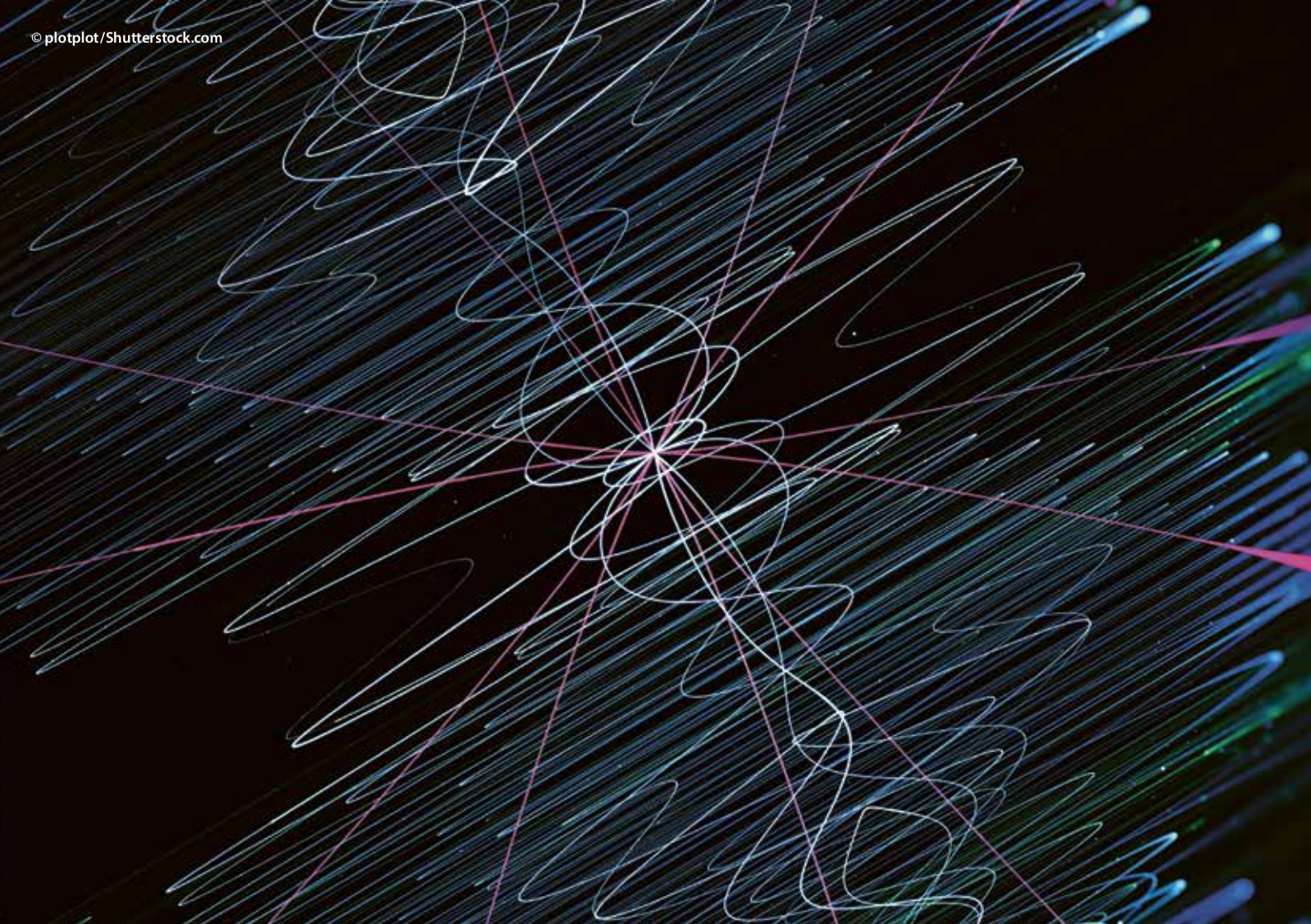

Electronic Protective Measures

XVIII

It's About Protecting Access, Not Aircraft

By Mr Dirk A. D. Smith and
Mr Steve 'Tango' Tourangeau
Reginald Victor Jones Institute

While the world can argue about whether words can hurt, one thing is clear: misunderstanding words can kill, especially in the context of the military. In the world of electromagnetic warfare, just such a misunderstanding of the term 'Electronic Protective Measures' (EPM) has left NATO less prepared for the field of battle and has already caused soldiers to fall when and where they should not. This article addresses the confusion, clears up the definitions through examples of each, and makes the obvious suggestion of what needs to be done.

