MAY 2019
Vol. 42, No. 5

ASSOCIATION OF OLD CROWS

JED

The Journal of Electronic Defense

www.crows.org

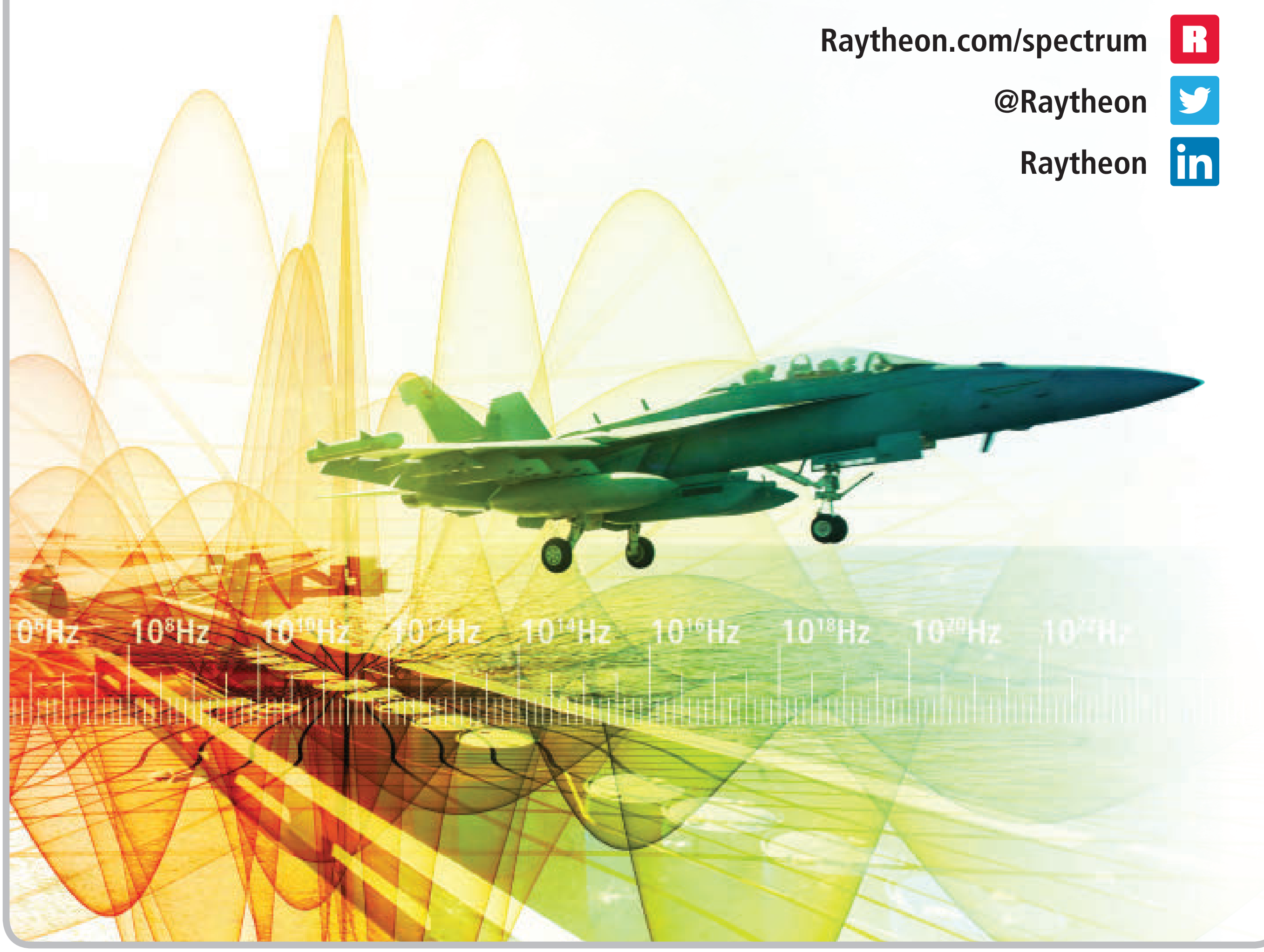
Europe's Helicopter EW Programs

Also in this issue:

Future Electronic Attack: Coherent, Distributed and Cheap

Survey: Counter-UAS Systems

What Does the EM Domain Look Like?



New for 2019

RWR Tester

- 16 Emitters
- 0.5-2GHz Omni port
- 2-18GHz 4 port Amplitude DF
- 10u chassis for portability
- Optional portable Cal kit

RF Photonic Link

- Move RF across long distances >100m
- Wideband operation 0.5-18GHz
- Low insertion loss
- Low Harmonics and Spurious
- Large Dynamic Range

Applications include:
Used in conjunction with the RWR tester to extend the reach to SUT
Distribution of RF in Laboratories, Anechoic chambers or Installed Test Facilities

Ultra Electronics Limited - EWST
A8 Cody Technology Park, Ively Road
Farnborough, Hants GU14 0LX
Tel: +44 (0)1252 512951
Fax: +44(0)1252 512428
info@ewst.co.uk
www.ewst.co.uk

The guided-missile destroyer USS Gravely *(DDG 107) fires a training chaff round during an air defense exercise while participating in Joint Warrior 19-1 on April 7 in the Sea of Hebrides. Gravely was underway as the flagship of Standing NATO Maritime Group 1 to conduct maritime operations in the northern Atlantic.*

US NAVY PHOTO

News

Features

Departments

COVER PHOTO COURTESY OF TIM FELCE. TABLE OF CONTENTS PHOTO COURTESY OF US NAVY.

DISTRIBUTED EW IS A MINDSET

This month's *JED* includes an excellent article by Lt Col Jeff "Seed" Kassebaum, USAF, titled, "Future Electronic Attack: Coherent, Distributed and Cheap." In his article, he describes where the US Air Force's Airborne Electronic Attack (AEA) mission is today and how it will probably look in the future. The bottom line is that the Air Force will need to make a balanced investment in people and technology and at the same time change its traditional approach to EW.

From its very beginnings in World War II, the EW mission has been an outlier in most military forces. EW has traditionally been conducted by specially trained operators fighting from specially equipped weapons platforms. By the 1990s, the phrase that described EW was "low-density high-demand" (LDHD). Today, this LDHD approach is no longer adequate because the electromagnetic contest between radars, radios, GNSS, etc. on one side and EW on the other is too vast, too complex and also too strategic. With the widespread availability of commercial electronics technology, the idea that we can fight this electromagnetic contest with special weapons platforms operated by specially trained personnel begins to break down. As Lieutenant Colonel Kassebaum explains, part of the future AEA mission is going to be "coherent, distributed and cheap." What this means in the bigger picture is that EW – both in terms of materiel and skilled practitioners – needs to be better integrated into the larger force structure. In order to achieve this, we need to change our thinking – inside the EW community as well as outside.

To some extent, this is already happening. I would argue that an F-35 pilot, for example, spends far more time planning, thinking and maneuvering in the Electromagnetic Environment (EME) than he or she does actually flying the plane. We don't call this F-35 operator an EWO, and we don't need to. But we do need to recognize that many weapons systems operators across all the Services will need to learn more about maneuver in the EME, perhaps as a core competency. In this sense, the idea of EW being "distributed, coherent and cheap" applies to personnel, as well as materiel. EW needs to grow beyond the idea of "special" people in "special" platforms.

This is where I think the EW Community can evolve its thinking and grow its understanding. Instead of focusing primarily on EWOs and EWO development, we can step up and help military leaders understand how to blend more EM maneuver knowledge into the larger force structure. Modern military organizations will always need high-level EW expertise (i.e., EW operators and planners). No one is suggesting they don't. But today, they need much more than this. They need to develop a wider knowledge base that isn't so much centered on EW "expertise" as it is focused on providing electromagnetic maneuver "competence." It's a mindset, and we can help to make this a reality. – *J. Knowles*

ASSOCIATION OF OLD CROWS
www.crows.org
JED
The Journal of Electronic Defense

MAY 2019 • VOL. 42, NO. 5

Subscription Information: Please contact Glorianne O'Neilin at (703) 549-1600 or e-mail oneilin@crows.org.

The Journal of Electronic Defense
is published for the AOC by
NAYLOR
ASSOCIATION SOLUTIONS
5950 NW 1st Place
Gainesville, FL 32607
Phone: (800) 369-6220 • Fax: (352) 331-3525
www.naylor.com

COVER PHOTO COURTESY OF TIM FELCE.

PUBLISHED APRIL 2019/JED-M0519/6754

MAY

Sea-Air-Space
May 6-8
National Harbor, MD
www.seaairspace.org

Electronic Warfare Europe 2019
May 13-15
Stockholm, Sweden
www.eweurope.com

11th Annual Electronic Warfare Capability Gaps and Enabling Technologies Conference
May 14-16
Crane, IN
www.crows.org

2019 Special Operations Forces Industry Conference (SOFIC)
May 20-23
Tampa, FL
www.sofic.org

JUNE

International Microwave Symposium
June 2-7
Boston, MA
www.ims2019.org

10th Annual Cyber & Electronic Warfare Convergence Conference
June 4-6
Charleston, SC
www.crows.org

Paris Air Show
June 17-23
Paris
www.siae.fr

Electronic Warfare Technology Conference
June 18-21
Swindon, Wiltshire, UK
www.cranflield.ac.uk

SEPTEMBER

MSPO 2019
September 3-6
Kielce, Poland
www.targikielce.pl

3rd Electromagnetic Maneuver Warfare Systems Engineering and Acquisition Conference
September 10-12
Dahlgren, VA
www.crows.org

DSEI
September 10-13
London
www.dsei.co.uk

AFA 2019 Air, Space and Cyberspace Conference
September 16-18
National Harbor, MD
www.afa.org

Modern Day Marine
September 17-19
Quantico, VA
www.marinemilitaryexpos.com

OCTOBER

5th Annual Cyber Electromagnetic Activities (CEMA) Conference
October 8-10
Aberdeen Proving Ground, MD
www.crows.org

AUSA Annual Meeting
October 14-16
Washington, DC
www.ausa.org

Seoul ADEX 2019
October 15-18
Seoul, ROK
www.seouladex.com

AOC conferences are noted in red. For more info or to register, visit www.crows.org. Items in blue denote AOC Chapter events.

MAY

AOC Virtual Series Webinar: Radar Cross Section and Stealth
May 9
1400-1500 ET
www.crows.org

Fundamentals of Radar Signal Processing
May 13-16
Denver, CO
www.pe.gatech.edu

Signals Intelligence Fundamentals
May 14-15
Atlanta, GA
www.pe.gatech.edu

Advanced Radar Signals Collection and Analysis
May 14-16
Atlanta, GA
www.pe.gatech.edu

Military Electronic Warfare
May 20-24
Swindon, Wiltshire, UK
www.cranfield.ac.uk

AOC Virtual Series Webinar: The World of Airborne Expendables and Small UAS
May 23
1400-1500 ET
www.crows.org

JUNE

AOC Virtual Series Live Course: DRFM Technology and Design for Electromagnetic Maneuver Warfare
June 3-26
8 sessions, 1300-1600 ET
www.crows.org

Introduction to Intelligence, Surveillance, Reconnaissance (ISR) Concepts, Systems, and Test Evaluation
June 4-7
Atlanta, GA
www.pe.gatech.edu

AOC Virtual Series Webinar: ELINT and RESM – Getting the Facts Straight
June 6
1400-1500 ET
www.crows.org

Airborne AESA Radar
July 9-11
Las Vegas, NV
www.pe.gatech.edu

Radar-Cross-Section Reduction
June 10-12
Atlanta, GA
www.pe.gatech.edu

AOC Virtual Series Webinar: Space EW Part 2
June 20
1400-1500 ET
www.crows.org

JULY

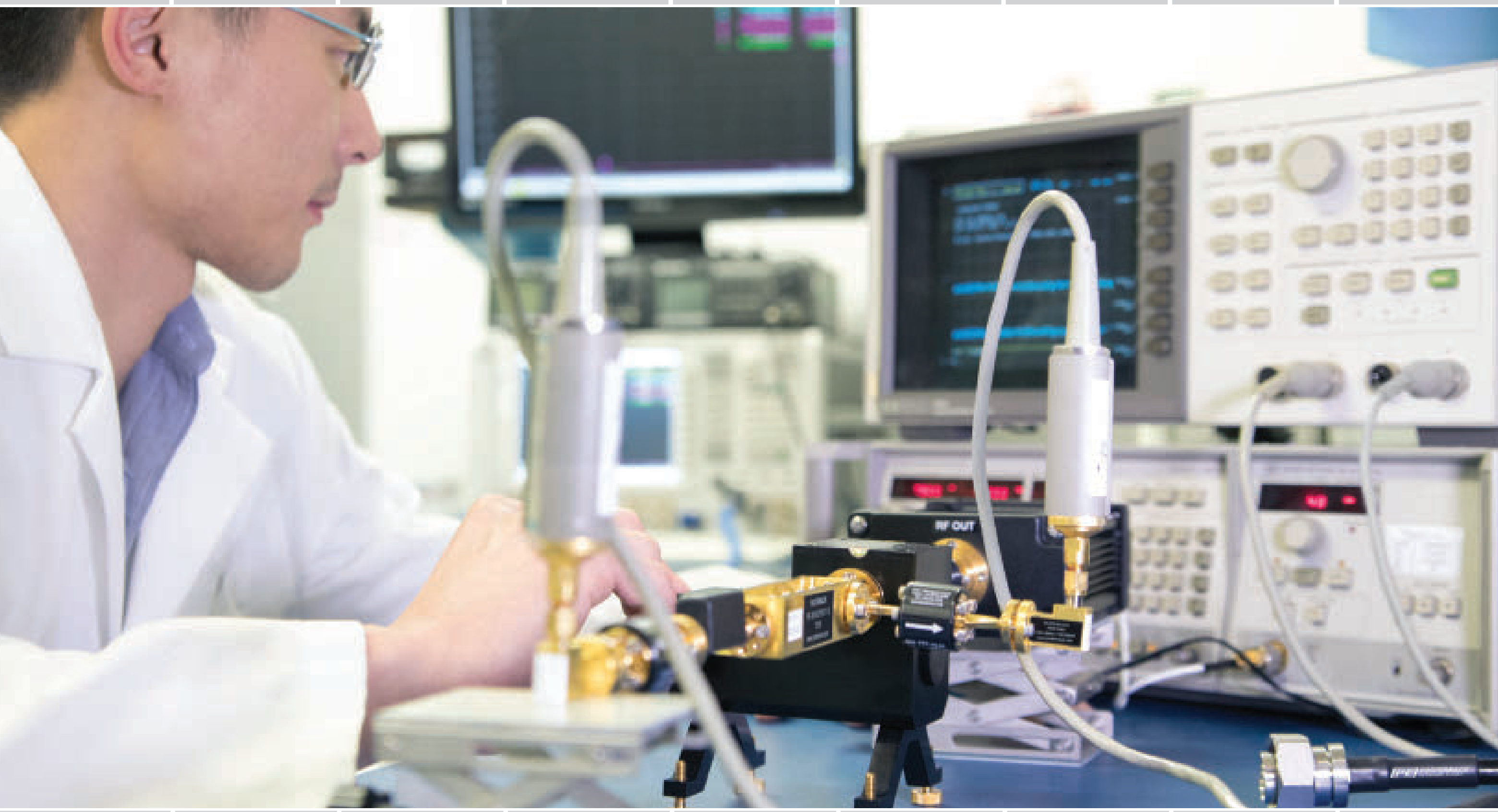
Airborne Electronic Warfare Systems Integration
July 9-11
Atlanta, GA
www.pe.gatech.edu

AOC Virtual Series Webinar: Understanding Tracking Radars
July 11
1400-1500 ET
www.crows.org

AOC Virtual Series Live Course: Introduction to Radar Systems
July 29 - August 9
6 sessions, 1300-1600 EDT
www.crows.org

Cyber Warfare/Electronic Warfare Convergence
July 30 - August 1
Atlanta, GA
www.pe.gatech.edu

AOC courses are noted in red. For more info or to register, visit www.crows.org. Items in blue denote AOC Chapter courses.



MOVING QUICKER

When I worked on the DOD's Airborne Electronic Attack Analysis of Alternatives (AEA AOA) team back in 2000-2002, we looked at a multitude of platforms and profiles that would enable penetration or survivability in an Anti-Access/Aerial Denial (A2/AD) environment. Optimum survivability was achieved using a system-of-systems approach that included a variety of platforms and system characteristics, such as altitude, speed, signatures, and offensive and defensive EW. Moving forward 19 years, Russia, China and other countries have invested considerable energy and resources into developing new A2/AD capabilities, such as advanced surface-to-air missile systems, decoys, HPM, EW and cyber effectors. As a result, our 4^{th}- and 5^{th}-generation aircraft, as well as our C4ISR support aircraft and sensors, have been "pushed back" from the battlespace. How will our strike platforms penetrate and survive?

We have fielded systems, such as the EA-18G Growler, MALD-J and multiple UAS capabilities. But as a main component of the system-of-systems approach, we need to actively pursue stand-in AEA capabilities. Much discussion has included unmanned air systems (UASs), from both a survivability and endurance aspect, as well as small and inexpensive expendable platforms. In the future, our commanders will need weapons that provide not only kinetic and non-kinetic effects, but they will also need to network, act cooperatively in "swarms," feature cognitive capabilities (with adaptive machine learning) and provide sensing and communications. As we extend this concept to include stand-in unmanned platforms and weapons, we are now beginning to realize the true potential for a system-of-systems approach to penetration and operation in the A2/AD environment.

So how do we develop these capabilities and coordinate this electromagnetic "dance" on the battlefield? Technologies exist, but who is driving the integration of multiple capabilities – sense, detect, identify, locate, and deliver kinetic and non-kinetic effects, both temporary and enduring? We have multiple stove-pipes in our acquisition process (e.g., platforms, sensors, SIGINT, EW, cyber, communications, etc.), and we have not even discussed battle planning, CONOPs development, modeling and simulation, testing, training, C3 and integration of coalition capabilities. How do we recognize what data is critical? How do we pass the critical data between platforms? How do we optimize the right effect on the right target at the right time? And how do we obtain real-time BDA that enables optimization of assets?

The Services are all exploring/developing stand-in capabilities, and DARPA is working integrated effectors on the battlefield with multiple programs like MOSAIC Warfare, CONERTO and CODE. But how can we functionally organize, acquire, train and equip faster to achieve this system of systems capability? With multiple research and development projects, US and coalition efforts on-going, can we do a better job of collaborating, coordinating, focusing and optimizing efforts to achieve results faster and get capabilities to the war-fighter sooner? Operating in the A2/AD environment will be a Joint and coalition/partner fight, and we need to figure it out. – *Muddy Watters*

the monitor

news

DOD FY2020 BUDGET PROPOSAL EW PROGRAM HIGHLIGHTS

In March, the DOD released its $713.8 billion FY2020 budget request to Congress. The proposal calls for $104.3 billion for Research, Development, Test and Evaluation, and $143.1 billion for procurement. The following are some of the electronic warfare and signals intelligence program elements included in the budget.

Air Force

PE 0602204F Aerospace Sensors: In its Applied Research programs, the Air Force consolidated previous EW 6.2 R&D work under PE 0602204F Aerospace Sensors, Project 624920 Electronic Warfare Technology. The Air Force requested $34.8 million for PNT in contested and denied environments, RF EW technologies, and EO/IR threat warning and countermeasures technologies. This is an administrative adjustment and not a new start.

PE 0602605F: The Air Force requested $124.4 million for Directed Energy Technology – split between Lasers and Imaging Technology (Project 624866) ($92.4 million) and High-Power Microwave R&D (Project 624867) ($32 million).

PE 0603270F: In its Advanced Technology programs, the Air Force requested $48.4 million for Electronic Combat Technology.

