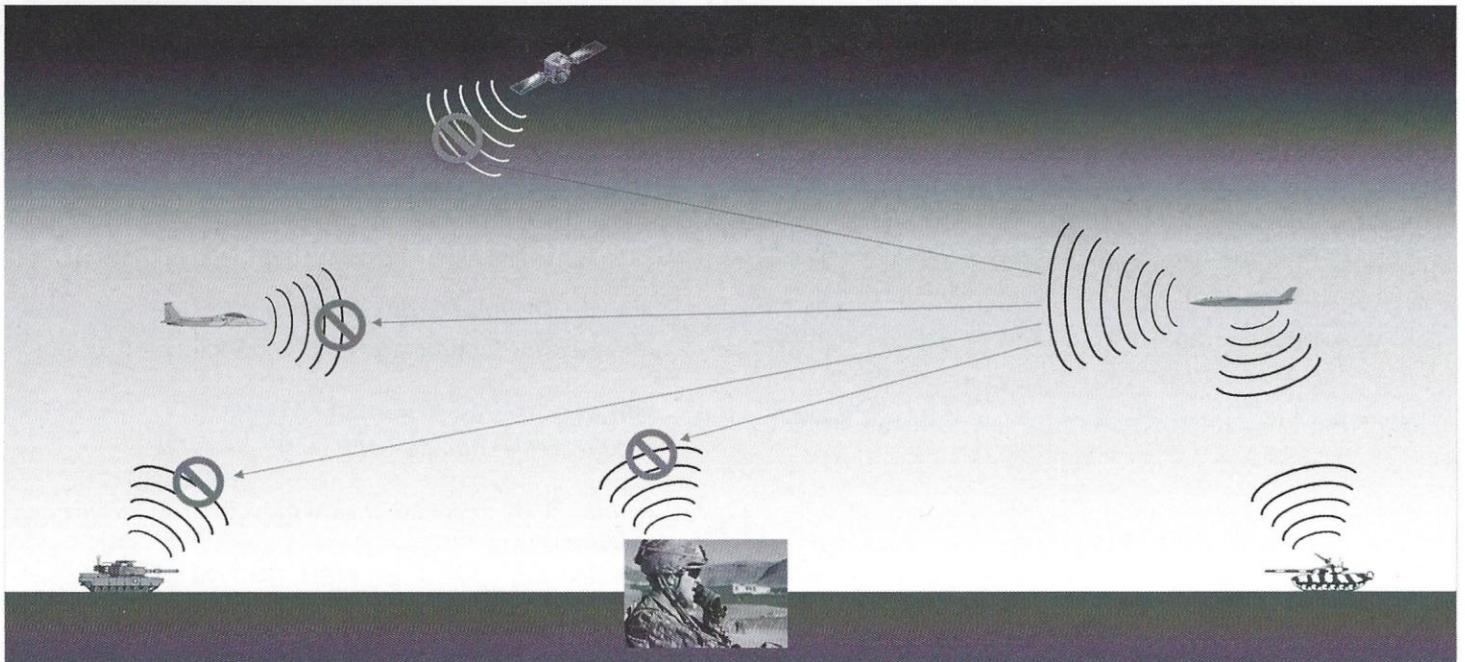
Indy controls the situation in *Raiders of the Lost Ark* (1981). (Courtesy Photo LucasFilms Ltd/Paramount Pictures).

EW/EMSO and the Spectrum

Delivering soldiers, materiel and fuel to the fight cannot be done without "owning" the spectrum. The spectrum, or the electromagnetic spectrum, is the medium through which all radio, radar, cellular, wireless data, visual, and communications signals pass; therefore, it is where EW operates. To use a newer, perhaps more encompassing term, it is the field of EMSO. The spectrum is categorized by frequencies and wavelengths, and each device we (and our adversaries) use (that is not connected to a wire) uses frequencies in the spectrum to transmit and/or receive signals in the form of radiated energy. It is what enables radar and radar jamming. It is what enables communications and communications jamming. Navigating and navigation jamming. In short, with it, we win. Without it, they win.

Denial of the Spectrum

For the last 25 years, the Air Force has operated with impunity in the battlespace, with virtually 100% spectrum availability. Confident in that conclusion, the Air Force abandoned its Cold War tactics, techniques, and procedures (TTPs) and migrated to policies, plans, and procedures that are 100% reliant on availability of the spectrum. Then there was the wakeup call: counter-IED fratricide resulted in our own communications channels being jammed, prohibiting us from communicating with our own forces. It came down to protecting the troops, or communicating. We had not trained to operate "comms-out". We shut off our jammers and we got blown up. This was a specific, battlefield situation in which we were denied use of the spectrum because we had been denying the possibility that it



Electronic Warfare (EW) is any action involving the use of the electromagnetic spectrum or directed energy to control the spectrum, attack of an enemy, or impede enemy assaults via the spectrum.