The Confusion

When most people think of EPM, they think about platform self-protection (such as jammers or chaff and flares), but that is incorrect. Jammers and the like are classified as Electronic Defence (ED). In contrast, EPM is about protecting our access to, and the ability to operate in, the electromagnetic

spectrum, regardless of conditions (e.g., when access is contested, congested, or even denied). An example of EPM features would be the use of low probability of detection communication technology to hide our signals.[1]

This confusion is not new, but it is problematic. The conflation of EPM and ED, especially by people at remarkably high levels, results in the belief that EPM is automagically part of ED and, therefore, built into the systems that we have operating today … it is not. For example, the new Active Electronically Scanned Array (AESA)[2] antennas that replace parabolic dish antennas in US forces are wreaking havoc with US Radar Warning Receivers (RWR) operating nearby. The AESA works fine but its transmissions interfere with the RWR which does not have sufficient EPM features and results in the loss of situational awareness of the threat environment for the aircrew. In contrast, in aircraft with the traditional parabolic dish antenna that operated on specific frequencies, it was easy to blank out those frequencies on the RWR. With AESA and its much broader frequency range, it is very difficult to blank out those frequencies without making the RWR virtually useless.

A more graphic example of deployed systems that were not built with (or tested for) adequate EPM was described by Dave Tremper, Director of Electronic Warfare at the Office of the United States Secretary of Defense for Acquisition and Sustainment, when speaking as a panellist in a January 2021 webinar hosted by the Potomac Officers Club[3]: 'CREW, a radio-controlled IED jammer, puts out energy across the spectrum which is intended to stop IEDs from being communicated with.[4] CREW can overlap with the way that we communicate, so we had to turn one on and turn one-off to keep moving and that has resulted in some pretty awful scenarios that are unclassified.' Tremper went on to describe not just what could be, but what in general terms has occurred: 'There is the warfighter who's in the convoy who gets pinned up against the guard rail which is a prime IED location. He's got his CREW jammer going but he can't talk because his radio isn't working when his CREW jammer is on so you've got this scenario

in which you can either talk and try to get help and turn your jammer off and risk the chance that this IED is going to explode or you can keep your jammer on and attempt to fight your way out. It becomes this life-or-death situation and that is completely unacceptable.' And that is what happened during numerous operations: CREW was operating, jamming as designed. However, when members of the various convoys needed to communicate, CREW was shut down, IEDs went off, and soldiers died.

Michael Ryan[5], then Deputy Project Manager for Electronic Warfare in the Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO IEWS), stated in a 2013 SIGNAL Magazine article that the Army is rife with documented cases where a soldier had to choose between protection from an active jammer or turning off the jammer to communicate and some of these forced decisions led to loss of life.[6]

Clearing Up Definitions

Before clarifying EPM versus ED, one other item of lexicon house-cleaning is needed. Generations of warfighters who jammed enemy radar or communications were known commonly as electronic warfare soldiers. Now that is changing to electromagnetic. The term electronic refers to the control of electric current by various devices[7] while electromagnetic refers to electromagnetic waves.[8] Therefore, while electronic refers to computers and myriad other devices, electromagnetic narrows the focus to waves and the use of same throughout the electromagnetic spectrum. While both terms are still commonly used, the change is embedded in US Air Force doctrine, such as in the 'Introduction to Electromagnetic Warfare', published by the Curtis E. Lemay Center for Doctrine Development and Education.[9] With respect to EPM and ED, and because the differences can seem rather gray at first, it is helpful to envision hard examples. Thus, consider the following two examples of ED, followed by two examples of EPM:

What Electronic Protective Measures are NOT

In contrast to EPM, ED systems are stand-alone systems that include features like jamming to confuse enemy detection and communication and decoys that steer incoming missiles away.