PE 0605931F: In its System Development and Demonstration (SDD) portfolio, the Air Force sought $294.4 million for the B-2 Defensive Management System-Modernization program. DT/OT continues in FY2020, and a Milestone C decision is scheduled for the 4th quarter of FY2020. R&D spending tapers off to $164.6 million in FY2021 and $71 million in FY2022, as production ramps up beginning in FY2021.

PE 0207171F: Another major EW program for the Air Force is the F-15 Eagle Passive/Active Warning Survivability System (EPAWSS) program. FY2019 was a big spending year for the development phase of the program, and funding begins to ramp down in FY2020 with a request of $47.3 million. In terms of Production, the EPAWSS program is split into two "decision points" instead of a traditional Milestone C decision, with the intention that EPAWSS can be fielded earlier. Decision Point 1, which covers the beginning of system production, is slated for 4th Quarter FY2019, and Decision Point 2, which covers system installation on the aircraft, is scheduled for 4th Quarter FY2020.

PE 0207253F: The Air Force requested $15.8 million for continued development of its Compass Call Baseline 3 and Baseline 4 airborne Electronic Attack aircraft. These cover efforts such as low-band antenna design, advanced military and commercial communications offensive capabilities, emerging and modern targets, and studies and analysis for current/future baseline development planning. Baseline 3 development winds down in FY20 as the program begins integration and test. Baseline 3 fielding is scheduled for FY2023. It's worth noting that Congress added $20.2 million in FY2018 and $30 million in FY19 to accelerate the rehosting of mission equipment from EC-130H aircraft to the EC-37B.

Navy

PE 0602271N: In its Applied Research programs, the Navy requested $83.5 million for Electromagnetic Systems Applied Research, which includes $43.5 million for EW Technology, $7.1 million for EO/IR Technology and $7.8 million for Navigation Technology (GPS and alternatives).

PE 0603925N: The Navy requested $118.2 million for Directed Energy and Electric Weapon Systems Technology, including $9 million to begin Project 2731 - High Energy Laser Counter ASCM Project (HELCAP) to "assess, develop, experiment, and demonstrate the various laser weapon system technologies and methods of implementation (e.g. laser sources, mission analysis, lethality, advanced beam control with atmospheric mitigation, target and tracking sensors, control systems) required to defeat ASCMs in a crossing engagement." The Navy also requested $89.2 million for continued development of Project 3402 - The Surface Navy Laser Weapon System (SNLWS).

PE 0604272N: The Navy sought $68.3 million for its Tactical Airborne Directed Infrared CM (TADIRCM) program for continued development of the Distributed Aperture IR Countermeasures (DAIRCM) system and to integrate the DAIRCM solution on the Navy's MH-60S helicopters. Additional DAIRCM recipients are expected to include the AH-1Z, UH-1Y and MH-60R helicopters

PE 0604269N: The Navy requested $143.6 million for its EA-18 Squadrons to continue developing ALQ-218 Airborne Electronic Attack Systems Enhancements (ASE) and Integrated Capability Package (ICP)-3. This also covers transition of Reactive Electronic Attack Measures (REAM) technology from an ONR future Naval capabilities (FNC) science and technology effort to the platform.

PE 0604274N: The Navy requested $529 million to continue development of the Next Generation Jammer (NGJ) Mid-Band pod. The program schedule calls for delivery of seven System Demonstration Test Article Pod shipsets (2 pods per shipset) in 1st Qtr. FY 2020 which will be used for final developmental test efforts, tactics development and operational test.

PE 0604282N: Following on the heels of the MGJ Mid-Band pod development, the Navy sought $111.1 million to complete two Demonstration of Existing

Technologies (DET) contracts for the NGJ Low-Band pod program. The program schedule calls for an EMD or rapid prototype award in the 3rd quarter of FY2020.

PE 0604503N: The Navy requested $27.3 million for continuing upgrades to the BLQ-10 submarine EW system. The Navy also plans to begin developing a coherent electronic attack system for the Multifunction Modular Mast beginning in FY2023.

PE 0604757N: Under the Ship Self Def (Engage: Soft Kill/EW) project, the Navy asked for $97.4 million, primarily to continue development of the Advanced Offboard EW (AOEW) program ($54.3 million), which is preparing for Milestone C production decision in FY2020, and for the SEWIP Block 3 system ($22.1 million), which winds down its EMD phase in the 1st quarter of FY2020.

PE 0304785N: Among its SIGINT programs, the Navy requested $101.3 million for Tactical Cryptologic Systems, which included $53.5 million for Project 2134, Shipboard IW Exploit. This will provide $12.6 million for continued enhancements to the Ship's Signal Exploitation Equipment (SSEE) Increment F system, as well as $27.3 million for further development of Spectral, the Navy's "next-generation SIGINT, EMW, and IO weapons system" which is slated to begin Low-Rate Initial Production in FY2023.

PE 0205601N: The Navy also sought 138.4 million for AGM-88 HARM Improvements, which included $119.6 million for continued development of its AGM-88G Advanced Anti-Radiation Guided Missile–Extended Range (AARGM ER), which is scheduled to begin "free flight" testing in FY2021 and enter Low-Rate Initial Production (LRIP) in the 3rd Quarter of FY2021.

Army

In its Applied Research (6.2) and Advanced Technology (6.3) budget lines, the Army re-aligned its traditional EW program element numbers (0602270A and 0603270A) into other programs.

PE 0602148A: Within its Future Vertical Lift (FVL) Technology Applied Research program, the Army requested $21.8 million for EW and ASE-related efforts, including signature reduction, cognitive countermeasures technology development, multispectral threat warning and countermeasures, and "Tunable Pyrotechnics Technologies," which calls for the development of "nano, reactive, and advanced/novel materials and energetic manufacturing processes to enable, customize and 'tune' a family of countermeasure decoys for FVL platforms."

PE 0602150A: The Army requested $50.8 million for Air and Missile Defense Technology Applied research, which addressed a number of directed energy projects, such as High Energy Laser (HEL) Tactical Vehicle Demonstrator Technology (Project AC9), HEL Enabling and Support Technology (Project AD2) and Close Combat High Energy Laser Technology (Project AD9).

PE 0602213A: The Army's C3I Applied Cyber program requested $18.9 million, including $3.9 million for Network Access and Effects Technology (Project 3CY). "This Project investigates the application of machine learning technologies to assist in capability development and mission execution processes with respect to Offensive Cyber Opera-

tions (OCO)/Radio Frequency (RF) Enabled capabilities."

PE 0603457A: In its Advanced Technology portfolio, the Army requested $13 million for C3I Cyber Advanced Development, including $1.4 million for Network Access and Effects Advanced Technology (Project 9CY), and $2 million for Offensive Cyber Operations (OCO) Mirror Advanced Technology (Project CB4).

PE 0603462A: The Next Generation Combat Vehicle Advanced Technology program had several EW projects. The Army asked for $23.4 million for Ground Systems Active Defense (GSAD) Advanced Technology (Project BG7); $3.1 million for Obscuration Advanced Technology (Project BG9); and $13 million for Survivability Systems Controls Advanced Technology (Project BH1), which "advances the design and capability of the Modular Active Protection System (MAPS) framework and controller to enable integrating emerging survivability technologies into safe and secure configurations and demonstrating them in a representative operational environment."

PE 0604021A: One significant newstart program is Electronic Warfare Technology Maturation (MIP) ($18 million request), which seeks to rapidly develop and field the Terrestrial Layer System (TLS) "to provide Army maneuver forces integrated Signals Intelligence (SIGINT), Electronic Warfare (EW), and offensive Cyber-enabling integrated solution to support Multi Domain Operation capability gaps and provide Force Protection, Situational Development, and Information Superiority to the maneuver forces." The schedule for the two-year, $36.8 million development program (FY2020 and FY2021) is followed by a five-year production phase beginning in FY2022.

PE 0604270A: The Army requested $70.5 million for Electronic Warfare Development, including $23.5 million for continued development of the Electronic Warfare Planning and Management Tool (Project DX5); $41.6 million for Multi-Function Electronic Warfare (MFEW) (Project DX6), which covers MFEW Air Large development; and $55 million for Integrated EW Systems (Project VS6), which covers CREW system improvements.

PE 0605035A: The Army requested $46.3 million for continued development of the Common Infrared Countermeasures (CIRCM) systems.

PE 0605049A: The Army's next-generation missile warning system, the Advanced Threat Detection System, is undergoing an acquisition strategy update that is due in 2nd Quarter FY2020. As a result, the funding request for this effort was $1.5 million.

The DOD budget is expected to be a contentious political issue this year for two reasons. The White House boosted defense spending while trimming the budget of other government departments, which has angered Democrats who control the House and can filibuster spending bills in the Senate. Also, the DOD request included $173.1 billion for Overseas Contingency Operations (OCO), of which only $66.7 billion is marked for "direct war requirements" or "enduring requirements." This has led many congressional members from both parties to criticize the use of OCO funding to get around budget caps established in the 2011 Budget Control Act. The Senate is scheduled to mark up its version of the National Defense Authorization Act (NDAA) in mid-May, and the House expected to mark up its version of the bill in early June. – *J. Knowles*

CONGRESS BRIEFED ON NAVY AND MARINE CORPS MODERNIZATION AND AVIATION PROGRAMS

The Tactical Air and Land Forces Subcommittee of the House Armed Services recently heard testimony from representatives of the Navy and Marine Corps, who updated Congress on the progress of several Navy modernization and aviation programs.

In a prepared statement for the April 4 hearing, LtGen David Berger, Deputy Commandant of Combat Development and Integration and Commanding General of the Marine Corps Combat Development Command, and Jimmy Smith, Assistant Secretary of the Navy Expeditionary Programs and Logistics Management, addressed Navy modernization efforts, including Fleet Marine Force (FMF) operations in the information environment (OIE).

"We cannot count on uncontested access to the electromagnetic spectrum any more than we can count on uncontested freedom of maneuver at sea," the statement read. To that end, the FMF has been developing the Electronic Warfare Ground Family of Systems (MEGFos) within the Multi-Function Electronic Warfare (MFEW) program in order to "employ a common backplane hardware infrastructure, which enables plug & play capability, using software defined transceivers, amplifiers, and specialized modules to provide upgradable, networked electronic warfare systems for use across the FMF."

The MFEW program, which involves the modernization of Counter Radio-Controlled Improvised Explosive Device – Electronic Warfare (CREW) systems, aims to "provide networked and distributed MFEW capabilities to sense and attack the adversary while providing protection from a multitude of advanced spectrum reliant threats."

Speaking to the progress of Navy aviation programs were Daniel Nega, Deputy Assistant Secretary of the Navy Air Programs, LtGen Steven Rudder, Deputy Commandant for Aviation, and RADM Scott Conn, Director of Air Warfare. Their statement addressed Airborne Electronic Attack (AEA) capabilities, including the EA-18G Growler and the Next Generation Jammer (NGJ).

"The EA-18G Growler is a critical enabler for the Joint force as it brings fully netted electronic warfare capabilities to the fight, providing essential capabilities in the Electromagnetic Maneuver Warfare environment," the statement read. Procurement of the Growlers will be completed in July 2019, with 160 aircraft in use by the Navy at that time. The President's FY 2020 Budget requested $143.6 million in Research, Development, Test and Evaluation (RDT&E) funds for further maintenance and modernization of the aircraft.

The statement also addressed the progress and needs of the Navy's three NGJ variants – Mid-Band, Low-and and High-Band. NGJ Mid-Band is in development following a redesign in June 2018, and the program is scheduled for Initial Operating Capability (IOC) in FY2022 fol-

NAVAIR SEEKS NEXT-LEVEL EW TRAINING SERVICES

Last month, Naval Air Systems Command's Specialized and Proven Aircraft Program Office, PMA-226 (Patuxent River, MD), issued a formal full request for proposal for the High Endurance Electronic Warfare Jet (HEEWJ) Capabilities program, which seeks airborne threat simulation services that will "train shipboard and aircraft squadron weapon systems operators and aircrew on how to counter potential enemy Electronic Warfare (EW) and Electronic Attack (EA) operations in today's Electronic Combat (EC) environment."

The solicitation follows a February pre-solicitation Conference where PMA-226 detailed performance goals for the HEEWJ program, which would provide simulation capabilities for the US Navy fleet and foreign customers. Specifically, the program seeks aircraft and personnel to deliver services for various mission areas – Electronic Attack (EA), Stand-Off Jamming and Target Banner Tow (TBT). Required support is to include a variety of "venues, from basic 'schoolhouse' Air Intercept Control (AIC) training; Test and Evaluation (T&E) of new platforms and systems; to large multinational exercises or small, single-unit training exercises, including target/banner tow missions."

Desired EA capabilities include a communications suite that offers EW operator intercommunication system (ICS) capability, digital radio frequency memory (DRFM) operations to include reconfigurable for "noise on" B, C/D, E/F/G, I-band jamming IAW the IRD, and simultaneous support for two different bands of DRFM jamming, along with RF cabling for support of government-furnished antennas mounted in ALQ-167 pods. Also required are two sets of D-band identify friend or foe (IFF) antennas and cables.

Stand-Off Jamming requirements include provisioning for the government-provided APX-123 IFF transponder and control head, support for four different bands of DRFM jamming, as well as B-Band noise jamming and external pod mounts that support two simultaneous pods, such as the ALQ-188, ALQ-167 and others. A spectrum analyzer capable of detecting and providing a line of bearing to radar signals between 400 MHz and 18 GHz, and communications signals from 100 MHz to 3 GHz.

NAVAIR Specialized and Proven Aircraft Program Office, PMA-226, Contracted Air Services (CAS), Integrated Product Team (IPT) anticipates awarding a single award, firm-fixed price, indefinite delivery, indefinite quantity contract. The solicitation number is N00421-18-R-0009. The points of contact are Brij Mohann, (301) 757-7629 or brij.mohan1@navy.mil, and Michael J. Coon, (301) 757-7114 or michael.coon@navy.mil. Responses are due May 28. – *E. Richardson* lowing a budget request for $524.3 million in RDT&E for FY 2020. (See related story about the DOD's FY2020 budget request in this month's "Monitor" section.) The Navy also requested $111.1 million in RDT&E for the NGJ Low-Band program for demonstrating existing technologies and future development contracts. – *H. Swedeen*

ADVANCED THREAT MISSILE DEFENSE OPERATIONS

Representatives from the US Army and Missile Defense Agency (MDA) gave testimony on missile defense programs, including directed energy initiatives, before the Strategic Forces Subcommittee of the Senate Armed Services. The April 3 hearings included testimony by LTG James Dickinson, Commanding General of US Army Space and Missile Defense Command/Army Forces Strategic Command, and USAF Lt Gen Samuel Greaves, Director, MDA

In Dickinson's prepared statement, he said, "We expect cyber and electronic attacks will be increasingly relied upon in potential adversaries' anti-access/area-denial (A2/AD) strategies. Our ability to successfully counter these continuously advancing threats will rely heavily on our increased use of space and space-enabled capabilities. Space sensors, in greater numbers and sensor modalities, would expand our capability and capacity to track, discriminate, and successfully engage ballistic, cruise, and hypersonic threats."

To that end, Dickinson outlined programs and strategies of the US Army Space and Missile Defense Command and Army Forces Strategic Command (USAAMDC/ARSTRAT), as well as the Air and Missile Defense (AMD), including High Energy Laser (HEL) technology and Counter-Unmanned Aircraft Systems (C-UAS) initiatives intended to aid in missile defense efforts as adversaries' missile capabilities become increasingly complex.

Army AMD missile defense initiatives include advancements to C-UAS systems to better combat a growing range of tactical reconnaissance and attack UAS platforms, and the Army has deployed more than 500 C-UAS systems in response to a warfighter Joint Urgent Operational Needs Statement (JUONS). According to the statement, "The modification of counterfire target acquisition radars, equipped with multi-mission air surveillance target acquisition capabilities, improves the warfighter's ability to detect and defeat these low, slow, and small UAS threats."

Dickinson also outlined USASMDC/ARSTRAT's previous progress with HEL technology, including the High Energy Laser Mobile Test Truck (HELMTT), Multi-Mission High Energy Laser (MMHEL) and the Mobile Experimental High Energy Laser (MEHEL), all built in an effort to "develop ruggedized laser system components and subsystems, integrate them onto an Army vehicle, conduct demonstrations to characterize performance, and transition the technology to a Program Executive Office."

In his prepared statement for the MDA, Greaves addressed the initiatives outlined in the MDA's FY 2020 budget, including directed energy systems, which Greaves said will play an increasing role in the development of Ballistic Missile Defense Systems (BMDS).

According to Greaves' statement, "This budget request will continue the development and technology risk reduction of breakthrough technologies for integration into the BMDS, including discrimination improvements, Multi-Object Kill Vehicle technology, hypersonic defense technology, and high-powered lasers that have potential use against threat missiles in the boost phase of flight."

Of the $9.43 billion requested in the MDA's FY 2020 budget, $303.5 million will be dedicated to "Technology Maturation Initiatives to conduct ground and airborne demonstrations of advanced sensor systems and refine directed energy technologies for missile defense." Such initiatives will include laser maturation and power scaling development, and exploring Neutral Particle Beam system development to offer "new kill options for the BMDS and [add] another layer of protection for the homeland."

Greaves also outlined the future importance of hypersonic defense, for which the MDA requested $157.5 million in the FY 2020 budget "to execute the systems engineering process, identify and mature full kill chain technology, provide analysis and assessment of target of opportunity events, and execute near term space sensor technology and multi-domain command and control capability upgrades to address defense from hypersonic threats."

According to the statement, "An integrated set of enhancements will provide incremental capability measured by progress and knowledge points in the following areas: establishment of systems engineering needs and requirements to identify alternative material solutions; execution of a series of sensor technology demonstrations; modification of existing BMDS sensors and the C2BMC element for hypersonic threats; and definition of weapon concepts and investments in key technologies to enable a broad set of solutions, including kinetic and non-kinetic means." – *H. Swedeen*

DOD CONTINUES TO GROW INVESTMENT IN DIRECTED ENERGY AND QUANTUM SCIENCE

The Department of Defense's (DOD's) FY2020 Science and Technology Posture Hearing before the House Armed Services Subcommittee on Emerging Threats and Capabilities addressed several modernization priorities outlined in the 2018 National Defense Strategy (NDS), including directed energy and quantum science.

A prepared statement by Michael Griffin, Under Secretary of Defense for Research and Engineering, included plans to "[accelerate] operational weapon system development." According to Secretary Griffin, through the DOD's Laser Scaling Program, "four teams are on the path to build 300 kW high-energy lasers by 2022, increasing to 500-1000kW capability over the next decade. We have partnered with the Special Operations Command to accelerate programs for airborne and land-based laser strike weapons, with initial operational capability by Fiscal Year 2024."

Griffin also addressed the early-stage progress in quantum science and its potential uses in the near- and long-term. "While quantum science and technology will be important in the future, they are still in their formative stages. Despite media hype, we are many years from functional quantum computers.

"However, there is justifiable optimism that quantum clocks, magnetometers, and inertial navigation sensors could be available in a few years. Such devices could greatly reduce our dependence on space-based or other external systems for critical position, timing, and navigation functions, an important consideration for military operations in a GPS-denied environment. In R&E, we will work with USG partners from the National Science Foundation to the intelligence community to contribute to quantum computing advances, but our focus will be on deployment of clocks and development of sensors." *– H. Swedeen*

IN BRIEF

In March, the commander of US Army Cyber Command, LTG Stephen Fogarty, announced at AFCEA's 2019 Army Signal Conference that as the service transforms Cyber Command to meet the challenges of the multi-domain battlefield, it will evolve into something new, the working title for which is the Army Information Warfare Operations Command, which would encompass cyber, electronic warfare and information operations. The plan would shift Army information-related operations from Ft. Belvoir, VA, to the current home of Cyber Command at Ft. Gordon, GA, by 2020. The name change, scheduled by 2028, is specifically a title in progress, Fogarty noted, as information operations or information warfare are loaded terms that are also evolving. With cyber and EW capabilities already being revamped, the Service will spend the next 18 months on the information warfare component. Fogarty also announced during the Army Signal Conference that Army Cyber Command plans to put Cyber Electromagnetic Activities (CEMA) teams on the battlefield and into every brigade combat team (BCT), division, corps and Army service component beginning in June.