Spectrum Denial can render various systems ineffective.

(Warrior Support Solutions image).

could happen and therefore did not prepare for it. That loss serves as a critical foreshadowing of what engagements on any scale could turn into: spectrum denial and heavy loss...*for us.*

Spectrum Denial Events

Other world events have demonstrated just how far various adversaries have advanced their ability to jam our communications, block our data links, jam GPS signals (or even worse, spoof them) resulting in the loss of situational awareness, communications overall, and our ability to navigate. Remember the two recent incidents with Iran taking over our stealth drone, and the Navy vessel that drifted into Iranian waters? This is just speculation, but it is possible that both of those events were caused by denial of, or manipulation of, spectrum. Perhaps worse than not knowing where you are, is believing you are somewhere you are not. And last but not least, our critical radar operations such as acquiring aircraft positions, guiding missiles, and air-ground mapping would be severely impacted. It goes without saying that we would be less effective with our own jamming signals, just adding more confusion to the mix.

Let's look at the activities of our most sophisticated adversaries: Russia and China. Neither country has been saddled with the expense of the Middle East wars (even though Russia has certainly been active to some extent in Syria). Therefore, they have had the luxury of being able to direct significant resources to non-kinetic warfare research, testing and real-world spectrum commandeering activities, as follows:

Russia

Russian EW capabilities were well demonstrated during the country's invasions of Georgia in 2008 and Ukraine in 2014. In Georgia, Russian forces conducted a full-spectrum offensive to deny the use of radio waves as well as to prevent the use of the Internet within the country. As a result, the Russian offensive blinded the Georgian military and reduced drastically their command and control capacity.[1] A BBC article stated that "In the combat in eastern Ukraine, electronic jamming by specialized Russian units has been highly effective. Indeed, Russia has won the battle in the electromagnetic spectrum hands down."[2] And an article in The Diplomat stated that "The United States has been criticized for ignoring the rapid development of Russia's SIGINT and EW capability, which was put on full display at the onset of the Russian invasion into Crimea and east Ukraine, as Ukrainian cell-phones and communications equipment fell silent to Russian jammers."[3] Lt. Gen. Ben Hodges, commanding general for U.S. Army Europe, stated "We've seen the Russians display in Crimea electronic warfare capability at a tactical level that we absolutely don't have."[4]

China

An article in C4ISRNET.com stated that "China's efforts in the Pacific theater can be viewed under similar pretenses as Russia's projection of power and use of jamming capability." In addition to the nation's impressive and growing EW capabilities, China's very long geographic reach (A2/AD) could deny us the use of what capabilities we do have. No more proof is needed than their successful efforts to build islands in the South China Sea that extend their defense perimeter and provide a forward operating area that threatens the U.S. operational area as well as our network of alliances. The article concluded by stating that China's EW capabilities could also be used against less sophisticated nations such as Vietnam, India, Taiwan or Japan, and could complicate those nations' abilities to command and control their own forces.[5] And a New York Times article reported that "China successfully carried out its first test of an antisatellite weapon" by targeting and destroying one of their aging weather satellites, suggesting they can now destroy American communications and GPS satellites.[6]

Other Threats

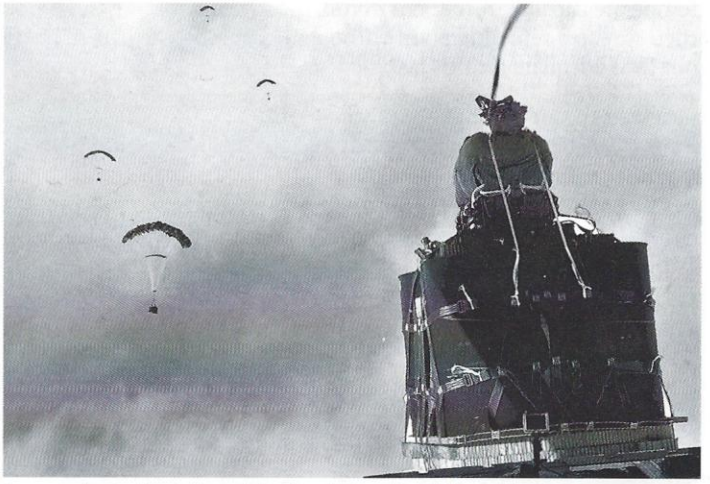
We already talked about Iran commandeering a drone, and possibly causing one of our mighty naval ships to drift into our adversary's waters. Early in the Gulf War, IED's disrupted our pervasive advantage in theatre, and got a lot of our warfighters killed. Violent Extremism employs suicide bombing, which denies everybody a chance to engage in some kind of fair fight. Enough said. And, before we leave this topic, here is something else to consider: Civil encroachment. Yes, our operations will be hampered by edicts both CONUS and abroad. As I write, portions of the spectrum are being sold off to the commercial enterprise. This means that testing and training our systems in the U.S. will have to move to other sections of the spectrum, so as to not deny spectrum to the new rightful users: American citizens. OCONUS, we cannot just show up to the fight and flip on the switch. We will aggravate local civilians if we block their ability to use their cell phones, and the Internet. We would have another enemy on our hands, then.