- **Jamming:** The AN/ALQ-131 Electronic Countermeasures (ECM) pod is a good example of a system with ED features, protecting both aircrews and aircraft since the 1990s. To date, and with periodic upgrades, more than 1,600 produced by Northrup Grumman have been deployed with recent variants found on the F-16 Block 60 and F-35 Joint Strike Fighter. The ALQ-131's ED features are enabled by responding against radar threats with repeater or transponder electronic jamming techniques. Weighing in at 600 pounds (270 kilogram), it has a modular design for multiple frequency band capability and can be quickly reprogramed against changing threats.[10]
- **Decoying:** The MK 53 DLS Nulka system is an Australian-designed and developed active missile decoy built by an Australian/American collaboration. It is a rocket-propelled, disposable, offboard, active decoy designed to seduce anti-ship missiles away from their targets. It has a unique design in that it hovers in mid-air while seducing the incoming anti-ship missile.

  Specifically, the MK 53 DLS system is fitted to the Canberra Class amphibious assault ships, Adelaide Class and Anzac Class frigates, and the new Hobart Class guided-missile destroyers.[11] It is also used on more than 122 US ships.[12] The word 'Nulka' is the Australian Aboriginal language meaning 'be quick,' which apparently it is.

What Electronic Protective Measures ARE

EPM are a way for systems to function within the spectrum no matter the conditions including contested, congested, denied access, etc. It is also

important to note that electromagnetic protection is not a platform or system. Rather, EPM are the features included in spectrum-dependent systems. That's it. Examples of EPM features include Low Probability of Interception/Low Probability of Detection (LPI/LPD), anti-jam, frequency hopping, and stealth.

- **Low Probability of Interception/Detection:** Radar often must contend with radar threats such as Electronic Attack (EA) systems and Anti-Radiation Missiles (ARM); systems designed to interfere with or degrade radar effectiveness or even destroy the radars themselves. Radar systems equipped with LPI/LPD features make radar signals less subject to interception and detection. Put another way, LPI/LPD is the ability to 'see and not be seen'.[13]

  Aytug Denk, author of a well-known thesis on the detection and jamming of LPI radar, stated that 'to survive these countermeasures and accomplish their missions, radars have to hide their emissions from hostile receivers. For this purpose, and to mask their presence, radars use power management, wide operational bandwidth, frequency agility, antenna side lobe reduction, and advanced scan patterns (modulations).'[14] This, then, is a good example of EPM because the features are designed to protect access to and use of the spectrum when faced with adversary attempts to prevent such use. An example of LPI Radar (LPIR) includes the Northrop Grumman AN/APG-77 deployed on the F-22 Raptor. Known as multi-mode tactical radar, this enables the pilot to track and shoot at multiple threat aircraft before the adversary's radar even detects the Raptor.
- **Frequency hopping:** While radio communications help Command and control (C2) of the battlefield, the transmissions can also be picked up by adversaries effectively eliminating the C2 advantage (or transferring that advantage to the adversary). One way to combat this risk is through the use of Software-Defined Radios (SDR) that enable different EPM features such as automated frequency hopping.

> An SDR is '… a radio in which the properties of carrier frequency, signal bandwidth, modulation, and network access are defined by software. Modern SDR also implements any necessary cryptography, forward error correction coding, and source coding of voice, video, or data in software as well.'[15]
>
> Another benefit of SDR is the ability to execute over-the-air or other remote reprogramming, allowing 'bug fixes' to occur while a radio is in service, thus reducing the time and costs associated with operation and maintenance.[16] Consider the difference with hardware-based radios which would require getting it to base, opening the system up, and replacing parts while the SDR system could be updated (repaired) while in use far afield (or airborne).

To sum it all up, EPM create the ability to defeat EA.

What Do We Do Next?

With the confusing conflation of EPM and ED that has sadly resulted in the deployment of systems with insufficient EPM that has in turn resulted in unnecessary deaths, we are now left with the question of how to resolve it. The first step is to simply understand this issue which is the intent of this article. That still leaves us with another most crucial step: Formal requirements that mandate full and proper EPM features as part of the development, production, testing and deployment of all electromagnetic spectrum-reliant systems. So, while it is true that misunderstanding words can kill, perhaps the words in this article will help reduce what Tremper called 'completely unacceptable'.