✪ ✪ ✪

The US Air Force is also shaping some of its organization around information operations by combining Air Combat Command's (ACC's) **24th Air Force** (Air Forces Cyber) and its **25th Air Force** into a single information warfare numbered air force. The 24th Air Force, which was re-aligned from Air Force Space Command to ACC last summer, conducts offensive and defensive cyber operations. The 25th Air Force, which includes the 55th Wing's RC-135 and EC-130H units, focuses on ISR and EW missions. The re-organization should position ACC to provide more effective support of multi-domain operations.

✪ ✪ ✪

The **Missile Defense Agency (MDA)** has issued a Request for Information (RFI) to gather industry input in support of its goal to upgrade the Ballistic Missile Defense System (BMDS) architecture with high power laser solutions that could lead to a laser scaling ground demonstrator within six or seven years. As such, MDA is requesting papers that allow understanding of industry capabilities to demonstrate a 1,000 kW-class electrically-pumped laser by the 2025-2026 timeframe. Concepts should include future options for reduction of size, weight and increasing power, electrical-to-optical efficiency, beam quality and lasing runtime for potential future platforms. The solicitation number is HQ0277-19-RFI-0001. The points of contact are Harris Brown, (505) 853-3307, harris.brown@mda.mil, and Kenneth Arnold, (256) 450-4037, kenneth.arnold@mda.mil. Responses are due by June 5.

✪ ✪ ✪

In late March, **Cubic Corp.** (San Diego, CA) acquired Nuvotronics (Durham, NC) for $64 million in cash. Nuvotronics, which builds antennas, filters and combiners for government, defense and commercial applications, has at its core a manufacturing process called PolyStrata, developed for DARPA to enable RF component production. The acquisition gives Cubic additional solutions to help build growing business in CISR capabilities and to address priority dual-use technologies for space, EW, hypersonic and 5G communications.

ELECTROMAGNETIC
MANEUVER WARFARE
THE VALUE OF
TRANSFORMING
HOW WE FIGHT
—AND WHERE.
Modern battles begin invisibly. That's why Northrop Grumman applies Electromagnetic Maneuver Warfare to seamlessly target and combat enemy threats across any domain. Leveraging traditional spectrum-based and next-generation innovations with our advanced Cyber, C4ISR, Strike, and Autonomous expertise means our forces have a decisive advantage. That's why we're a leader in transformative technologies to defeat tomorrow's threats.
THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN
northropgrumman.com/ew
© 2018 Northrop Grumman Corporation

world report

UK DISCUSSES PLANS FOR FLOATING OFFBOARD DECOY

The UK Ministry of Defence (MoD) has revealed plans to acquire a new passive offboard decoy system to provide soft-kill anti-ship missile defense for Royal Navy (RN) ships.

Known as the Naval Passive Off Board Decoy (N POD) system, the new solution will replace the RN's current Outfit DLF(3b) system. Outfit DLF (3b) was developed and manufactured by IrvinGQ (formerly Airborne Systems Europe). Designed as a floating decoy, the system inflates upon deployment and features multiple corner reflectors to lure radar-guided anti-ship missiles.

In February, the Maritime Combat Systems team within the MoD's Defence Equipment and Support (DE&S) organization advised that it was "considering replacing the current floating offboard decoy system (DLF[3b]) with a similar system," adding that the N POD requirement had been classified UK secret.

Later this year, the Maritime Combat Systems team will issue a pre-qualification questionnaire, with an Invitation to Negotiate following in the October 2019 timeframe. Program officials anticipate issuing a single contract award covering design, development, demonstration, manufacturing and up to five years of service support.


UK MOD

In terms of program schedule, the MOD is expected to award a contract in May 2020. The target "in service" date for N POD is expected to be 2023, with a full operating capability planned for 2025.

A proprietary variant of DLF(3b), given the designation FDS 3 by IrvinGQ, has been sold to the Canadian, New Zealand and US navies. The US Navy has assigned the system with the nomenclature MK 59 Mod 0. – *R. Scott*

AREXIS ESCORT JAMMING POD BEGINS TESTS AHEAD OF FLIGHT TRIALS

Saab's business unit EW has begun to perform ground qualification of a prototype low-band escort jamming pod. The system, which is being developed as part of its wider Arexis family of fast jet EW equipment, is being developed to meet the challenge posed by advanced Russian air defense systems.

The company's EW business unit plans to begin flight testing of the demonstrator system before the end of this year.

The Arexis jammer concept, which was originally introduced by the company in 2017, comprises a family of self- protection, escort jammer and escort jammer extended capability variants. The family of solutions leverages from technology building blocks already in development for the MFS EW self-protection suite developed for the company's JAS 39 Gripen E fighter. These building blocks include ultra wideband digital receivers and digital radio frequency memory devices (DRFMs), gallium nitride (GaN) solid-state active electronically scanned array (AESA) transmitters, interferometric direction finding systems and high speed digital signal processing architectures.

The Arexis pods will be flown in an escort role and will jam early warning radars in support of strike packages. The pod incorporates L band and S band GaN-based AESA antennas in its fore and aft sections. It also features large externally mounted VHF and UHF fin antennas. This version, weighing less than 350 kg, has been specifically designed for integration with single-engine fighters, such as the Gripen.

In 2017, Saab decided to fund the design and integration of a prototype Arexis system at the company's Järfälla, Sweden, facility. After completing environmental testing in the coming months, the company plans to commence a ground trial phase at Järfälla later this year. Flight testing is planned to follow at the end of 2019 on a Gripen D aircraft.

According to the company, the Arexis escort pod draws less than 5 kW of power from the host aircraft. However, the company recognizes that some aircraft will be hard pressed to provide sufficient electrical capacity to power the jammer. As a result, Saab has undertaken engineering studies for a larger, self-powered pod with extended capability. This solution will also incorporate a plug insert for a ram air turbine.

In addition to the Gripen, Saab is offering the Arexis escort jammer pod for other fast jet platforms, including the Eurofighter Typhoon, which has already been identified as a key target platform. – *R. Scott*

Europe's Helicopter Elec

By Andrew White

Reflecting emerging requirements from the contemporary operating environment in eastern Europe, a US Army AH-64 Apache helicopter works alongside a Polish army PT-91 Twardy main battle tank during Exercise Saber Strike 18 at Bemowo Piskie Training Area, June 15, 2018. DVIDS

Following nearly two decades of campaigns conducted in the permissive RF threat environments of the Middle East and Afghanistan, European armed forces are shifting more attention to regional priorities, especially requirements that address so-called near peer and high capability adversaries. Nowhere is this emerging threat more apparent than in eastern Europe, where Russia and its allies have been steadily fielding new air defense systems, including those deployed with its armor and artillery units. In response, NATO partners are seeking to upgrade the electronic warfare (EW) capabilities of their rotary-wing assets to bolster their survivability in the more complex and dangerous threat environments along NATO's eastern border.

In July, the Polish Ministry of National Defence will initiate a strategy to upgrade its legacy inventory of helicopters with next-generation self-protection and EW mission suites. Upgrades, which will initially focus on Mi-24D helicopters, are due to be undertaken between July and September 2019, with technology enhancements potentially being transitioned into more modern air frames, including the newly acquired S-70i Black Hawk and candidate aircraft being considered as part of the Kruk program. This is just one of many emerging helicopter EW programs around Europe which is calling for scalable and modular EW mission suites. In this article, we will take a look at the helicopter EW market across Europe and what types of Aircraft Survivability Equipment (ASE) solutions the region's EW companies are offering.

THE SWEDISH-SOUTH AFRICAN CONNECTION

According to Saab's product manager for airborne self-protection, Martin Vosloo, rotary-wing air frames offer armed forces a versatility not afforded by many fixed-wing aircraft, thereby making them an "integral" part of any military operation or campaign.

Speaking to *JED*, Vosloo described how the availability of "supportive and defensive countermeasures" for helicopters continues to emerge as an increasingly important component to the protection and mission success of military platforms operating in a complex battlefield environment, which is witnessing proliferating levels in radar-, laser-, and infrared (IR)-guided missile threats.

"Missions for combat search and rescue, surveillance and troop transportation are usually not conducted anymore without the availability of a serviceable defensive aids system," Vosloo explained, before outlining an emerging pattern of "need-based" replacement and acquisition upgrades across the military rotorcraft market.

"The presence of an ageing aircraft inventory has led to an increased focus on military forces upgrading their fleets with the latest technologies. Competing budget needs should see militaries compelled to invest in upgrading and modernizing their helicopter fleets to increase the service life of the existing rotary-wing aircraft," he warned.

Observing specific operating requirements across eastern Europe, Saab has noticed a definitive trend away from a focus on protection from shoulder-launched IR-guided missiles toward greater awareness of radar threats from upgraded ex-Soviet weapon systems equipped with modern processing capabilities.

"The advent of digital processing allows for upgrading of those deployed systems with upgraded capabilities," he explained. "In terms of laser threats, a growing presence of beam-rider missile systems have been noted, which in turn necessitates the use of suitable sensors for detecting these challenging systems due to their method of operation."

He further explained, "So the trend has become for forces to install defensive aids against all known threats. For example, where the threats used to be 'undefined,' forces are now preparing themselves more against known threats."

Saab's family of protective solutions includes the Integrated Defensive Aids Suite (IDAS) family of products, which has been designed to enhance the survivability of aircraft across "sophisticated, diverse and dense" threat environments. Comprising a fully integrated, multi-spectral self-protection capability, IDAS provides air crews with tactical situation awareness and early warning of threat activity, which can, in turn, reduce the workload and stress levels of operators, allowing them to concentrate on the core mission.

The IDAS family of solutions includes the IDAS-3 and Compact IDAS (CIDAS). According to Vosloo, CIDAS comprises a smaller and lighter weight variant featuring just EO sensors and a smaller control unit, specifically designed to protect air frames against IR-guided and laser-based threats, many of which are encountered in the currently prevailing peacekeeping environment.

Both IDAS-3 and CIDAS solutions feature the LWS-310 laser warning system, which operates across the 0.5-1.7nm wavelength range to provide threat classification and direction of arrival for laser rangefinders, designators and missile guidance lasers. A total of four laser warning sensors provide a helicopter with 360-degree coverage, with up to six sensors used to provide similar coverage for larger air frames.

Also integrated into IDAS-3 and CIDAS is the MAW-300 missile approach warning system, which features a series of passive ultraviolet (UV) sensors that are capable of detecting and processing multiple targets simultaneously and disseminating data to an EW controller, where information is integrated with inertial navigation systems (INS) information to compensate for platform movement, attitude and altitude. A total of four MAW-300 sensors must be integrated to provide 360-degree protection of an air frame, Saab confirmed.

IDAS-3 and CIDAS, both of which can be upgraded with Digital Receiver (DRx) technology, can also be integrated with Saab's BOP-L advanced lightweight countermeasures dispensing system.

Describing the IDAS's modular system architecture, Vosloo also explained how the various sub-systems within IDAS-3 and CIDAS could be reconfigured for specific mission types. To date, IDAS variants have been integrated on rotary-wing air frames including Oryx, Puma, Cougar/Super Puma, Rooivalk, A109, Super Lynx 300, Dhruv, Chinook and H225M.

As Vosloo explained, Saab remains focused on improving a series of capabilities to enhance the protection capabilities of rotorcraft in the future. Areas of interest include improved radar warning in the presence of communication signal noise and continuous wave (CW) signals; New-technology digital receivers, providing improved performance in respect of sensitivity and frequency channelization allowing improved detection capability against new-generation RF threats in environments with lots of radio frequency (RF) noise; and finally, improved UV missile warning performance capable of detecting old- and new-generation IR-guided threats.

Saab also continues to enhance countermeasure dispensing capabilities with smart and adaptive technology, as well as improved laser warning technology designed to assist in protection levels against new-generation laser threats, including beam riders. Saab also explained how it plans to further optimize Hostile Fire Indication capabilities, using both passive and active technologies, against small arms fire and rocket propelled grenades (RPGs).

ITALIAN INGENUITY

According to Elettronica's corporate chief scientist, Daniela Pistoia, helicopters remain the most exposed military asset in both traditional and emerging conflict scenarios.

"Budget-concerned customers are reasoning according to platform role, and this approach is defining specific self-protection capability and cost procurement plans," she explained to *JED* while describing how requirements can range from standard self-protection suites for utility helicopters through to high-end, multi-spectral solutions for attack or Combat Search and Rescue (CSAR) helicopters.

Discussing existing threat profiles associated with the contemporary op-

One of the UK Royal Navy's latest rotary wing platforms – the AW159 helicopter – is fitted with Leonardo's SAGE ESM solution. LEONARDO

erating environment, Pistoia explained how both guided- and non-guided weapon systems had not changed much over recent years. However, what has changed, Pistoia warned, is the movement toward a more contested electromagnetic spectrum, where the enemy is using all possible means to degrade friendly combat capabilities through a mix of hybrid or information warfare.

"All scenarios, including urban environments, require a very fast EOB recognition," Pistoia explained, before describing how unmanned aerial vehicles (UAVs), operating in swarms or as loitering munitions, also represent a new threat to rotary-wing air frames.

Seeking to overcome many of these emerging operational requirements, Elettronica has identified RF and EO enhancements to legacy protection systems.

Solutions include gallium nitride (GaN) and Quantum Cascade Laser (QCL) technologies which, according to Pistoia, are capable of supporting existing systems in self-protection electronic attack (EA); all-signal processing innovations for EW support and specific emitter identification; low-probability-of-intercept (LPI) detection; and adaptive (i.e., machine learning) solutions.

"This is enabled by analog-to-digital wideband conversion and artificial intelligence," Pistoia said. However, she warned, "What should not be overlooked is the importance of the networking technology that allows a multi-platform EW layer of real-time and overall EOB awareness and electronic attack. This represents a big step ahead: The technology is mature, but what needs to be worked on is the doctrine and the connectivity."

Elettronica's helicopter EW solutions include the Virgilius Integrated System, which comprises a multifunction unit equipped with DF antennas, low-band solid-state transmitters, and medium-band and high-band active phased array transmitters, providing simultaneous ESM and ECM capabilities.

Virgilius supports RF emitter recognition in high-density electromagnetic environments, multi-threat jamming against simultaneous threats, direction finding and passive location, and ac-

The MILDS AN/AAR-60 MWS is designed to detect, track and provide warning of threatening missiles at maximum range.
HENSOLDT

quisition and tracking of sidelobe emissions, Pistoia explained.

Elettronica has also designed the ELT-572 directed infrared countermeasures (DIRCM) system, which features a mirror turret, laser generator unit and an electronic control unit, which can be integrated with missile warning systems to provide end users with rapid reaction to multiple and simultaneous MANPAD threats.

Both Virgilius Integrated System and EO ELT-572 Direct Infrared Countermeasure (DIRCM) active and passive countermeasure technologies are already integrated onboard the Italian Air Force's CSAR AW-101 helicopter. According to Pistoia, integration remains ongoing with the solution currently installed and undertaking flight tests onboard the AW101 helicopter.

Elettronica also confirmed how the latest ELT162 multispectral EW system and ELT-600 DIRCM have already been made available to customers. Featuring a newly designed form factor, the ELT-600 DIRCM, designated EuroDIRQM and currently in development with Spanish EW company Indra, provides end users with protection against any IR-guided threat based on thermal trackers up to 3rd generation (signal processing-based seekers) and up to 4th generation when in cooperation with flares. Supported by QCL technology, the EuroDIRQM can also be integrated with a solid-state multi-band high-power laser to further extend protection levels while also providing jamming on target within 700m/sec of a threat declaration from a missile warning system. Pistioa added that the ELT-600 can also be integrated onboard any large body helicopter also equipped with a legacy self-protection suite.

Saab's Integrated Defensive Aids Suite (IDAS) family of products has been designed to enhance the survivability of aircraft across "sophisticated, diverse and dense" threat environments. SAAB

SMART SUITES FOR THE UK

According to Kyle Alexander, head of EW rotary campaigns at Leonardo, platform protection also remains a critical capability requirement for military helicopters in the contemporary operating environment.

Describing how most rotary-wing upgrade and new build procurement programs now include some kind of EW requirement, Alexander highlighted to *JED* how capabilities demanded would depend upon expected mission tasks and areas of operation for the platform in question.

"MANPAD missile warning and countermeasures (flare dispensing or DIRCM) remain a core requirement for 'low and slow' aircraft such as helicopters," he explained. "As potential operating environments develop, requirements for RF sensors and effectors are increasingly common, as are systems that will address latest generation threats and Integrated Air Defense Systems (IADS)."

However, Alexander observed, evolving threats continue to drive EW requirements, which continue to be fulfilled through the parallel development of sensor and countermeasure capabilities. "Sensor development is required to be able to accurately detect signature and launch events, while countermeasure development is required to successfully address new-generation systems and IADS," he said.

Leonardo's helicopter EW offerings include the SEER radar warning receiver

(RWR) which has been designed to provide "highly accurate, high-fidelity and instantaneous threat detection and aircrew notification." Available in E- to J-, C- to D- and E- to K-band configurations, SEER can be integrated into legacy multimission displays to assist air crew in the identification and reporting of radar threats. Comprising an 11kg payload, SEER supports direction finding at less than 10 degrees RMS, while pulsed/pulsed Doppler/ CW technology supports the detection of threats. The solution is also equipped to support mission recording capacity for up to 20 hours.

AgustaWestland's AW101 continues to be upgraded with EW mission suites, including Elettronica solutions for the Italian Air Force's CSAR platform. LEONARDO

Another Leonardo offering, the SAGE ESM system, has been designed to provide growth potential toward more strategic EW intelligence gathering and analysis of the EW/threat environment whilst maintaining tactical threat awareness. Featuring a series of direction-finding antennas, SAGE features a dual-role ESM/RWR, allowing it to "pinpoint" targets; identify weapon systems; and enable users to discern tactics, techniques and procedures of enemy forces as well as cueing external sensors, jamming and electronic attack systems. Operating from 0.5 GHz to 40 GHz, SAGE provides a one-degree direction finding accuracy according to the company.

Leonardo also offers the Miysis DIRCM, which provides full spherical coverage against advanced IR threats. Miysis DIRCM has been designed with a modular and open architecture design, which allows for its integration with a customer's in-service missile approach warners and other defensive aids systems.

SAGE and SEER are supported by Leonardo's EW Operational Support (EWOS) tools for mission data programming and replay. Such a capability, Alexander continued, allows armed forces to optimize the utility of SAGE as well as providing the ability to independently update the system to recognize new threats as they arrive in theater.

According to Leonardo, the wider integration of these various sub-systems into an "Intelligent IDAS" increases survivability levels of an air frame through data correlation and mission management, reduced aircrew workload, prioritization of threats and cueing of the most effective countermeasures.

"Our work to integrate the latest subsystems into our IDAS offering includes partnering with Thales to integrate their Elix-IR Threat Warning System with our Miysis DIRCM and developing our capacity to work with forthcoming smart countermeasure dispensers," Alexander explained. He also noted the launch of Leonardo's BriteCloud 55-T Off-Board Expendable Active Decoy in 2018, which is also suitable for rotary wing platforms.

Leonardo continues to supply Boeing and the US Army with delivery of the Aircraft Gateway Processor (AGP) in support of the AH-64 Apache program. According to Alexander, every AH-64 which comes off the Boeing production line for all customers now features an integrated the AGP DAS computer, which he describes as the EW controller for the ASE suite. Elsewhere, Leonardo is also contracted to support the British Army's fleet of AH-64E Apaches with EW protection equipment. The news follows an April 2018 contract from the UK Ministry of Defence tasking Leonardo to provide DAS for the British Army's inventory of Apaches.