Denial of Spectrum Denial

Consider the impact to operations if the U.S. is forced to operate in a denied spectrum environment:

- Do we have TTPs in place to operate comms-out?
- If GPS is being denied or spoofed, can the current crew skillset get the mission done?
- Have we been adequately training for such scenarios?

No. Not even close. This truth paints an even grimmer state of affairs: An entire generation of warfighters has enjoyed unfettered access to the spectrum, and this has resulted in the assumption that



A parachute bundle with the Joint Precision Air Drop system is dropped from a C-130J Hercules to a remote Forward Operating Base, 27 November 2011. The JPAD system uses a GPS navigation system to guide parachute bundles to precise drop zones, minimizing collateral damage, troops' ground travel, and the vulnerability of the aircraft. However, the success of this mission is 100% dependent on availability of spectrum. (U.S. Air Force Photo/SrA Tyler Placie).

the spectrum will always be available. As proof, the Air Force continues to develop capabilities (from systems to TTPs) that are more and more dependent on spectrum availability, and yet, little to nothing is being done to ensure our access to it. This, then, results in a dangerous condition known as Denial of Spectrum Denial (DoSD), in which we attempt to prevent (to deny) the other side's use of the spectrum but they block (deny) our abilities resulting in them owning the spectrum and the day.

A perfect example of the risk of Denial of Spectrum Denial (DoSD) of the Army's Joint Precision Airdrop System (JPADS). It is a laudable capability to be able to air-drop GPS-guided palettes of critical supplies to their target. However, the success of this mission is 100% dependent

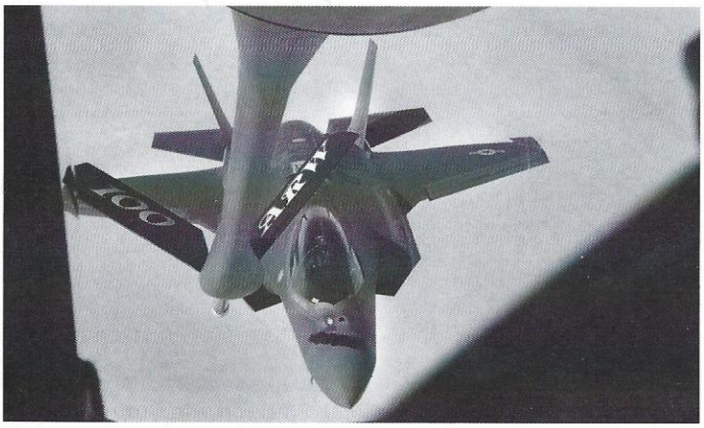
on availability of spectrum. To have developed this capability without a backup plan, namely, when the GPS signal is jammed or spoofed, is really short-sighted. To train for this mission with GPS available 100% of the time puts our crews at risk.

Preparing for Denial of Spectrum Denial

To drive this point home, it is possible that you, the reader, are frequently in Denial of Spectrum Denial. Suppose you are going to visit somewhere that you've never been before. You obtain the address, and say to yourself, "I'll just plug it into my GPS." Do you also print out a copy of the directions from mapping software to bring as a backup? And, do you also have a Rand McNally™ Atlas in your car, and know how to read it and use it? If not, what will you do if the area has poor coverage and you cannot get satellite reception? Your GPS just conked out; now what will you do? It may not be so bad if you are just going to visit a friend, but what about our warfighters in theater? You can be sure the impact to our troops is much graver. If the TTPs and training scenarios are not in place to operate in denied spectrum, then we are denying the possibility of it even happening. We need to reform this thinking, and we need to do it fast. Let's start with asking some questions for two key areas of mobility operations.

1. Training

Do we conduct training scenarios for tactical ops without GPS, or ground-based navigation aids? Can we continue to fly airdrop/airland sorties with crews that are not adequately trained to conduct the mission when GPS is denied? Are our pilots adequately trained for denied spectrum environments, and are they proficient enough to operate capably in that environment? Can any of our crews find their way to a refueling point without GPS or air-to-air TACAN? Are our INSs adequate for this task?



Fighter pilots have three RF-spectrum-dependent methods to use in-flight in order to find their tanker. One way is to use the tanker's tactical air navigation system (TACAN) channel to provide directions. Other ways include GPS coordinates, and onboard radar. Once again, however, being able to use these systems successfully is 100% dependent on availability of spectrum. (USAF Photo).