Mr Dirk A. D. Smith is Director of Research for the Reginald Victor Jones Institute (RVJ Institute) Center for Excellence in Electromagnetic Spectrum Operations and is an international award-winning technical writer and freelance journalist. He specializes in the research, analysis, writing and presentation/publishing of complex technical knowledge. This work often includes interviewing Subject Matter Experts (SME) for internal and external corporate, military, and intelligence communications.

Mr Steve 'Tango' Tourangeau is the Vice President and Chief Operating Officer of Warrior Support Solutions, LLC as well as Co-Founder and Dean of the Reginald Victor Jones Institute (RVJ Institute) Center for Excellence in Electromagnetic Spectrum Operations. He provides expertise for the DoD, industry and academia to advance Electromagnetic Spectrum capabilities. Tango is a retired Air Force officer with over 1,500 hours as Flight Test Navigator and Electronic Warfare Officer.

Endnotes

1. 'Low Probability of Detection Communication: Opportunities and Challenges', IEEE Wireless Communications, Volume: 26, Issue: 5, Oct. 2019 (published online 25 Oct. 2019), https://ieeexplore.ieee.org/document/8883125, accessed 26 Mar. 2021.
2. https://military.wikia.org/wiki/Active_electronically_scanned_array, accessed 26 Mar. 2021.
3. https://potomacofficersclub.com/events/poc-achieving-spectrum-dominance-in-the-digital-battlespace/, accessed 26 Mar. 2021.
4. Van Pool, J. Elise, 'CREW: helping defeat IEDs', US Army, https://www.army.mil/article/67963/crew_helping_defeat_ieds#:~:text=CREW%20systems%20are%20helping%20Soldiers,to%20detonate%20the%20devices%20remotely.&text=CREW%20has%20been%20highly%20effective,by%20cell%20phones%20said%20Bowers, accessed 26 Mar. 2021.
5. LinkedIn profile Michael Ryan: https://www.linkedin.com/in/michael-ryan-0223/, accessed 26 Mar. 2021.
6. Ackermann, Robert K., 'Consolidation Is the Course for Army Electronic Warfare', SIGNAL Magazine, 1 Apr. 2013, https://www.afcea.org/content/consolidation-%E2%80%A8the-course-army-%E2%80%A8electronic-warfare, accessed 26 Mar. 2021.
7. Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/electronic, accessed 26 Mar. 2021.
8. Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/electromagnetic, accessed 26 Mar. 2021.
9. Curtis E. Lemay Center, 'Air Force Doctrine Publication (AFDP) 3-51, Introduction to Electromagnetic Warfare', https://www.doctrine.af.mil/Portals/61/documents/Annex_3-51/3-51-D03-EW-EW-Introduction.pdf, accessed 26 Mar. 2021.
10. National Museum of the USAF, ALQ-131 ECM Pod (published online 29 May 2015) https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/197590/alq-131-ecm-pod/, accessed 26 Mar. 2021.
11. Royal Australian Navy, Nulka active missile decoy, https://www.navy.gov.au/weapon/nulka-active-missile-decoy, accessed 26 Mar. 2021.
12. US Navy, Naval Sea Systems Command, MK 53–Decoy Launching System (Nulka) (last updated 16 Jan. 2019), https://www.navy.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=1&ModuleId=724&Article=2167877, accessed 26 Mar. 2021.
13. Fuller, K. L., 'To see and not be seen', IEE Proceedings F 137 (1): p. 1–9, https://digital-library.theiet.org/content/journals/10.1049/ip-f-2.1990.0001, accessed 26 Mar. 2021.
14. Denk, Aytug, Naval Postgraduate School, Monterey, California, Thesis: 'Detection and Jamming low probability of intercept (LPI) Radars' (published 2006), https://apps.dtic.mil/dtic/tr/fulltext/u2/a456960.pdf, accessed 26 Mar. 2021.
15. Fette, Bruce A., 'History and Background of Cognitive Radio Technology' (published online 2009), https://www.sciencedirect.com/topics/engineering/software-defined-radio#:~:text=A%20software%20defined%20radio%20is,data%20in%20software%20as%20well., accessed 26 Mar. 2021.
16. Wirelessnavigation.org, 'Software Defined Radio', https://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf, accessed 26 Mar. 2021.