In addition to the built-in Leonardo AGP, the company is integrating the SG200-D radar warning receiver (the UK-specific variant of the company's SEER family) and is re-using a number of systems that are currently onboard the British Army's fleet of Apache AH Mk1, including Leonardo's S1223 laser warning receiver, the AN/AAR-57 Common Missile Warning System from BAE Systems and the Thales Vicon countermeasure dispensing system. Existing UK Apache AH Mk1 helicopters are equipped with the company's Helicopter Integrated Defensive Aids Suite (HIDAS) system. Leonardo also provides HIDAS to the British Army and Royal Navy AW159 Wildcat helicopters.

Leonardo is also contracted to retro-fit the UK MoD's inventory of CH-47 Chinook helicopters, including the latest HC Mk 6, with DAS technologies. Under this project, Leonardo has combined all of the Chinook's existing sensor and effector systems into an integrated system that offers suite management capabilities similar to the HIDAS system. Comparable upgrades have also been made to the UK's Puma and Merlin fleets, Alexander added. Similar to the Apache AH-64E, both Royal Air Force Puma and Chinook fleets are also receiving updated radar warning capabilities in the form of Leonardo's SG200-D RWR.

GERMANY PUSHES EW DEVELOPMENT

Germany's Hensoldt sees helicopters challenged by a variety of threats, including laser-guided missiles, IR missiles, radar-guided missiles, rocket-propelled grenades and tracer munitions. The company notes that a significant number of helicopters worldwide are still either unprotected or have gaps in their protection level.

As a result, Erich Wagenbauer, head of self-protection sales at Hensoldt, explained how the company is seeking to assist customers aiming to overcome many of these existing capability gaps. Areas of interest include protection against MANPADS and rocket propelled grenades (RPGs) by reliable missile warning and Hostile Fire Indication systems, as well as protection against laser-guided threats, including target designators and laser beam-riding missiles.

Hensoldt's product manager for electronic support, Frank Kessler, explained, "Conventional radar warning receivers cannot cope with new radar threats such as LPI radars [radars with complex intra-modulation using wider frequency ranges] and congested spectrum [expansion of mobile communications signals requires more sophisticated digital spectrum monitoring]."

Hensoldt solutions include the Airborne Missile Protection System (AMPS), which is capable of accommodating a variety of warning sensors, countermeasures and avionic equipment to protect rotorcraft from IR, laser or radar guided missiles.

The AMPS is capable of supporting UV missile warning systems as well as active confirmation sensors which have been designed to "virtually" eliminate false alarms at a systems level, Hensoldt officials said.

"We are working on a combination of a passive MWS (MILDS) and an active confirmation sensor to provide reliable detection of RPGs fired against helicopters," Wagenbauer described while confirming how Hensoldt's UV MWS could be used in an HFI function to detect hostile fire without requirement for additional sensors and equipment.

The MILDS AN/AAR-60 MWS is designed to detect, track and provide warning of threatening missiles at maximum range, including rapid discrimination of stationary and moving UV point sources. This, according to Wagenbauer, supports operations in urban environments with a minimal false alarm rate. MILDS, which can also feature HFI technology, can also support multi-threat handling of up to eight targets per system, it was added. Wagenbauer said that Hensoldt EW equipment is already installed on more than 20 helicopter platform types, including the H135M, H145M, H215, H225, UH60, CH-47, Bell 407, CH-53 and Mi-17 air frames.

Seeking to future-proof its technology, Hensoldt is also in the process of developing a new generation of fully digital radar warning receivers which, Kessler claimed, will be able to handle "all current scenarios and provide inherent growth potential by means of artificial intelligence methods." A new product will be introduced into the market before the end of the second quarter of 2019, Hensoldt confirmed.

SPAIN'S QUEST FOR SPECTRUM DOMINANCE

Finally, Spanish company Indra has identified a growing market in self-protection and sensor technology for helicopters, which can be associated with current utility of helicopters as well as an "eruption" in new designs of Vertical Take-Off and Landing (VTOL) capabilities, including unmanned aerial vehicles (UAVs).

As Raul Pajarin, responsible for the airborne segment within Indra's platforms business line, described to *JED*, "big and slow" helicopters require greater levels in self-protection across an increasingly contested operating environment.

"For rotary-wing platforms, self-protection capabilities are subject to improvements because these types of platforms are an easier target compared to other platforms. Also, communications is an area of big improvement, with more bandwidth of operation for data links, more immunity against interference, better crypto-protection and permanent connection (including satellite comms) demanded."

According to Indra, spectrum dominance will play a major role in future helicopter requirements. Hence the reason why the company remains focused on the "direct digitization of the environment at sensor level (including Radar, IR and communications) in order to provide a full instantaneous view and immunity against all kinds of interference, especially for helicopters or slow motion rotary wing platforms in urban areas." Also identifying its co-developed EuroDIRQM with Elettronica as an improved self-protection solution based on QCL technology, Indra remains focused on the miniaturization of sub-systems to reduce size, weight and power.

Working in close collaboration with the Spanish MoD, Indra continues to research radar mission systems for rotary wing platforms which, according to the company, are close to entering the market. Indra solutions include an EWS system for a range of helicopters, including NH90, Tiger, Cougar, Chinook (Spanish MoD), Cougar and CH53GA in Germany.

LOOKING TO THE FUTURE

Beyond urgent operating requirements associated with the contemporary battlespace, European industry players are also considering the future of the rotary-wing self-protection solutions.

As Saab's Vosloo explained: "We foresee EW becoming standard fit for an increased number of military platforms, and not only for special-mission rotary-wing aircraft, due to the threat environment. This will also drive an increase in replacing and upgrading legacy EW systems with new systems."

Looking further ahead, European market players are paying significant attention to increased networking capabilities between multiple platforms and sensors across a single battlespace. As an example, Vosloo highlighted how "sensor fusion" over multiple platforms will enhance capabilities to increase levels in detection accuracy. Similar observations were echoed by Elettronica's Pistoia, who described how Manned-Unmanned Teaming (MUM-T) concepts of operation would also assist a future "breakthrough" for rotary wing self-protection systems.

Finally, Leonardo's Alexander predicted an increase in RF sensor and countermeasure requirements, driven by threat system development and proliferation.

"To understand and address a complex and congested threat environment, there will be an increase in intelligent system linking and the utilization of data. We are expecting to see increased utilization of open-architectures and 'app-able' software which will provide flexibility with minimal integration, qualification and certification effort," he concluded.

FUTURE ELECTRONIC COHERENT, DISTRIBU

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.

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 valu-

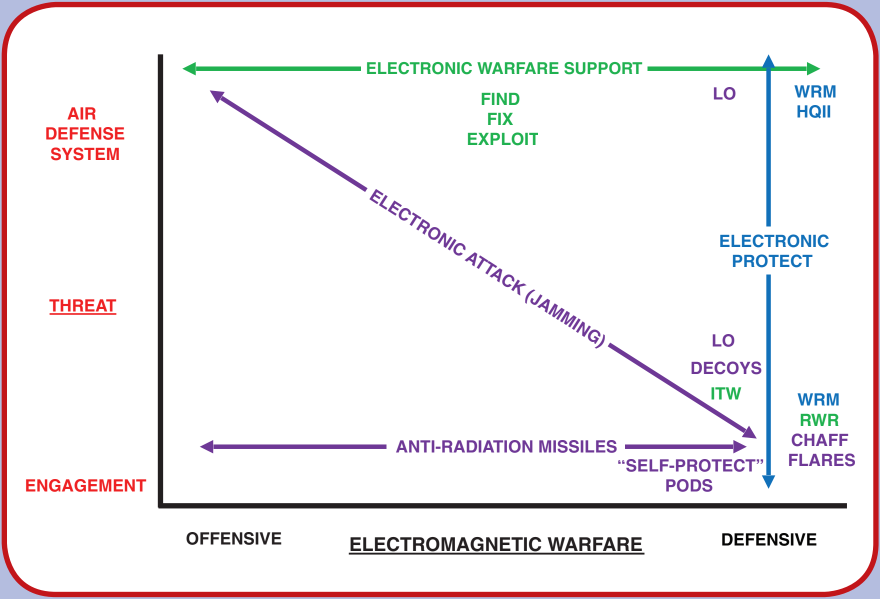


Figure 1. Electromagnetic Warfare versus Threat Scale.

ATTACK:
TED AND CHEAP

able. 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.

1 For a more thorough discussion of these concepts, see "Fighting the Kill Chain: Concepts and Methods of Electronic Attack" JED, May 2014

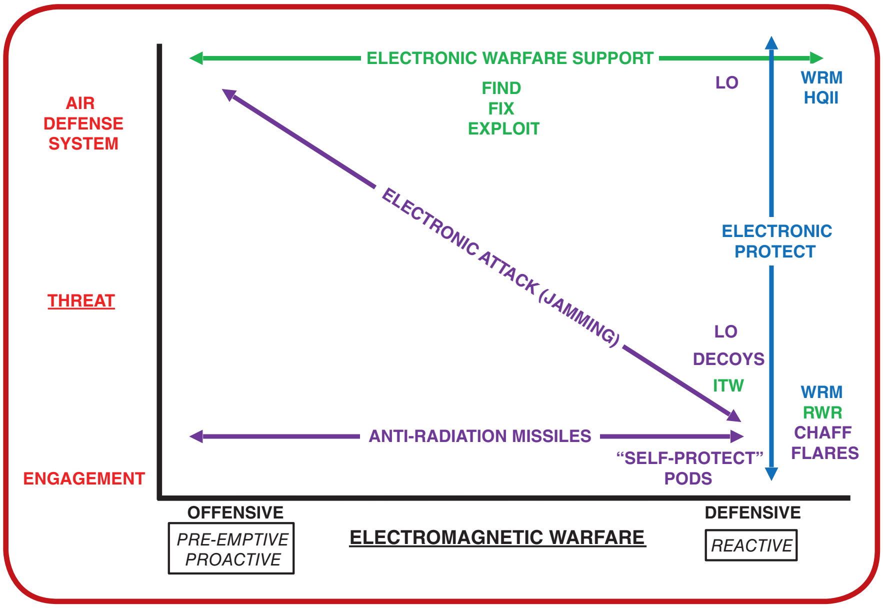


Figure 2. Electromagnetic Warfare Targeting versus Threat Scale

What is our plan to counter and attack Red when the IADS moves to bistatic, 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.**

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.

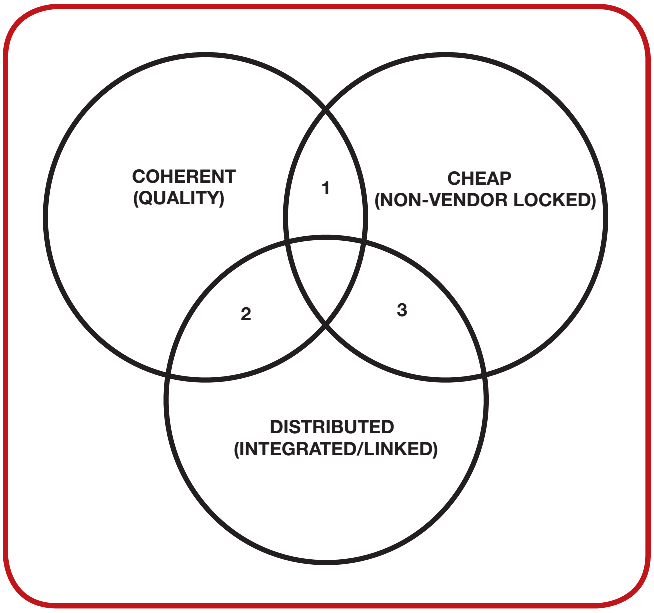


Figure 3. Electronic Attack Triple Constraint

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.

RF Amplifiers and Sub-Assemblies for Every Application

Delivery from Stock to 2 Weeks ARO from the catalog or built to your specifications!

- Competitive Pricing & Fast Delivery
- Military Reliability & Qualification
- Various Options: Temperature Compensation, Input Limiter Protection, Detectors/TTL & More
- Unconditionally Stable (100% tested)

ISO 9001:2000 and AS9100B CERTIFIED

OCTAVE BAND LOW NOISE AMPLIFIERS

Model No.	Freq (GHz)	Gain (dB) MIN	Noise Figure (dB)	Power-out @ P1-dB	3rd Order ICP	VSWR
CA01-2110	0.5-1.0	28	1.0 MAX, 0.7 TYP	+10 MIN	+20 dBm	2.0:1
CA12-2110	1.0-2.0	30	1.0 MAX, 0.7 TYP	+10 MIN	+20 dBm	2.0:1
CA24-2111	2.0-4.0	29	1.1 MAX, 0.95 TYP	+10 MIN	+20 dBm	2.0:1
CA48-2111	4.0-8.0	29	1.3 MAX, 1.0 TYP	+10 MIN	+20 dBm	2.0:1
CA812-3111	8.0-12.0	27	1.6 MAX, 1.4 TYP	+10 MIN	+20 dBm	2.0:1
CA1218-4111	12.0-18.0	25	1.9 MAX, 1.7 TYP	+10 MIN	+20 dBm	2.0:1
CA1826-2110	18.0-26.5	32	3.0 MAX, 2.5 TYP	+10 MIN	+20 dBm	2.0:1

NARROW BAND LOW NOISE AND MEDIUM POWER AMPLIFIERS

Model No.	Freq (GHz)	Gain (dB) MIN	Noise Figure (dB)	Power-out @ P1-dB	3rd Order ICP	VSWR
CA01-2111	0.4 - 0.5	28	0.6 MAX, 0.4 TYP	+10 MIN	+20 dBm	2.0:1
CA01-2113	0.8 - 1.0	28	0.6 MAX, 0.4 TYP	+10 MIN	+20 dBm	2.0:1
CA12-3117	1.2 - 1.6	25	0.6 MAX, 0.4 TYP	+10 MIN	+20 dBm	2.0:1
CA23-3111	2.2 - 2.4	30	0.6 MAX, 0.45 TYP	+10 MIN	+20 dBm	2.0:1
CA23-3116	2.7 - 2.9	29	0.7 MAX, 0.5 TYP	+10 MIN	+20 dBm	2.0:1
CA34-2110	3.7 - 4.2	28	1.0 MAX, 0.5 TYP	+10 MIN	+20 dBm	2.0:1
CA56-3110	5.4 - 5.9	40	1.0 MAX, 0.5 TYP	+10 MIN	+20 dBm	2.0:1
CA78-4110	7.25 - 7.75	32	1.2 MAX, 1.0 TYP	+10 MIN	+20 dBm	2.0:1
CA910-3110	9.0 - 10.6	25	1.4 MAX, 1.2 TYP	+10 MIN	+20 dBm	2.0:1
CA1315-3110	13.75 - 15.4	25	1.6 MAX, 1.4 TYP	+10 MIN	+20 dBm	2.0:1
CA12-3114	1.35 - 1.85	30	4.0 MAX, 3.0 TYP	+33 MIN	+41 dBm	2.0:1
CA34-6116	3.1 - 3.5	40	4.5 MAX, 3.5 TYP	+35 MIN	+43 dBm	2.0:1
CA56-5114	5.9 - 6.4	30	5.0 MAX, 4.0 TYP	+30 MIN	+40 dBm	2.0:1
CA812-6115	8.0 - 12.0	30	4.5 MAX, 3.5 TYP	+30 MIN	+40 dBm	2.0:1
CA812-6116	8.0 - 12.0	30	5.0 MAX, 4.0 TYP	+33 MIN	+41 dBm	2.0:1
CA1213-7110	12.2 - 13.25	28	6.0 MAX, 5.5 TYP	+33 MIN	+42 dBm	2.0:1
CA1415-7110	14.0 - 15.0	30	5.0 MAX, 4.0 TYP	+30 MIN	+40 dBm	2.0:1
CA1722-4110	17.0 - 22.0	25	3.5 MAX, 2.8 TYP	+21 MIN	+31 dBm	2.0:1

ULTRA-BROADBAND & MULTI-OCTAVE BAND AMPLIFIERS

Model No.	Freq (GHz)	Gain (dB) MIN	Noise Figure (dB)	Power-out @ P1-dB	3rd Order ICP	VSWR
CA0102-3111	0.1-2.0	28	1.6 Max, 1.2 TYP	+10 MIN	+20 dBm	2.0:1
CA0106-3111	0.1-6.0	28	1.9 Max, 1.5 TYP	+10 MIN	+20 dBm	2.0:1
CA0108-3110	0.1-8.0	26	2.2 Max, 1.8 TYP	+10 MIN	+20 dBm	2.0:1
CA0108-4112	0.1-8.0	32	3.0 MAX, 1.8 TYP	+22 MIN	+32 dBm	2.0:1
CA02-3112	0.5-2.0	36	4.5 MAX, 2.5 TYP	+30 MIN	+40 dBm	2.0:1
CA26-3110	2.0-6.0	26	2.0 MAX, 1.5 TYP	+10 MIN	+20 dBm	2.0:1
CA26-4114	2.0-6.0	22	5.0 MAX, 3.5 TYP	+30 MIN	+40 dBm	2.0:1
CA618-4112	6.0-18.0	25	5.0 MAX, 3.5 TYP	+23 MIN	+33 dBm	2.0:1
CA618-6114	6.0-18.0	35	5.0 MAX, 3.5 TYP	+30 MIN	+40 dBm	2.0:1
CA218-4116	2.0-18.0	30	3.5 MAX, 2.8 TYP	+10 MIN	+20 dBm	2.0:1
CA218-4110	2.0-18.0	30	5.0 MAX, 3.5 TYP	+20 MIN	+30 dBm	2.0:1
CA218-4112	2.0-18.0	29	5.0 MAX, 3.5 TYP	+24 MIN	+34 dBm	2.0:1

LIMITING AMPLIFIERS

Model No.	Freq (GHz)	Input Dynamic Range	Output Power Range Psat	Power Flatness dB	VSWR
CLA24-4001	2.0 - 4.0	-28 to +10 dBm	+7 to +11 dBm	+/- 1.5 MAX	2.0:1
CLA26-8001	2.0 - 6.0	-50 to +20 dBm	+14 to +18 dBm	+/- 1.5 MAX	2.0:1
CLA712-5001	7.0 - 12.4	-21 to +10 dBm	+14 to +19 dBm	+/- 1.5 MAX	2.0:1
CLA618-1201	6.0 - 18.0	-50 to +20 dBm	+14 to +19 dBm	+/- 1.5 MAX	2.0:1

AMPLIFIERS WITH INTEGRATED GAIN ATTENUATION

Model No.	Freq (GHz)	Gain (dB) MIN	Noise Figure (dB)	Power-out @ P1-dB	Gain Attenuation Range	VSWR
CA001-2511A	0.025-0.150	21	5.0 MAX, 3.5 TYP	+12 MIN	30 dB MIN	2.0:1
CA05-3110A	0.5-5.5	23	2.5 MAX, 1.5 TYP	+18 MIN	20 dB MIN	2.0:1
CA56-3110A	5.85-6.425	28	2.5 MAX, 1.5 TYP	+16 MIN	22 dB MIN	1.8:1
CA612-4110A	6.0-12.0	24	2.5 MAX, 1.5 TYP	+12 MIN	15 dB MIN	1.9:1
CA1315-4110A	13.75-15.4	25	2.2 MAX, 1.6 TYP	+16 MIN	20 dB MIN	1.8:1
CA1518-4110A	15.0-18.0	30	3.0 MAX, 2.0 TYP	+18 MIN	20 dB MIN	1.85:1

LOW FREQUENCY AMPLIFIERS

Model No.	Freq (GHz)	Gain (dB) MIN	Noise Figure dB	Power-out @ P1-dB	3rd Order ICP	VSWR
CA001-2110	0.01-0.10	18	4.0 MAX, 2.2 TYP	+10 MIN	+20 dBm	2.0:1
CA001-2211	0.04-0.15	24	3.5 MAX, 2.2 TYP	+13 MIN	+23 dBm	2.0:1
CA001-2215	0.04-0.15	23	4.0 MAX, 2.2 TYP	+23 MIN	+33 dBm	2.0:1
CA001-3113	0.01-1.0	28	4.0 MAX, 2.8 TYP	+17 MIN	+27 dBm	2.0:1
CA002-3114	0.01-2.0	27	4.0 MAX, 2.8 TYP	+20 MIN	+30 dBm	2.0:1
CA003-3116	0.01-3.0	18	4.0 MAX, 2.8 TYP	+25 MIN	+35 dBm	2.0:1
CA004-3112	0.01-4.0	32	4.0 MAX, 2.8 TYP	+15 MIN	+25 dBm	2.0:1

CIAO Wireless can easily modify any of its standard models to meet your "exact" requirements at the Catalog Pricing.