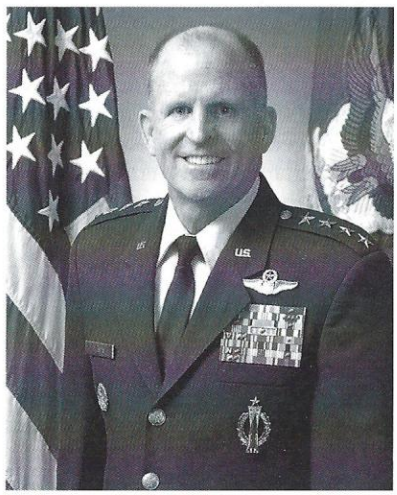
2. Command & Control

Do we have policies and procedures in place to enable operations without comms for C2? Do we have adequate alternative comms capabilities in place in case our primary and backup comms are denied? Do we have TTPs in place to support comms-out (EMCON) operations, and are our aircrews proficient in their use? How often do we train in a comms-out environment?

About a year ago, Gen. Carlton "Dewey" Everhart, Commander, Air Mobility Command, asked me to help him develop cloaking devices and lasers to protect AMC aircraft. Sir, with respect, I offer that we need to be concentrating on successfully getting to the fight before we concern ourselves with how we will win it, or even survive it.

EW ECCT

There is some good news: last November, Gen. Steve "Seve" Wilson, VCSAF, announced that the third Enterprise Collaboration Capability Team (ECCT) would be Electronic Warfare/Electromagnetic Spectrum (EW/EMS) Superiority.[7] The EW/EMS Superiority ECCT will identify and quantify DOTMLPF-P solutions to fill key capability gaps. Gen. Everhart's request for a "cloaking device" would be advantageous for all aircraft in the inventory, and the ECCT may be the answer to getting that capability. The ECCT construct considers funding above the platform level, and across the Service Core Functions. The ECCT may begin to address funding challenges for a capability that doesn't fall directly within a single command. Within 18 months, the ECCT will publish a Flight Plan that outlines how we will go about developing and fielding the right EW capabilities for the entire Air Force.



Gen. Stephen W. "Seve" Wilson is Vice Chief of Staff of the U.S. Air Force, Arlington, Va. As Vice Chief, he presides over the Air Staff and serves as a member of the Joint Chiefs of Staff Requirements Oversight Council and Deputy Advisory Working Group. (USAF Photo).

What this means for AMC is, the ECCT's Flight Plan will change the way AMC personnel do their jobs. I foresee new TTPs and policies that resurrect our operations during the Cold War era, modified to accommodate our current capabilities. Ironically, we must look back to look forward. If we don't, we will end up like the doomed swordsman in the market square. ■

Warrior Support Solutions, LLC provides indispensable Electronic Warfare (EW) and Electromagnetic Spectrum Operation (EMSO) subject matter expertise (SME) to the Department of Defense (DOD), industry, and academia. We advocate for joint, collaborative, cross domain solutions that protect and defend our warfighters, decisively assuring mission success.

Those readers with EW/EMS technologies – or ideas to move EW/EMS forward – can reach Tango via email at stourangeau@warriorSS.com.

Visit www.WarriorSS.com

1 Understanding Cyber Warfare and its Implications for Indian Armed Forces, by Col. R.K. Tyagi, Copyright 2013, chapter 3, "Offensive Action", United Service Institution of India, New Delhi.

2 "Are Russia's military advances a problem for NATO?", by Jonathan Marcus, Diplomatic Correspondent, BBC News, 11 August 2016: http://www.bbc.com/news/world-europe-37045730

3 "Russia's Surging Electronic Warfare Capabilities", by Caitlin Patterson, 9 April 2016, The Diplomat: http://thediplomat.com/2016/04/russias-surging-electronic-warfare-capabilities.

4 "Threat from Russian UAV jamming real, officials say", by Mark Pomerleau, 20 December 2016, C4ISRNET: http://www.c4isrnet.com/articles/threat-from-russian-uav-jamming-real-officials-say

5 "Breaking down China's electronic warfare tactics", by Mark Pomerleau, 27 March 2017, CS4IRSNET.com: http://www.c4isrnet.com/articles/breaking-down-chinas-electronic-warfare-tactics

6 "Flexing Muscle, China Destroys Satellite in Test", by William J. Broad and David E. Sanger, 19 January 2007, New York Times: http://www.nytimes.com/2007/01/19/world/asia/19china.html

7 "Air Force Launches Major Electronic Warfare Study: VCSAF", by Colin Clark, 28 November 2017, breakingdefense.com: https://breakingdefense.com/2017/11/air-force-launches-major-electronic-warfare-study-vcsaf/