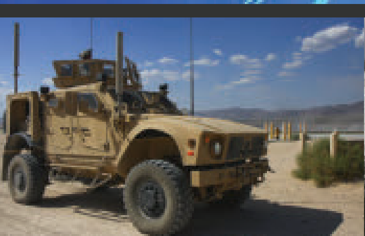
Visit our web site at **www.ciaowireless.com** for our complete product offering.

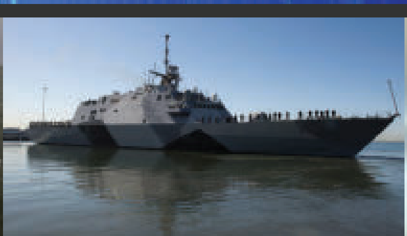
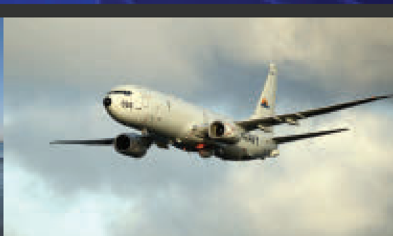
Ciao wireless

Ciao Wireless, Inc. 4000 Via Pescador, Camarillo, CA 93012

Tel (805) 389-3224 Fax (805) 389-3629 sales@ciaowireless.com


MULTI-CHANNEL
SOFTWARE DEFINED RADIOS
Enabling Critical Warfighter Missions Worldwide



TECHNOLOGY SURVEY

A SAMPLING OF COUNTER-UAS SYSTEMS

By John Knowles and Hope Swedeen

The market for counter-UAS systems, also known as counter-drone systems, is not even 10 years old, but it has seen explosive growth across military, government and civilian applications. The drones they are designed to detect and defeat are often small, inexpensive and simple to operate. Their payload is typically a camera providing real-time, full motion video that is data-linked back to the operator. But some users have weaponized these drones, as well, which makes them higher-priority threats. These drones are everywhere, and this market factor, more than any other, is driving the strong demand for counter-UAS systems.

Drones are heavily dependent on accessing the Electromagnetic Spectrum (EMS). They use the EMS for the command link from the operator to the drone, for the camera sensor, for the datalink from the drone back to the operator, and sometimes for GPS/GNSS-based navigation. As a result, drones are vulnerable to passive RF detection, identification and tracking, as well as RF jamming and EO/IR jamming. Thus, many counter-UAS systems employ electronic attack subsystems as part of their countermeasures suites.

Over the past several years, the user base has become more sophisticated about defining requirements. A Brigade Combat Team, for example, may have a need for a deployable counter-UAS system that can detect and engage multiple drones at longer ranges, and it may be primarily interested in quickly damaging or destroying the drone(s). On the other hand, a requirement to protect a government facility may emphasize multiple sensors integrated with a command and control system and countermeasures that are more automated (to minimize the man-power needed to operate the system). The counter-UAS system may also be integrated with other facility security systems. In another example, a counter-UAS system that is protecting a public event typically needs to be deployable, perhaps operate at shorter ranges and employ non-kinetic countermeasures that enable security personnel to take control of a drone's command link and to safely land it away from crowds.

With such an evolving variety of users and requirements, industry has responded with a wider range of counter-UAS solutions. Some are as simple as a hand-pointed, high-gain directional antenna connected to a backpack-mounted control unit and battery. This type of system relies on the operator's eyes and ears as sensors and is typically designed for short-range engagements. Others are more sophisticated, with multiple sensors, such as radar, EO/IR and ESM systems, a command and control system and multiple types of kinetic and non-kinetic countermeasures.

Comparing this month's survey to *JED*'s first Counter-UAS Survey in September 2017, one continuing trend is companies offering a range of counter-UAS solutions, with each one suited to different sets of customer requirements. The industry's use of teaming and partnerships also remains strong, as new players emerge with partial solutions that are competitive either in terms of price or performance.

A few of the larger defense electronics companies are beginning to commit more resources to counter-UAS opportunities, especially for programs with unique military requirements. A few of them are reflected in this survey, but most of these companies are working under development contracts from the DOD to adapt high-energy laser (HEL) or high-power microwave (HPM) technologies to meet counter-UAS requirements.

This month's survey differs slightly from the previous counter-UAS survey (from September 2017) in that we included systems that only provide ESM and DF detection and tracking systems. (Our previous survey only included systems that provided an integrated countermeasures solution.) Most of these "detection and tracking-only" types of systems interface with multiple third-party countermeasures solutions. Several new companies are listed, as well, which reflects how rapidly the market is growing.

THE SURVEY

In the survey table, the first column lists the model name. Working from left to right, the next two columns cover the sensors used to detect and track the drones. (In the case of manpack "drone guns," the detection and tracking columns are empty because the "sensors" are usually the human operator.) The next column indicates if the system provides a direction finding (DF) capability, which is useful in locating the drone as well as the drone operator. The next column indicates if the counter-UAS system features a command and control capability with a workstation or other type of user interface. The next few columns cover the system's countermeasures performance characteristics, such as techniques, range and operating frequencies. The remaining columns list configuration, size and weight.

Next month, *JED*'s technology survey will focus on airborne EW self-protection suites.

COUNTER-UAS SYSTEMS

MODEL	DETECTION SENSORS	TARGET TRACKING SENSORS	DF SYSTEM	C2 SYSTEM	COUNTERMEASURES
Allen-Vanguard; Ottawa, Ontario, Canada; +1 613-739-9646; www.allenvanguard.com					
ANCILE	Communication interface capability to link to other partnering detection systems.	*	No	Yes	Selective RF spectrum jamming and GPS/GNSS jamming with range of specialized algorithms
ApolloShield; New York City, NY, USA / Tel Aviv, Israel; +1 888-474-5646; www.apolloshield.com					
ApolloShield C-UAS	RF, radar, EO/IR	RF, radar, EO/IR	Yes	Yes	RF jamming, control link disruption, GNSS jamming, non-jamming De-Sync selective protocol manipulation
ApolloShield Portable C-UAS	RF	RF	Opt.	Yes	RF jamming, control link disruption, GNSS jamming
RFG Counter-Drone RF Gun	*	*	*	*	RF jamming, control link disruption, GNSS jamming
ASELSAN; Ankara, Turkey; 90 (312) 592 10 00; aselsan.com.tr					
iHTAR	ACAR Ku-Band Pulse Doppler Radar	HSY EO System	*	Yes	GERGEDAN RF jamming system
iHAVASAR	*	*	*	*	RF jammer
Battelle; Columbus, OH, USA; +1 800-201-2011; www.battelle.org					
Drone Defender	*	*	*	*	RF jamming, control link disruption, GNSS jamming
CACI International, Inc.; Alexandria, VA, USA; +1 703-707-2509; www.caci.com					
SkyTracker® CORIAN™	ESM (RF), EO/IR, DF	ESM (RF), EO/IR, DF	Yes	Yes	RF barrage jamming; control link disruption/manipulation, GPS/GNSS jamming
SkyTracker® AWAIR™	ESM (RF), EO/IR, DF	ESM (RF), EO/IR, DF	Yes	Yes	RF barrage jamming; control link disruption/manipulation, GPS/GNSS jamming
SkyTracker® Small Form Factor	ESM (RF), EO/IR, DF	ESM (RF), EO/IR, DF	Yes	Yes	RF barrage jamming; control link disruption/manipulation, GPS/GNSS jamming
CerbAir; Boulogne-Billancourt, France; +33 9 72 62 58 58; www.cerbair.com					
CerbAir Stationary Unit	DW-RF-01 RF detector; DW-OP-01 EO sensor	*	*	Yes	RF jamming, control link disruption, GNSS jamming

COUNTERMEASURES RANGE	JAMMING FREQ./ BANDS	PLATFORM	SIZE (in./cm)	WEIGHT (lb/kg)	FEATURES
Government formal competitive test results available	Addresses all sUAS including GNSS based systems; fully programmable to address future threats	Grd-fix, grd-mob, man-portable	Two cases for quick deploy config: one case, 48 x 48 x 40 cm; second case, 64 x 48 x 44 cm	Two cases for quick deploy config: one case, 12 kg; second case, 38 kg	Fielded to protect the G7 leadership; delivers ahemispherical (360/180) dome of protection; sectored antenna solutions for bespoke installations if required.
Up to 3 km	2.4 GHz, 5.8 GHz, GNSS/GLONASS, 433 MHz, 900 MHz, 1.2 GHz, custom bands non-jamming selective De-Sync available in same frequencies	Grd-fix, grd-mob	Config dep.	Config dep.	Modular detect, track, identify and defeat system. Fully autonomous operation and white list capabilities.
Up to 1 km	2.4 GHz, 5.8 GHz, GNSS/GLONASS, 433 MHz, 900 MHz, 1.2 GHz, custom bands non-jamming selective De-Sync available in same frequencies	Man-portable	*	15 kg / 33 lb	Autonomous, hands-free operation; optional – advanced control by operator.
Up to 1 km	2.4 GHz, 5.8 GHz, GNSS/GLONASS, 433 MHz, 900 MHz, 1.2 GHz, custom bands non-jamming selective De-Sync available in same frequencies	Man-portable	*	4 kg / 9 lb	Lightweight counter-drone gun; versions available with or without a backpack unit.
*	GPS, Wi-Fi, ISM, GSM 900/1800, 3G and 4G	Grd-fix	*	*	ACAR features track while scan in surveillance mode, 360 degree sector scanning and a detection range of 5km against targets with RCS of 0.5 m^2.
*	400 MHz - 3 GHz; 5.7-5.9 GHz	Manpack	*	*	Manually directed; 50-w RF output power; high-gain directional antenna; 1.5 hr operation from Li-Ion batteries.
400m	*	Man-portable	Less than 15 lb	*	Battery power runs up to 5 hours continuously.
10 km	20 MHz - 6.1 GHz	Grd-fix	132 in. (min) - 294 in. (max) (H) x 60 in. (W) x 78 in. (D)	626 lb	Detect, track and defeat individual drones or multiple drones simultaneously. Includes the ability to view and jam video link and the ability to geolocate the drone and drone receiver.
5 km	20 MHz - 6.1 GHz	Grd-mob	6 (H) x 20 (W) x 24 (D) in.	163 lb	Detect, track and defeat individual drones or multiple drones simultaneously; utilizes user-friendly GUI.
2 km	20 MHz - 6.1 GHz	Man portable	12 (H) x 5.3 (W) x 4 (D) in.	9 lb	Includes the ability to view and jam video link and the ability to geolocate the drone and drone receiver.
Up to 1 km	432-436 MHz; 900-1170 MHz; 1171-1380 MHz; 1570-1620 MHz; 2400-2500 MHz; 5-5.4 GHz; 5.4-5.9 GHz	Grd-fix	*	*	SESP jammer optional.

MODEL	DETECTION SENSORS	TARGET TRACKING SENSORS	DF SYSTEM	C2 SYSTEM	COUNTERMEASURES
D-Fend Solutions, Ltd; Ra'anana, Israel; sales@d-fendsolutions.com; www.d-fendsolutions.com					
EnforceAir™	Passive comm	Comm	*	Part of the product, optional API	Cyber / communication
Dedrone; San Francisco, CA, USA; +1 415-813-6116; www.dedrone.com					
Drone Tracker	RF detector; audio, near IR, Wi-Fi sensor, EO (daylight)	*	*	Yes	RF jamming, GNSS jamming
Department 13; Columbia, MD, USA; +1 410-989-5313; www.department13.com					
MESMER	RF detector	*	*	*	RF control link protocol manipulation
Diehl Defence GmbH; Überlingen, Germany; +49 7551 89-01; http://drohnenabwehr.de					
Guardion	ESM	ESM	Yes	TARANIS	RF jcontrol link jammer, Wi-Fi disruptor; GNSS jamming, HPEM
DroneShield; Sydney, Australia; +61 2 9995 7280; www.droneshield.com					
DroneSentry	Radar, RF DF	Radar, EO/IR, RF DF	Yes	Yes	RF barrage jamming, command link control, GPS/GNSS jamming
DroneGun Tactical	*	*	No	No	RF barrage jamming, command link control, GPS/GNSS jamming
DroneNode	*	*	No	No	RF barrage jamming, command link control, GPS/GNSS jamming
Elbit Systems EW and SIGINT - Elisra; Holon, Israel; +972-77-293-9798; www.elbitsystems.com/elisra					
ReDrone	DF, geolocation, radar, EO/IR, acoustic	DF, Geo-location, radar, ESM, EO/IR, acoustic	DF of drone and operator	Map-based display	Command link jamming; GPS/GNSS jamming
Elettronica Group - ELT GmbH; Meckenheim, Germany; +49 2225 88060; www.elettronicagroup.com					
MUROS-S (c-UAS configuration)	Radar 2D FMCW, RF interceptor	Radar 3D FMCW, EO/IR Tracking Unit, low-end RF DF	Yes	Yes	*
Elettronica Group - ELT Roma; Rome, Italy; +39 06 41541; www.elt-roma.com					
ADRIAN	Radar 2D, radar 3D, EO/IR, acoustic, ESM, DF	Radar2D, Radar 3D, EO/IR, Acoustic, ESM, DF	Yes	Yes	RF barrage jamming, RF selective jamming, cyber attack to take control of a drone's command link, GPS/GNSS jamming, GPS spoofing
Elta Systems Ltd.; Ashdod, Israel; +972-8-857-2312; www.iai.co.il					
Drone Guard	ESM, radar	EO/IR	*	*	RF jamming; GNSS jamming
Hensoldt Holding Germany GmbH; Taufkirchen, Germany; +49.89.51518-0; www.hensoldt.net					
XPELLER	Radar; EO/IR; RF, including radar classifier	Radar; EO/IR; RF	Sector, LOB or Positon	Yes	RF/GNSS jamming, Hunter drone

COUNTERMEASURES RANGE	JAMMING FREQ./ BANDS	PLATFORM	SIZE (in./cm)	WEIGHT (lb/kg)	FEATURES
Up to 2 mi	*	Grd-fix, grd-mob	SDR Sensor: 17 x 17 x 5 in. / 44 x 43 x 12 cm; antenna radome: height: 9 in. / 23 cm; Ø: 18 in. / 46 cm	104 lb / 47.2 kg	Passive detection, IFF, non-jamming, non-kinetik, full take-over and safe landing.
*	GPS, GLONASS, Galileo, WLAN 2.4, and from 5-6 GHz	Grd-mob	*	*	
*	Wi-Fi	Grd-mob	19-in. 6 RU	*	
*	*	Grd-fix	*	*	Partnership between ESG (TARANIS C2 system), Rohde and Schwarz (ARDRONIS ESM and jamming and WiFi Disconnect) and Diehl (HPEMcounterUAS); radar and EO sensors optional.
2 km	433 MHz 915 MHz 2.4 GHz ISM 5.8 GHz ISM GNSS L2 and L1	Grd-fix, grd-mob	4.36m3 shipping size	516 kg shipping weight	Flexible deployment platform or fixed-site solution. Integrated sensor detection and RF counter-measures.
1-2 km	433 MHz 915 MHz 2.4 GHz ISM 5.8 GHz ISM GNSS L2 and L1	Man-portable	56 x 17 x 8 in.	7.3 kg	Rifle-style portable counter-measures.
1 km	2.4 GHz ISM 5.8 GHz ISM GNSS L2 and L1	Man-portable	23 x 20 x 12 in.	15.7 kg	Covert (Pelican Case) portable counter-measures.
3000 m (min)	Frequency bands: 400/900 MHz, 2.4 GHz, 5.8 GHz, GPS & GLONASS L1	Grd-fix, grd-mob, man-portable	*	37 kg	Acoustic sensors for perimeter sensing and alert; drone and operator handling; swarm handling.
*	*	Grd-fix, grd-mob	Config dep.	Config dep.	Detect, track and characterize multiple drones from different directions; automatic or manual operation; open and scalable configuration; algorithms for target characterization.
300 m - 2.5 km	400 MHz, 900 MHz, 2.4 GHz, 5.8 GHz, GFSK/OFDM/FH/ DSSS	Grd-fix, grd-mob, shp	Config dep.	Config dep.	Detect, track and defeat multiple drones from different directions; take control of most commercial drones; automatic or manual operation; minimize interference to wireless connection operative in the area; algorithms for target classification and identification.
*	*	Grd-fix	*	*	Can be configured with the company's ELM-2026D, ELM-2026B and ELM-2026BF for short (10km), medium (15km) and long (20 km) ranges; EO sensors can provide visual identification.
Up to 9 km	500 MHz up to 6 GHz + GNSS	Manpack (Gear); grd-mob (Rapid); grd-fix (Guard);	Config dep.	Manpack starting from 22 kg; grd-mob & grd-fix starting from 60 kg	Modular counter-UAV solution to address individual user groups (civil and military) requirements in regards to mobility, range and countermeasures; radar classifier (Doppler analysis); ITAR free.

COUNTER-UAS SYSTEMS

MODEL	DETECTION SENSORS	TARGET TRACKING SENSORS	DF SYSTEM	C2 SYSTEM	COUNTERMEASURES
H.P. Marketing & Consulting Wuest GmbH; Reinfeld, Germany;+49 4533 7011-0; www.hp-jammer.de					
HP 47	*	*	*	*	Jammer Dronegun
HP 3055T	*	*	*	*	Modular Rack Jammer
HP 3962 H	*	*	*	*	Trolley Case Jammer
Jordan Electronic Logistics Support Co.; Amman, Jordan; +962796679716; www.jels-tech.com					
Sky Sweeper	ESM	electronic scanning	electronic scanning	Yes	Smart jamming
Kirintec Ltd; Ross-on-Wye, Herefordshire, UK; +44 (0) 1989 568350; www.kirintec.com					
Sky Net Longbow	Sensor agnostic	Sensor agnostic	Sensor agnostic	K- Net Mesh Network	RF jamming of control, video and GPS links
Sky Net Recurve Max	Sensor agnostic	Sensor agnostic	Sensor agnostic	K- Net Mesh Network	RF jamming of control, video and GPS links
Sky Net Recurve	Sensor agnostic	Sensor agnostic	Sensor agnostic	K- Net Mesh Network	RF jamming of control, video and GPS links
L-3 Communications ASA Ltd; Fleet, Hampshire, UK; +44 (0) 1252 775750; www.l-3asa.com / www.l3-droneguardian.com					
L3 Drone Guardian™	Sensor agnostic to suit protected area, including: Radars, EO/IR, Acoustic, ESM (RF TDOA), and DF	Sensor agnostic to suit protected area, including: Radars, EO/IR, Acoustic, ESM (RF TDOA), and DF	Yes	L3 Drone Guardian C2 system operates in automatic autonomous mode and manual mode with browser-based GUI for workstation or mobile devices	RF barrage jamming of drone contol links, GPS and GLONASS targeted RF jamming
Leonardo Airborne and Space Systems; Luton, Bedfordshire, UK; +44-0-1582 886478; www.leonardocompany.com					
Falcon Shield	Radar, ESM	ESM, NERIO EO, thermal and laser rangefinder sensors	*	Vantage C2 and Situational Awareness System	RF jamming of command link
Lockheed Martin: Bethesda, MD, USA; +1 607-751-3199; www.lockheedmartin.com					
ICARUS	ESM	EO, acoustic	*	*	RF barrage jamming; control link manipulation
METIS Aerospace Ltd; Lincoln, Lincolnshir, UK; +44 (0) 1522 963125; www.metisaerospace.com					
SKYPERION	ESM	ESM	Yes	Yes	*
Netline Communications Technologies; Tel Aviv, Israel; +972-3-6068100; www.netlinetech.com					
C-Guard DroneNet	ESM	ESM	*	*	RF jamming
Rafael Advanced Defense Systems Ltd.; Haifa, Israel; +972-4-8795143; www.rafael.co.il					
Drone Dome	ESM, radar	EO/IR	*	Yes	RF jammer; high-energy laser
Rohde & Schwarz; Munich, Germany; +49 89 4129-0; www.rohde-schwarz.com					
R&S®ARDRONIS - P	RF Receiver - reliable signal classification (20 MHz - 6 GHz); W-LAN receiver	Geolocation of drone uplink and downlink signals	R&S DDF 550	R&S®ARDRONIS Control Center, Protobuf open interface	RF smart follower/sweep jammer - selective disruption; W-LAN link - selective disruption
R&S®ARDRONIS - D	RF Receiver - reliable signal classification (20 MHz - 6 GHz); W-LAN receiver	Geolocation of drone uplink and downlink signals	R&S DDF 550	R&S®ARDRONIS Control Center, Protobuf open interface	W-LAN link - selective disruption
R&S®ARDRONIS - R	RF Receiver - reliable signal classification (20 MHz - 6 GHz); W-LAN receiver	*	*	R&S®ARDRONIS Control Center, Protobuf open interface	RF smart follower/sweep jammer - selective disruption; W-LAN link - selective disruption

COUNTERMEASURES RANGE	JAMMING FREQ./ BANDS	PLATFORM	SIZE (in./cm)	WEIGHT (lb/kg)	FEATURES
*	Customizable	Man portable	*	7.5 kg	All in one piece, no backpack needed.
*	Customizable	Grd-fix, grd-mob	19-in. rack	*	Open interface; directional and omnidirectional jamming possible.
*	Customizable	Man portable (Trolley)	Customized	*	Mobile version.
No less than 3 km	2.4 GHz & 5.8 GHz	Grd-fix, grd-mob	1200 x 700,850 mm	70 kg	Nework centric, platform identification, multi-jamming cell.
9 to 1 ratio	Fully programmable between 20 MHz - 6GHz	Grd-fix, grd-mob	10 (H) x 20 (W) x 17 (D) in.	41 kg	Fully and rapidly programmable system covering all known and likely future threats. Completely sensor agnostic.
6 to 1 ratio	Fully programmable between 20 MHz - 6GHz	Grd-fix, grd-mob	18 (H) x 12 (W) x 11 (D) in.	20 kg	Fully and rapidly programmable system covering all known and likely future threats. Completely sensor agnostic.
4 to 1 ratio	Fully programmable between 400 MHz - 6GHz	Man-portable	18 (H) x 12 (W) x 5 (D) in.	10 kg	Fully and rapidly programmable system covering all known and likely future threats. Completely sensor agnostic.
Antenna power options to suit protected area and anticipated pilot locations	Targeted jamming from 20 MHz - 6 GHz	Grd-fix, grd-mob	Config dep.	Config dep.	Multiple sensor types resulting in a high probability of detection, accurate tracking and false alarm filtering; L3 simplified C2 GUI and alerting system with integration to PSIM and jammers.
*	*	Grd-fix, grd-mob, man-portable	*	*	Option for advanced electronic attack capability to deny, disrupt or take control of UAV command and data links.
*	*	Grd-fix, grd-mob	*	*	*
*	30 MHz - 18 GHz	Grd-fix, grd-mob, air; shp	Manpack or 40 x 40 x 15 cm to 80 x 80 x 45 cm	12 kg	Scalable meshed network ESM capability. 30MHz to 18GHz, standard format for C-UAS 400MHz to 6GHz. TRL9 Optional EA Jamming capability.
*	20 MHz - 6 GHz	Grd-fix	*	*	*
*	*	Grd-fix; man-portable	*	grd-fix, portable	*
Smart Jammer: max 2/3 of detection range; W-LAN: up to 500 m	20 MHz - 6 GHz; W-LAN (2.4 GHz and 5.8 GHz) disruption	Grd-fix, grd-mob	Devices: integrated box with 2 x 19 in., 6 HU; DF antenna: 0.34 x 0.42 m; jamming antenna: 0.21 x 0.28 m; W-LAN antenna: 0.72 x 0.075m	80 kg	Detection of multiple drones and RCs, device classification, direction finding of drones and RCs, localization (based on multiple DFs) of drones and RCs, W-LAN drone detection and link disruption, intuitive GUI, automatic warning, white listing, automatic remote notification, smart jamming of single drone, jamming of multiple drones, video stream visualization.
W-LAN: up to 500 m	W-LAN (2.4GHz and 5.8 GHz) disruption	Grd-fix, grd-mob	Devices: integrated box with 1 x 19 in. 6 HU; DF antenna: 0.34 × 0.42 m; W-LAN antenna: 0.72 x 0.075 m	40 kg	Detection of multiple drones and RCs, device classification, direction finding of drones and RCs, localization (based on multiple DFs) of drones and RCs, W-LAN drone detection and link disruption, intuitive GUI, automatic warning, white listing, automatic remote notification, video stream visualization.
Smart Jammer: max. 2/3 of detection range; W-LAN: up to 500 m	20MHz - 6 GHz; W-LAN (2.4GHz and 5.8 GHz) disruption	Grd-fix, grd-mob	Devices: integrated box with 1 x 19 in., 6 HU; jamming antenna: 0.21 × 0.28 m; W-LAN antenna: 0.72 x 0.075 m	40 kg	Detection of multiple drones and RCs, device classification, W-LAN drone detection and link disruption, intuitive GUI, automatic warning, white listing, automatic remote notification, video stream visualization.

COUNTER-UAS SYSTEMS

MODEL	DETECTION SENSORS	TARGET TRACKING SENSORS	DF SYSTEM	C2 SYSTEM	COUNTERMEASURES
SESP; Paris, France; +33 (1) 73 04 91 17; www.sesp.com					
Drone Defeater	*	*	*	*	RF control link jamming; GNSS jamming
Systems & Processes Engineering Corporation; Austin, TX, USA; +1 512-479-7732; www.spec.com					
ADEP Blade	Radar	Radar	*	Yes	RF barrage jamming, control link manipulation, GPS/GNSS jamming, DRFM based anti-radar/anti signal techniques
SRC, Inc.; North Syracuse, NY, USA; +1 315-452-8000; www.srcinc.com					
Silent Archer® Counter-UAS Technology	Any one or combination: AN/TPQ-50 with LSTAR® air surveillance software; SkyChaser® on-the-move radar; Gryphon R1410 multi-mission radar SRC EW systems for RF detection	Any one or combination: AN/TPQ-50 with LSTAR® air surveillance software; SkyChaser® on-the-move radar; Gryphon R1410 multi-mission radar	WhisperHunter spectrum sensor, Gryphon S1200 spectrum sensor	Yes	SRC EW systems for full spectrum electromagnetic engagement
TCI International; Fremont, CA, USA; +1 510-687-6100; www.tcibr.com					
TCI Drone Detection Systems	Yes	RF receiver	Yes, DF on drone, DF on drone controller	Yes	*
Thales Air Systems; Paris, France; +33 (0) 1 79 61 40 00; www.thalesgroup.com					
Counter UAS	Squire radar, Black Finder DF	Margot 8000 EO system	Yes	Yes	RF jamming
WhiteFox Defense Technologies, Inc.; San Luis Obispo, CA, USA; +1 805-240-9690; www.whitefoxdefense.com					
DroneFox	Passive (non-detectable) RF	Passive RF & proprietary algorithm.	Yes	Yes	Drone control protocol via safe & selective algorithm.
Scorpion	Passive (non-detectable) RF	*	No	No	Control break via safe & selective algorithm.

SURVEY KEY – COUNTER-UAS SYSTEMS

MODEL
Product name or model number.

DETECTION SENSORS
Indicates sensors types and models used to detect and acquire the target UAS.
- ESM = electronic support measures

TARGET TRACKING SENSORS
Indicates sensor types and models used to track the target UAS.

DF SYSTEM
Indicates if a direction finding (DF) system is used to determine the direction of the drone and/or the drone operator.

C2 SYSTEM
Indicates if the system provides a command and control system to manage tracking sensors and countermeasures.

COUNTERMEASURES
Indicates the type of countermeasures and/or the countermeasures techniques the system employs to defeat the target drone.

COUNTERMEASURES RANGE
Indicates the typical effective range of the Counter UAS system's countermeasures.

JAMMING FREQUENCIES
Indicates the system's jamming frequencies in MHz or GHz.

COUNTERMEASURES RANGE	JAMMING FREQ./ BANDS	PLATFORM	SIZE (in./cm)	WEIGHT (lb/kg)	FEATURES
*	*	Grd-mob	*	*	*
*	20 MHz to 2.5 GHz, opt. to 3.6 GHz	Grd-fix, grd-mob, man-portable	5 x 7.9 x .89 in.	<2 lb	Full remote control and very low power requirements; backpackable comms jammer and low frequency radar DRFM; can also be used on any test range to provide either distributed ES/EA and can be synchronized over wireless Ethernet control.
*	*	Grd-fix, grd-mob, air	Config dep.	Config dep.	Detects, tracks, identifies and defeats single drones and swarms; uses a system of systems approach and can be integrated with other sensors and defeat technologies.
*	*	Grd-fix, grd-mob	Grd-fix: 126 x 95 x 23 in.; grd-fix: 47 x 26 x 30 in.; grd-portable: 14 x 18 x 14 in.	Grd-fix: 210 lb; grd-portable: 46 lb; antenna: 29 lb	Fully integrated system with antennas, receivers and operator terminals; 20MHz to 8GHz coverage; automatically detects drones and their radio controllers; geolocates and tracks the drone and/or controller.
*	*	Grd-fix; man-portable	*	*	*
1 km	*	Grd-mob	30.63 x 23.06 x 27 in.	181.95 lb / 82.5 kg	Drone threat detection, identification and mitigation device; passively analyzes radio frequencies (RF) being transmitted by drones, and through a series of safe a selective proprietary algorithms enables the user to lock out the original pilot and return the drone to its operator. Whitelist capable.
500 m	*	Man-portable	2 x 3 x 1.25 in.	3.5 oz / 100 g	RF-signal denial device that autonomously detects and defeats targeted wireless devices without barrage jamming. Whitelist capable.

PLATFORM

air = airborne
grd-fix = fixed ground installation
grd-mob = ground mobile vehicle
shp = ship based

SIZE

H x W x L/D in inches, millimeters or centimeters

WEIGHT

Indicates system weight in pounds (lb) or kilograms (kg)

FEATURES

Additional features

** Indicates answer is classified, not releasable or no answer was given.*

JUNE 2019 PRODUCT SURVEY: AIRBORNE EW SELF-PROTECTION SUITES

This survey will cover integrated EW self-protection suites for aircraft. Please e-mail JEDEditor@naylor.com to request a survey.


ApisSys
Direct sampling up to X-Band
AV Series
APISSYS
OpenVPX
“The Partner for Your Solution”
Visit us at
EW Europe 2019
Stand B13
The Leading Provider of High Speed Data
Conversion and Signal Processing Solutions
ApisSys
www.apissys.com

New EA Techniques Part 4

4 Jamming Track-via-Missile Threats (First Half)

By Dave Adamy

Editor's Note: Due to an editorial error, last month's EW 101 article within the "New EA Techniques" series was misnumbered. Last month's article should have been named as "Part 3" (not as "Part 2") in this series. We apologize for the error.

Many of the new generation missile systems use a complex type of guidance to enhance their performance; this is known as "track-via-missile" (TVM**).** Since we are dealing with multiple signal paths and cooperative jamming of each, this subject will require two columns.

TRACK-VIA-MISSILE GUIDANCE

As a missile moves toward its target, it travels farther from its guidance radar. The skin return signal arriving at the radar's receiver is reduced as a function of the *4th power* of the radar-to-target range. Missiles using TVM guidance have another receiver in the missile to receive the skin return signal, as shown in **Figure 1**. Late in the missile's flight, the missile is close to the target, so the skin return is stronger than the signal received from the distant radar. The new-generation missiles have significantly longer guidance range than legacy missiles. This is partially enabled by the down-range location of the missile's receiver.

The information about the target aircraft's skin return, including the direction of arrival, is transmitted from the missile to the guidance radar over a data link. This allows the radar to generate missile steering commands based on information from both the tracking radar and the missile's receiver. The skin return signal is reduced as the *square* of the distance from the target to the missile and the *square* of the distance from the radar to the target. This reduction in range allows the threat to receive a higher quality signal during the terminal portion of the engagement (see **Figure 2**). The link from the missile to the tracking radar can be optimized for the engagement, and it is also reduced only by the square of the radar-to-missile range. It is important to consider that the radar cross section (RCS) applicable to the skin return to the missile's receiver is bistatic in that the radar signal is received by the target from one direction, and the target reflects this signal in a different direction. Depending on the nature of the target and the location of the missile, the bistatic RCS can be either greater or less than the retro-direction RCS.

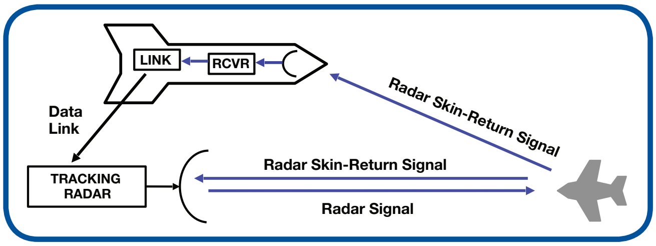


Figure 1: A threat that employs track-via-missile guidance has a receiver in the missile that receives skin return signals and passes information to the tracking radar guidance processing to enhance range and accuracy.

JAMMING TVM THREATS

The geometry of the self-protection jamming problem against a TVM threat is shown in **Figure 3.** If a jammer jams the tracking radar, the system can continue to guide the missile to the target using the information collected by the missile's receiver and forwarded by the data link. On the other hand, if the missile receiver or the data link is jammed, the radar can continue to track the target using the information from the main tracking radar. If the jammer is applying deceptive jamming, the ability of the radar to see the target from two directions (radar vs. missile) means the effectiveness of the

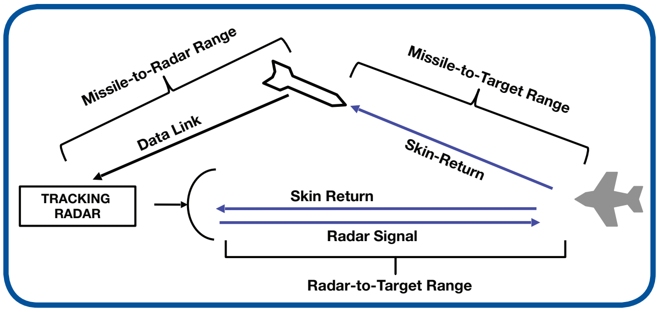


Figure 2: As the missile approaches a target, the radar signal reflected to the missile is stronger than the signal reflected to the receiver on the tracking radar, and it has a different angular geometry. This allows more time for an engagement range and enhances the radar's electronic protection performance.

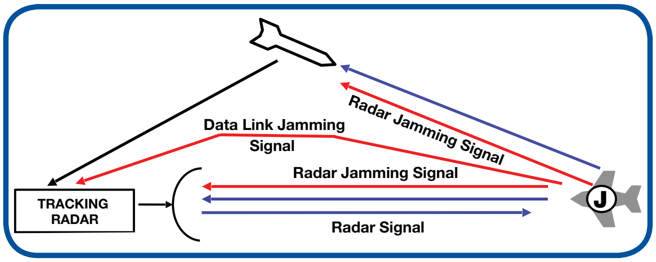


Figure 3: For self-protection jamming against a threat with a track-via-missile feature, the jammer must jam the tracking radar and also jam the missile receiver and/or the link from the missile to the radar.

deception may be reduced. There are three signals to consider in the jamming task: those received by the radar receiver, the missile's receiver and the data link receiver.

A legacy jammer typically uses an antenna with broad spatial coverage, so the same jamming signal would be transmitted toward both the radar and the missile receiver. Since next-generation jammers are expected to use directional (multiple beam phased array) transmitting antennas, there will need to be separate beams to jam the missile receiver and the radar receiver.

The data link between the tracking radar and the missile will be at a different frequency from the radar signal, so the jammer must produce both signals. Also, these two jamming signals must have different modulations; the radar jamming signal will have the optimum cover or deceptive jamming waveform, and the data link jamming signal will be optimum for jamming a digital data link.

JAMMING TO SIGNAL RATIOS FOR SELF-PROTECTION JAMMING OF A TVM THREAT

There are three jamming functions, so there are three different J/S formulas for: the main radar, the missile receiver and the data link. These three functions can be evaluated throughout the engagement to determine the effective jamming protection.

In *jamming the direct radar signal*, the jamming-to-signal-ratio formula is the same as that shown in the February 2019 column:

$$\mathbf{J/S = ERP_J - ERP_S + 71 + 20 \log R - 10 \log RCS}$$

Where: *J/S* is the jamming-to-signal ratio in dB,
ERP_J is the effective radiated power of the jammer (the dB sum of the jammer transmitter power and the gain of the jamming antenna in the direction of the radar) in dBm,
ERP_S is the effective radiated power of the jammed radar in dBm,
R is the range from the radar to the target (and jammer) in km, and
RCS is the radar cross section of the target in m^2.

The jamming to signal ratio for the *jamming signal used against the missile receiver* is:

$$\mathbf{J/S = 71 + ERP_J - ERP_S + 20 \log (R_{MT}) - 10 \log RCS_B}$$

Where: *J/S* is the jamming-to-signal ratio in dB,
ERP_J is the effective radiated power of the jammer in dBm,
ERP_S is the effective radiated power of the RADAR in dBm,
RMT is the range from the missile to the target in km, and
RCSB is the bi-static radar cross section of the target in m^2.

For the *jamming signal used against the data link,* the J/S ratio is:

$$\mathbf{J/S = ERP_{JL} - ERPL - 20 \log(R) + 20 \log (R_{MR})}$$

Where: *J/S* is the jamming-to-signal ratio in dB,
ERP_{JL} is the effective radiated power of the jammer against the data link in dBm,
ERP_L is the effective radiated power of the data link transmitter in dBm,
R is the range from the radar to the jammer (which is on the target), and
R_{MR} is the range from the missile to the radar in km.

AN ENGAGEMENT EXAMPLE

Figure 4 shows the positions of the radar, the target and the missile for this engagement.

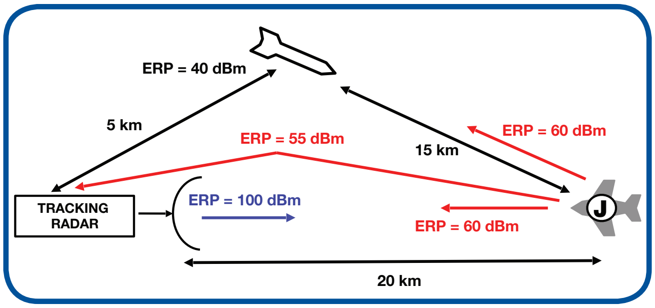


Figure 4: This is the geometry for the J/S calculation example. The target is 20 km from the radar and 15 km from the missile. The missile is 5 km from the radar. The ERP of the radar is 100 dBm, the data link ERP is 40 dBm, the jammer ERP is 60 dBm on the radar frequency and 55 dBm on the data link frequency.

The ERP of the radar is 100 dBm,
the ERP(s) of the jammer are:
toward the data link receiver: 55 dBm, and
toward the main tracking radar and the missile receiver: 60 dB.
The radar cross section of the target is:
toward the tracking radar: 10 m^2, and
toward the missile receiver (i.e., the bistatic RCS) – 8 m^2.
The range from the
jammer (on the target) to the radar is 20 km,
target to the missile is 15 km, and
missile to the radar is 5 km.
The J/S against the tracking radar is:

$$\mathbf{J/S = ERP_J - ERP_S + 71 + 20 \log R - 10 \log RCS = 60 - 100 + 71 + 26 - 10 = 47\ dB}$$

The J/S against the missile receiver is:

$$\mathbf{J/S = 71 + ERP_J - ERP_S + 20 \log(R_{MT}) - 10 \log RCS_B = 60 -100 +23.5 -8 = 46.5\ dB}$$

The J/S against the data link is

$$\mathbf{J/S = ERP_{JL} - ERP_L - 20 \log(R) + 20 \log (R_{MR}) = 55 - 40 - 26 + 14 = 3\ dB}$$

Remember that all of these three values will change as the relative locations of the target and missile change over the course of the engagement.

WHAT'S NEXT

Next month, we will continue this discussion of jamming a TVM threat with calculations of the burn-through ranges, stand-off jamming and the effectiveness of multiple jammer strategies. For your comments and suggestions, Dave Adamy can be reached at dave@lynxpub.com.

FEATURED LIVE WEB COURSES:

EDUCATIONAL COURSES

DRFM Technology and Design for Electromagnetic Maneuver Warfare

MONDAYS & WEDNESDAYS
13:00 – 16:00 EDT (17:00 – 20:00 UTC)
June 3rd – 26th
This course examines both the design of the DRFM as well as the technologies and strategies used to create superior false target decoys.

Introduction to Radar Systems

MONDAYS, WEDNESDAYS, & FRIDAYS
13:00 – 16:00 EDT (17:00 – 20:00 UTC)
July 29th – August 9th
This course introduces the audience to radar systems in a military context, with a focus on search and tracking radars associated with modern day threats.

Airborne Expendables/UAS Capabilities and Potential

MONDAYS & WEDNESDAYS
13:00 – 16:00 EDT (17:00 – 20:00 UTC)
August 19th – 28th
This course provides attendees with a strong foundation in expendables/sUAS, from basic airframe classes and capabilities, to EW potential, to the current FAA airframe and pilot certification/flight approval process.

SPACE EW

MONDAYS, WEDNESDAYS, & FRIDAYS
13:00 – 16:00 EDT (17:00 – 20:00 UTC)
September 4th – 20th
In the eight sessions of this course, we will cover the nature of EW in space and go on to work practical EW problems appropriate to the space environment.

21st Century Electronic Warfare, Systems, Technology, and Techniques

MONDAYS, WEDNESDAYS AND FRIDAYS
13:00 – 17:00 EST (18:00 – 22:00 UTC) | **February 3rd – February 21st 2020**
This course offers a comprehensive overview of modern electronic (EW) warfare systems, technology, and techniques.

Fundamental Principles of Electronic Warfare

SATURDAY & SUNDAY
08:00 – 17:00 EDT (12:00 - 22:00 UTC)
October 26th – 27th
This is a two day overview of Electronic Warfare (EW) with little math above Algebra. It assumes no prior knowledge of the field, but will allow you to understand the underlying principles of EW and make some important performance calculations.

56 AOC INTERNATIONAL SYMPOSIUM & CONVENTION WASHINGTON D.C.

Advanced Principles of Electronic Warfare

THURSDAY & FRIDAY
08:00 – 17:00 EDT (12:00 - 22:00 UTC)
October 31st – November 1st
This is a follow-on overview course to the EW Fundamentals course presented at the beginning of the AOC convention. It builds on the earlier discussion, extending coverage to new generation radar and communication threats and countermeasures against them.

FOR COURSE LISTINGS AND MORE VISIT **CROWS.ORG**

What Does the EM Domain Look Like?

Last month, we discussed some general ideas about warfighting domains and their attributes. This month, we will look at the structure of a warfighting domain and, more specifically, the structure of the Electromagnetic (EM) Domain.

STRUCTURE OF A WARFIGHTING DOMAIN

One trait that all warfighting domains share is that each one (Air, Land, Sea, Space, Cyberspace and the EM Domain) is part of a larger Global Commons. The idea behind recognizing these Global Commons is that every nation can access them in some way and use them. For example, Australia, acting as a sovereign nation, can access the air, land, sea, space, cyberspace and electromagnetic environments in, above, below and around it. Its citizens can fly in Australian air space, fish in its territorial waters, mine its minerals (on land and at sea), etc. Within its air, land and sea borders, the Australian government manages the way these commons are accessed and used. This model is fine for a single nation. The idea of a Global Commons, however, recognizes that these continuous physical spaces don't pay attention to national borders. For example, when an Australian airline wants to fly through Indonesian air space to reach its destination in Kuala Lumpur, it must first have the permission of the Indonesian Government. Thus, sovereign nations collectively manage the use of these Global Commons through international treaties, conventions and laws. The same is true of the three other Global Commons that are more difficult to define with political borders – Space, Cyberspace and the Electromagnetic Environment. So, there are two key traits that characterize a Global Commons: the idea that we *use* these Global Commons and the idea that we *manage* the use of these Global Commons.

When we talk about these Global Commons in relation to national security, we usually define them as warfighting domains – that is, unique physical maneuver spaces that are strategically important to military operations. Military forces seek to *use* or access each of these warfighting domains, and they seek to *manage* the use of these domains. But there is an additional dimension, too, because military forces seek to exert *control* over each of these domains.

Let's take the Air Domain as an example. A military force will seek access to and use of the air environment in the battlespace in order to fly supplies from one location to another, conduct bomber strike missions or launch a missile at a target. When the number of users in the air space grows, the military force must actively manage those users by establishing flight rules that every user must follow, and it may also manage these users through an air operations center. This deconfliction is particularly important around a friendly air base or over a target. Finally, this military force must deny the use of the air environment in the battlespace to the enemy by exerting military *control* over the air space via its own fighter aircraft and ground-based air defense systems. Regardless of the technologies being used, this same set of functions – use, manage and control – apply to the Naval Domain, the Ground Domain, the Space Domain, the Cyberspace Domain and the Electromagnetic Domain.

Another important concept is that these three functions are interrelated. Going back to the Air Domain example, every Air Domain user (manned or unmanned) is responsible for following rules and procedures that help with management and deconfliction of the air environment. Within the air management function, an air operations center can assist with the control function by directing where the fighter aircraft should fly to intercept an adversary or by helping to coordinate the ground-based air defenses. And the fighter aircraft and air defense assets that perform the control function by shooting down adversary aircraft, for example, help to ensure that the users can retain access to the air environment. These are basic examples, and the interrelationships are far more complex. The important point, however, is that these three domain functions are mutually dependent and must be integrated with one another.

Going back, for a moment, to last month's discussion, it is worth noting that we use technology to achieve each of these domain functions. In the air domain, transports, bombers and surface-to-surface missiles must be able to access and use the air environment in order to fulfill their purpose. A Combined Air Operations Center (CAOC) is used to manage and deconflict all of the air users in a given battlespace. And F-22s and Patriot air defense systems are needed to exercise control over the air environment in the battlespace. However, none of these technologies defines the Air Domain; nor do they define the specific functions they perform. They are simply tools.

STRUCTURE OF THE EM DOMAIN

So, what does the EM Domain look like in this "use, manage and control" domain model? You will often hear the EM environment described as "congested and contested," and this is not an exaggeration. The military EM users constitute the thousands and sometimes millions of military EM-dependent systems in a battlespace. This includes all the radios, radars, GNSS receivers, EO/IR sensors, combat ID systems, etc., that need free access to the EM Environment. It's also worth remembering that an EM-dependent system does not need to be complex. It can be something as seemingly simple as an altimeter on an aircraft. Because many EM-dependent systems are highly automated, most weapons system operators don't even realize how many ways their weapons systems need access to the EM Environment in order to perform well. What helps to ensure that these spectrum-dependent systems retain access to the EM Environment are Electronic Protect (EP) technologies, techniques and procedures. This is traditionally known as electronic counter-countermeasures (ECCM), and it is also part of Electronic Defence in NATO doctrine.

In many EM Operating Environments, this "user group" of military EM-dependent systems is competing for EM access alongside an equal or larger number of civilian and government EM-dependent systems, such as air traffic control radars, telecommunications systems, all the way down to RF networked security systems in homes and businesses, remote car starters, etc. This makes for a very complex EM environment, which requires military users to depend on military electromagnetic spectrum management strategies and schemes, such as EM frequency maneuver and fixed EM frequency allocation for specific types of EM-dependent systems, to deconflict all of these EM users. This EM congestion is not evenly spread through the battlespace. The EM environment on a street in Baghdad, for example, can be much more congested and complex than say, the EM environment 40,000 feet above Baghdad.

The control function in the EM Domain is familiar to most of us in the form of Electronic Warfare Support (ES) and Electronic Attack (EA). In its simplest form, we use receivers to sense the EM environment for signals of interest, and then we use transmitters in our attempts to jam those frequencies when we want to deny to our adversary the ability to use them.

It is important to point out that EM control is a fairly humble concept. We are not describing the ability to "control" the entire EM Environment any more than the control function in the Air Domain seeks to deny anything and everything from accessing the Air Environment (an impossible task!). Instead, EM control simply seeks to deny an adversary's ability to use the EM Environment at specific frequencies in certain specific locations for limited periods of time. Even an EW system as sophisticated and powerful as an EA-18G Growler or an EC-130H Compass Call is not capable of doing more than this.

NEXT TIME

We are beginning to draw an outline around what the EM Domain looks like and what functions take place in the EM Environment. In the next column, we will look at these EM Domain functional elements – use, management and control – from an integrated perspective. This is important, especially when a warfighting domain functions at the speed of light.

INPUT-PROTECTED, LOW-NOISE AMPLIFIERS

Pasternack (Infinite Electronics), has introduced a new line of input-protected, low-noise amplifiers (LNAs) intended for radar systems, EW applications, communications and test instrumentation. There are 12 models included in this line of amplifiers, including models PE15A63000 to PA15E63011, each offering no damage up to +30 dBm CW input power. These amplifiers cover frequency bands between 10 MHz and 3.5 GHz and feature low noise levels from 0.8 to 1.6 dB and high-small signal gain from 25 to 40 dB. *Pasternack; Irvine, CA, USA; +1 (949) 261-1920; www.pasternack.com.*

GALLIUM NITRIDE AMPLIFIER

Empower RF Systems, Inc. has released model 1219, a solid state gallium nitride (GaN) amplifier that operates between 0.6 and 6 GHz. This module delivers a minimum of 30W (40W typical) and uses 50V GaN on SiC transistors for lower leakage levers, higher thermal conductivity and SWaP optimization. The 1219 is intended for defense applications, including jamming and product testing. *Empower RF Systems, Inc.; Inglewood, CA, USA; +1 (310) 412-8100; www.empowerrf.com.*

6U OPENVPX BLADE SERVER

Mercury Systems, Inc. has expanded its line of EnsembleSeries blade servers to include the HDS6605, a 6U OpenVPX server built to support artificial intelligence (AI) applications. The server uses a Second Generation Intel Xeon Scalable processor, which delivers 2.6 TFLOPS of processing power. The server is built with up to 100 Gbps in-chassis switch fabrics and offers optional modified-off-the-shelf (MOTS+) as well as BuiltSECURE™ technology for improved durability and security. Built for size, weight and power (SWaP) optimization, high processing performance and resilience, the HDS6605 has a readiness level of nine (TRL-9) and is intended for defense applications in rugged environments, including C4I, sensor fusion and deep learning. *Mercury Systems, Inc.; Andover, MA, USA; +1 (978) 967-1366; www.mrcy.com.*

4-WAY POWER DIVIDER

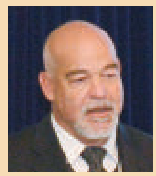
Planar Monolithics Industries, Inc. has released a new 4-way power divider model, the ADP-4-500M18G-SFF-30W. This power divider operates between 0.5 and 18 GHz, with a minimum isolation of 12 dB from 0.5 to 0.6 GHz, and 14dB from 0.6 to 18 GHz. This model features a low insertion loss at a maximum 5.5 dB, an amplitude balance of ±0.6 dB max, and a phase balance of ±6 degrees max. *Planar Monolithics Industries, Inc.; Frederick, MD, USA; +1 (301) 662-5019; www.pmi-rf.com.*

DIA AND AOC HOST 2019 MODERN THREATS: SURFACE-TO-AIR MISSILE (SAM) SYSTEMS CONFERENCE

The Defense Intelligence Agency's Missile and Space Intelligence Center (DIA/MSIC), in conjunction with the Association of Old Crows (AOC), hosted the 2019 Modern Threats: Surface-to-Air Missile (SAM) Systems Conference in Huntsville, Alabama, from February 4-6. The event was held in the MSIC auditorium, Redstone Arsenal, Alabama, with more than 325 attendees from all segments of the US DOD electronic warfare community, including acquisition program representatives, industry developers and the intelligence community.

The conference provided an opportunity to highlight DIA/MSIC's all-source scientific and technical intelligence analyses and assessments that support warfighters, acquisition programs and decision makers. During the event, MSIC analysts shared their latest assessments of foreign SAM systems, both in development and operationally deployed, with special emphasis on Russian, Chinese and Iranian origin.

Conference attendees had the opportunity to learn the latest findings from ongoing, all-source analysis of high-interest threat air defense systems, to include threat system capabilities and vulnerabilities, status of new development programs, and current and projected proliferation.


AOC President "Muddy" Watters

AOC President "Muddy" Watters kicked off the conference, and MSIC Senior Intelligence Officer and conference chair Scott Bigelow introduced keynote speaker Dr. William Conley, Director, Electronic Warfare, OUSD for Acquisition & Sustainment, who presented a briefing titled "Modern Threats and the Department's Response."

Subsequent conference activities included presentations by OUSD, MSIC analysts and other members from the IC, as well as displays and demonstrations. Each of the first two afternoons featured 10 hands-on displays and demonstrations of threat system hardware and software, which were well received by the attendees.

On the first evening of the conference, attendees were invited to a Beer & Badge, sponsored by AOC, at the Rocket City Tavern, located right outside of the base gate. It was an excellent opportunity for participants to pre-register and network. The following night, a social was hosted by title sponsor Dynetics at Straight to Ale, a local venue. Participants enjoyed a special axe throwing event. On the final day after conference events, attendees spent an evening at Yellowhammer Brewing, sponsored by Torch Technologies. All three socials provided excellent opportunities for networking, and feedback from the conference and post-survey has been extremely positive.


Keynote Speaker Dr. William Conley

The AOC extends a special thank you to the conference sponsors: Title Sponsor Dynetics, Platinum Sponsor Torch Technologies, and Gold Sponsors BAE and SRC.

Save the Date: Our next Modern Threats: SAM Systems Conference will be held from September 15-17, 2020.

DIXIE CROW CHAPTER PROVIDES EMS TRAINING

The Dixie Crow Chapter, with the support of the Georgia Tech Research Institute (GTRI) facilitators, hosted their annual Introduction to EW and C2ISR training courses at the Robins AFB. The sessions took place in the Base Theatre from February 25–26 and were geared toward new engineers, logistics management personnel and refreshers for those working in ISR or EW. Thank you to Lee Evans, GTRI and Rodney Brooks, the event organizer.

Introduction to C2ISR (ISR101)

The ISR101 training was a half-day short course with more than 60 attendees. The training covered ISR doctrine and definitions, collection platforms and processing, exploitation and dissemination of ISR data.

Introduction to EW (EW101)

The EW101 training was a full-day short course with more than 100 attendees. Course topics included: radar basics, radar warning receivers, radar jammers, electro-optics and infrared, and system Integration.

THE PASSING OF A CROW

We are saddened by the passing of the AOC Cabrillo Crows Chapter President Del Kintner, 82. Del, thank you for your service to the AOC and the Electromagnetic Warfare community. You will be missed.


5th Annual
Cyber Electromagnetic Activity (CEMA)
ASSOCIATION OF OLD CROWS
8-10 OCTOBER 2019
Aberdeen Proving Ground, MD
On the Road to Army of 2028 - Delivering Integrated EW, SIGINT and Cyber at the Tactical Echelon
CALL FOR PAPERS
Original papers are being solicited from the United States and Five Eyes Nations, Government, Academia, Industry, Operational Units, and Subject Matter Experts on how to fight and win decisively against any adversary in a joint, multi-domain, high-intensity conflict through employment of Cyber Electromagnetic Activity (CEMA) capabilities.
We will continue to expand the CEMA discussion from a doctrine, operational, technology and threat perspective, and how to integrate electronic warfare, cyber, signals intelligence, information operations and other forms of non-kinetic fires into operational formations. Conference presentations may be classified TS/SCI US Only or REL FVEY, or Secret Releasable FVEY.
Call for papers now open!
For more information, visit the conference website
www.crows.org/page/CEMA2019


3rd Electromagnetic Maneuver Warfare Systems Engineering and Acquisition Conference
ASSOCIATION OF OLD CROWS
SEPTEMBER 2019
Dahlgren, VA
SAVE THE DATE
Two-day classified event to provide a forum for EMW professionals from the military, Government, industry, and academic fields to discuss:
1. How our adversaries are challenging our dominance in the electromagnetic spectrum (EMS)
2. Current EMW capabilities being explored to ensure our dominance is maintained
3. Integration of capabilities into a warfare system
Call for papers now open!
COMING SOON Start preparing your abstracts for submission now!
For updates on and to view the submission guideline, please visit CROWS.ORG

AOC Industry and Institute/University Members

SUSTAINING
BAE Systems
Ball Aerospace & Technologies Group
Bharat Electronics LTD
The Boeing Company
CACI
Chemring Group Plc
Collins Aerospace
DRS Defense Solutions
Electronic Warfare Associates
General Atomics
General Dynamics
Harris Corp.
Huntington Ingalls Industries
Keysight Technologies
Leonardo MW Ltd.
Lockheed Martin Mission Systems and Training (MST)
Mercury Systems
Northrop Grumman Corporation
Raytheon Company
Rockwell Collins
Rohde & Schwarz USA
Saab

MILITARY UNITS
30 Cdo IX Gp RM
453 EW Squadron Research
51 Sqn, Royal Air Force
Air Command Denmark
French Air Force EW Unit
Helicopter Wing 53
Japan Air Self-Defense Force
New Zealand Defence Force
Osan AB 25 FS
Saudi Ministry of Defense
VMAQ-2
VMFAT-501
Zentrum Elektronischer Kampf Fliegende Waffensysteme

INSTITUTES/UNIVERSITIES
Electronic Warfare Studying Group, Korean Institute of Electromagnetic Engineering & Science
Georgia Tech Research Institute (GTRI)
Mercer Engineering Research Center
Riverside Research Institute
Research Association of Syracuse

GOVERNMENT GROUPS
Defence Science & Technology Agency (DSTA)
SAGE

GROUPS
3dB Labs Inc.
A.G. Franz, LLC
Advanced Test Equipment Rentals
Aeronix, Inc.
Aethercomm, Inc.
ALARIS Antennas
Allen-Vanguard
Amplus Corporation
Anaren Microwave, Inc.
Annapolis Micro Systems, Inc.
Anritsu Company
Antenna Research Associates, Inc.
ApisSys SAS
Arch Systems
Arctan, Inc.
Aselsan A.S.
Atkinson Aeronautics & Technology, Inc.
Atlanta Micro, Inc.
Azure Summit Technologies, Inc.
Base2 Engineering LLC
Battlespace Simulations, Inc.
Bird Technologies
Blue Ridge Envisioneering, Inc.
Booz Allen Hamilton, Inc.
Boyd Corporation
Broadern
Bryant Solutions, Inc.
CDM Electronics
CEA Technologies LLC
Centerline Technologies LLC
CISR Babcock International Group
Clearbox Systems
Cobham Advanced Electronic Solutions
Colorado Engineering Inc.
Communication Power Corporation
Communications & Power Industries LLC
COMSEC LLC
Comtech PST Corporation
CRFS Inc.
Cubic Global Defence
Darkblade Systems
Dayton-Granger, Inc.
dB Control
DCS Corp
Decodio AG
Defense Research Associates
DEFTEC Corporation
DEWC Pty Ltd
DHPC Technologies, Inc.
Digital Receiver Technology
DragoonITCN
D-TA Systems, Inc.
Dynetics, Inc.
Elettronica SpA
ELTA Systems Ltd.
Empower RF Systems
Epiq Design Solutions, Inc.
ERZIA Technologies S.L.
ESROE Limited
Esterline Defense Technologies
Evans Capacitor Company
EW Solutions
FEI-Elcom Tech, Inc.
Galleon Embedded Computing Norway
GFB GmbH
Gigatronics Incorporated
Hammer Defense Technologies LLC
Hanwha Systems
HASCALL-DENKE
Hensoldt Sensors GmbH
Hermetic Solutions
Herrick Technology Laboratories, Inc.
Independent Conultant, Jeffry Edgar
INDRA
Innovationszentrum Fur Telekommunikations -technik GmbH (IZT)
Intelligent RF Solutions
Interface Concept
ISPAS AS
IW Mircowave Products Division
IWTG Norfolk
JT4 LLC
Kerberos International, Inc.
Kihomac, Inc.
Kirintec
Kranze Technology Solutions, Inc. (KTS)
KRATOS GENERAL MICROWAVE CORPORATION
Kudelski Security, A Division of Nagravision S.A.
L3 Micreo
L3 Randtron Antenna Systems (L3 Randtron)
L3 TRL Technology
LCR Embedded Systems
Leonardo DRS
Liteye Systems, Inc.
LS Telcom AG
MacAulay-Brown
Mass Consultants Ltd
MBDA France
MC Countermeasures, Inc.
Meggitt Defense Systems
Metamagnetics
Micro Lambda Wireless
Microwave Products Group
Microwave Specialty Company
Military College of Telecommunication Engineering
Milso AB
MilSource
Mission Microwave Technologies
The MITRE Corporation
Modern Technology Solutions, Inc.
Motorola Solutions
MRC Gigacomp
MULTICONSULT SRL
My-konsult
MyDefence
MyDefence Systems Integration
N-Ask Incorporated
Narda Safety Test Solutions GmbH
National Technical Research Organization
Northeast Information Discovery, Inc.
Novator Solutions AB
Nuvotronics, Inc.
OCS America, Inc.
Overlook Systems Technologies, Inc.
Parry Labs
Parsons
Pentek
Peralex
Phase II Staffing and Contracting LLC
Phasor Innovation
Photonis Defense, Inc.
Physical Optics Corporation
Planar Monolithics Industries
Plath GmbH
Plexsa Manufacturing
Professional Development Tech Group Inc.
QinetiQ Target Systems
Qnion Co., Ltd.
QuantiTech
Quarterwave Corp.
RADA Technologies LLC
RADX Technologies, Inc.
Reliant Global Solution
RFHIC US CORPORATION
Rincon Research Corporation
Rohde & Schwarz GmbH & Co. KG
Rohde & Schwarz Norge AS
Roschi Rohde & Schwarz AG
Rotating Precision Mechanisms
S2 Corporation
SciEngines GmbH
Scientific Research Corp.
Selex Galileo, Inc. (a Leonardo-Finmeccanica company)
Sierra Nevada Corporation
Signal Hound
Silver Palm Technologies
SimVentions
SMAG Mobile Antenna Masts GmbH
Smiths Interconnect
Spectranetix, Inc.
Spherea GmbH
SR Technologies
SRC, Inc.
SRI International
Swedish Defence Materiel Administration T&E Directorate (FMV T&E)
SynQor
Syntonic Microwave
Systems & Processes Engineering Corp. (SPEC)
TCI International, Inc.
Tech Resources, Inc.
TEK Microsystems, Inc.
Tektronix, Inc.
Teledyne Technologies, Inc.
Teleplan Globe Defence
Tevet LLC
Textron Systems
Textron Systems Electronic Systems UK Ltd.
Third Wave Strategies LLC
Times Microwave Systems
TINEX AS
TMC Design
TMD Technologies Ltd.
Transformational Security LLC
TrustComm
TUALCOM, Inc.
Ultra Electronics - EWST
Ultra Electronics Avalon Systems
Ultra Electronics TCS, Inc.
US Technologies-Aldetec
Valkyrie Enterprises LLC
VEHERE INTERACTIVE PRIVATE LIMITED
ViaSat, Inc.
VIAVI Solutions
W.L. Gore & Associates, Inc. (Gore)
Warrior Support Solutions LLC
WGS Systems, Inc.
Wideband Systems, Inc.
Zodiac Data Systems

JED, The Journal of Electronic Defense (ISSN 0192-429X), is published monthly by Naylor, LLC, for the Association of Old Crows, 1555 King St., Suite 500, Alexandria, VA 22314.

Periodicals postage paid at Alexandria, VA, and additional mailing offices. Subscriptions: *JED, The Journal of Electronic Defense*, is sent to AOC members and subscribers only. Subscription rates for paid subscribers are $160 per year in the US, $240 per year elsewhere; single copies and back issues (if available) $12 each in the US; $25 elsewhere.

POSTMASTER:
Send address changes to
JED, The Journal of Electronic Defense,
c/o Association of Old Crows,
1555 King St., Suite 500
Alexandria, VA 22314-1652

Subscription Information:
Glorianne O'Neilin
(703) 549-1600
oneilin@crows.org

JED Sales Offices

NAYLOR
ASSOCIATION SOLUTIONS
5950 NW 1st Place
Gainesville, FL 32607
Toll Free (US): (800) 369-6220
Fax: +1 (352) 331-3525

Project Manager:
Tabitha Jenkins
Direct: +1 (352) 333-3468
tjenkins@naylor.com

Project Coordinator:
Amanda Glass
Direct: +1 (352) 333-3469
aglass@naylor.com

Advertising Sales Representatives:
Shaun Greyling
Direct: +1 (352) 333-3385
sgreylin@naylor.com

Erik Henson
Direct: +1 (352) 333-3443
ehenson@naylor.com

Chris Zabel
Direct: +1 (352) 333-3420
czabel@naylor.com

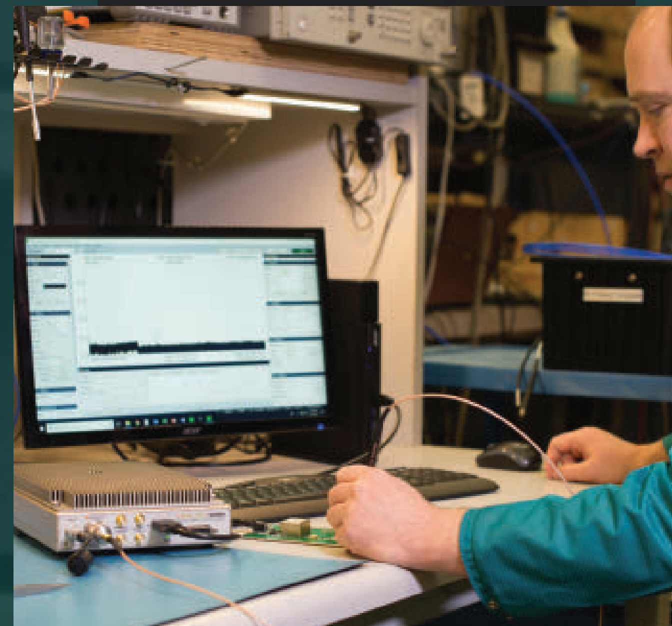
NAYLOR (Canada) Inc.
200 – 1200 Portage Ave.
Winnipeg, MB R3G 0T5 Canada
Toll Free (US): (800) 665-2456
Fax: +1 (204) 947-2047

Index of advertisers

Portable, small form-factor spectrum analyzers and signal generators

Ultra-fast sweep speeds and RF recording/playback functionality

Includes Spike™—our spectrum analysis and device control software—and a flexible, configurable API



radio operators
hardware devs
spectrum managers
field techs
engineers
Powerful, low-cost RF tools for **you**
soldiers
security pros
students
scientists
technicians

Signal Hound

SignalHound.com

Made in the USA

ASSOCIATION OF OLD CROWS 2019 AOC BOD Election Guide

Election runs June 1-30, 2019

Your participation is critical. Please exercise your right to vote for your AOC Board of Directors representatives.

You can familiarize yourself with the candidates with this election guide. This information describes the candidates' backgrounds, leadership styles and contributions to the AOC. The 2019 Nominating Committee carefully considered the impressive nominations it received before selecting this year's candidates. The slate of candidates was subsequently approved by the AOC Board of Directors. We are grateful to all of those who participated in this process and applaud those willing to submit their names for consideration.

Thank you for your continued support of AOC. Let your voice be heard by casting your vote for the new leaders of your association!

PRESIDENT

Glenn "Powder" Carlson

Glenn "Powder" Carlson retired from the USAF as a lieutenant colonel after more than 23 years of service and has over 33 years of EW experience, and he is a Life Member of the AOC. He received his Bachelors of Science in Electrical Engineering and was commissioned in the United States Air Force at Norwich University in 1984. He has also earned a Masters in Aeronautical Science from Embry Riddle Aeronautical University. He served as a B-52 Electronic Warfare Officer (EWO), Instructor, Evaluator, Flight Test, and numerous Wing and Staff positions at Loring, Castle, Offutt, Barksdale and Langley Air Force Bases. He earned Defense Acquisition University (DAU) Acquisition Professional Development Program (APDP) level 1 certification in Test & Evaluation, System Planning Research and Development Engineering, and Program Management while assigned to the 513th Engineering and Test Squadron as the B-52 EW Reprogramming chief. He deployed in support of Operations DESERT SHIELD, ENDURING FREEDOM, Pacific Deterrence during IRAQI FREEDOM and many International exercises around the globe. He also served as an instructor/research advisor and course director at Air Command and Staff College. His final assignment was to Headquarters Air Combat Command (ACC), Langley AFB, VA, as Chief, Airborne Electronic Attack (AEA), where he championed EW programs across Fighter and Bomber portfolio, Miniature Air Launched Decoy (MALD), MALD-J and Compass Call, before retiring in 2007. He then worked as a Senior Systems Analyst for MacAulay Brown at ACC, working numerous EW programs including Compass Call, MALD and F-15 EPAWSS. He is currently the Electronic Attack Capability Group Lead within Electronic Combat Solutions, at BAE Systems in Nashua, NH, overseeing a team of over 40 engineers supporting over two dozen programs.

Powder has been an active member of the AOC since he joined in 1986. He has been a member of a number of Chapters across the United States and has served in various positions to include; Vice President, Treasurer, Secretary, Awards and Membership on the local Board of Directors for the Strat Roost, Tidewater Chapter, and currently the Granite State Roost. He has served on the International Board since 2013 and has been the Secretary, on the EXCOM, Awards Chair, and has served on the Membership, Awards and Human Resources Committees. He currently serves as the Conference Chair and Northeast Region Director on the International Board.

Craig Harm

Craig has a deep and vested interest in advancing the future of EW through our Association, believing the EW community stands at the cusp of resurgence within the DOD and our partner nations. The AOC is in the position to take the lead in shaping this resurgent future of EW. Our foundation of members, chapters and events makes us uniquely qualified to be at the forefront of the advancement of EW. By expanding education programs, increasing membership, adding new chapters, hosting EW community conferences and events, as well as organizing government and industry advocacy efforts, we continue to broaden and bolster the world's understanding of EW and the imperative to get EW correct. We must capitalize on the hard work and successes of our past efforts and continue to advance them in serving our membership and our customers with the best EW professionals we are capable of growing.

The efforts to regrow EW experience levels within the DOD demands we continue to increase and inform our AOC membership to support and advocate for EW to prepare the next generation of EW leaders. Recent efforts to reinvigorate EW resourcing is bringing even more importance to our advocacy for a further understanding and application of EW. With counter-capabilities becoming available to a wide range of adversaries, the AOC will grow our relationship with the Intelligence Community to stay ahead of and influence future technology capabilities. With the world's most extensive network of EW professionals, our goal is to be where people and organizations turn to when they think EW.

Craig "Magnum" Harm is a retired US Air Force colonel with over 35 years in Intelligence, Operational Test and Evaluation, Planning, Information Warfare and Electronic Warfare. As a previous and current Director of the AOC's Board of Directors, Craig understands the activities, interests and business of the AOC and its community of chapters, across the globe. As Deputy Chief of Staff, and the IO/Cyber Policy Deputy Division Chief, he led USSTRATCOM's entrance into IO and EW. While Vice Commander of the National Air and Space Intelligence Center, Craig was responsible for a broad range of products and services related to EW, including threat and technology assessments, threat system modeling and EW data systems. His experience developing Air Force requirements for EW and IO capabilities, coupled with his years in Test and Evaluation give him a grasp and understanding for the needs of new systems and programs to effectively integrate into active operations. Craig served as an EC-130 Compass Call squadron commander and led his squadron in combat during Operation Iraqi Freedom. He has chaired multiple AOC conferences, presented at the AOC National Convention and worked numerous projects for various DOD organizations. He authored USSTRATCOM's Multi-Domain Engagement strategic concept for contested environments, directed cyberspace projects and led various EW modeling and simulation projects supporting Live Virtual Constructive environments.

An Operation IRAQI FREEDOM veteran, his flying experience includes combat, operational and flight test tours in the EF-111 and EC-130H Compass Call.

Rich Wittstruck

Dr. Rich Wittstruck has over 30 years of experience in national and international defense. He is responsible for executive leadership and oversight for design, development and demonstration of field experiments for C4ISR, integrated Cyber-Electromagnetic Activities, RSTA and Force Protection networked capabilities to enable the joint and coalition force to achieve full spectrum dominance. He served in the US Army's Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO IEW&S) culminating as the Deputy Program Executive Officer responsible for the executive management of a $17 billion program portfolio providing Army, joint and coalition forces with ISR, EW, Cyber and sensor systems. He is a senior advisor to NATO Headquarters in the fields of JISR, EW and C2 policy and trial. He is the NATO Chair Emeritus, Joint Capability Group for ISR, NATO Vice Chair Emeritus for All Source Intelligence Integration Sub-Group, and a former member of NATO's Joint ISR Project Group coordinating all Joint ISR efforts across the NATO alliance. He has also served in the Research and Development arena in both civil service and industry. Dr. Wittstruck holds a Doctorate Degree in Electrical & Computer Engineering from Rutgers University, a Master of Science Degree in Physics from the Polytechnic Institute of New York and a Bachelor of Science Degree in Physics from St. Johns University. Dr. Wittstruck has authored 19 journal articles, technical reports, conference proceedings and been awarded five US patents. He serves on the Editorial Advisory Board, The Journal of Electronic Defense, and is an At Large Director & Vice President of the global Association of Old Crows Board of Directors. He is a Senior Member of the Institute of Electrical and Electronic Engineers.

The AOC is a global community of trusted professionals committed to excellence, applying strategic, pioneering & resilient solutions to the world's toughest technological problems. Following this rich legacy, he believes he embodies these values and can serve the AOC as its president. His breadth and depth of international experience coupled with his technical and business acumen in AOC competencies makes him uniquely qualified to understand and discern the needs of our multi-faceted community shaping the administration and strategic navigation of the AOC. He envisions the future for the AOC to be bright and we must continue to integrate related communities of interest into our AOC. These communities include but are not limited to: artificial intelligence, big data analytics, converged SIGINT/EW/comms, and space. The AOC's strength is its members. He will continue to advocate for continuing education, professional development and certification for our members. Looking to the future, he is passionate on mentoring our young crows via a robust STEM curriculum. Our 2018 Symposium STEM exhibit educated over 1,000 participants, and he was proud to be one of its coordinators. We must strive to continue to offer a robust scholarship program. As the former AOC national scholarship director, he knows the difference a scholarship makes in a young professional's life. An investment in such young members is an investment in our future. Global government and industry affairs is another key area which the AOC must continue to cultivate. Policy is the primary retardant of technological advancement. The AOC must use its government and industry communities to shape, influence and educate our national leaderships to legislate effective policies and statutes that foster the advancement of our core competencies. He looks forward to serving you as your President.

AT LARGE

Nino Amoroso

In his over 30 years of involvement with the AOC, Nino Amoroso has been the chairperson of various activities and committees, including chairing symposia at the chapter, national, and international levels. Nino has over 42 years of both operational and procurement government and industry experience within the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), information operations and electronic warfare communities, where he has spearheaded new initiatives and directed the procurement of Air Force, Joint systems, special operations capabilities, counter-narcotics centers, coalition, command and control networks, aerial ground surveillance systems, and the rapid acquisition of critical technologies. He has had government and corporate responsibility for the planning, identification, and execution of programs within the C4ISR area, and he has held government leadership positions up to the System Program Office and Division level. Nino has also represented corporate organizations to senior government and industry across many focus areas, including the US Air Force, the US Intelligence Community, Battle Management, Aerial Ground Surveillance Systems, Battle Control Systems, International C4ISR programs, and Homeland Security (HLS). Nino holds a Bachelor of Arts degree from the Catholic University of America and a Master of Science degree from the University of Southern California. He is also a graduate of the Air War College, Federal Executive Institute, and programs within the Defense Intelligence College and Defense Acquisition University. In addition to military and civil service awards, he has also received two AOC awards, the Lifetime Achievement and Support the Intelligence Community awards, and other awards including the Hal Gershanoff Silver Medal for Electronic Warfare and Information Operations.

Brian Hinkley

CAPT Brian Hinkley, USN (Ret.) served almost 30 years in uniform in the EW, EMSO and CEMA communities as a Navy Electronic Counter Measures Officer (ECMO), having had the opportunity to support all Services with command of VAQ-135, the Fleet EW Center (FEWC) and JCCS-1 in Iraq. Additionally, he transitioned to a role specifically in EW as a Government contractor, contributing to service programs for the NSWC Crane, NSWC Dahlgren, Navy Marine Corps Spectrum Center, the FEWC and the Navy's Information Warfighting Development Center (NIWDC). Today he is excited to be in the middle of enhancing Fleet EW and IW readiness, actively participating with all Services, industry and academia advocating for strengthening current and future capability and capacity for maneuvering and winning inside the EMS battle space.

A member of the AOC since 1995, on the AOC International BOD since 2014, he has held leadership positions in AOC Ethics, Awards, Membership, STEM and Scholarship Committees. He continues to attend and speak at AOC conferences across the country and takes particular interest in talking to individual members to get insights and advocate for ways for AOC HQ to assist local Chapters.

Brian's platform for election is to continue to serve with passion and commitment for our AOC members and community, leveraging his AOC, Navy and Industry background, and to ensure all Services are equitably represented on the AOC BOD. Multi-Service leadership best represents our members, and is critical to successful advocacy in the Pentagon and on Capitol Hill.

Dr. Haruko Kawahigashi

Dr. Kawahigashi is a chief researcher of Information Technology R&D Center of Mitsubishi Electric Corporation. Haruko received her PhD in Electrical Engineering from the University of Tokyo. She joined Mitsubishi Electric Corporation after graduation, where she has been engaged in research and development of commercial carrier networks, defense networks, and EW. She has written over 100 conference papers and obtained 45 patents in Japan, the US and Europe.

Dr. Kawahigashi founded AOC Japan Chapter EW research group and has organized its annual conferences since 2012, cosponsored with IEICE (Institute of Electronics, Information and Communication Engineers) Japan. The annual conference has stimulated the AOC Japan Chapter and EW R&D community in Japan. She has participated in AOC annual symposium every year for the past eight years and has presented technical papers in majority of them.

Dr. Kawahigashi published Japanese versions of EW101, 102, 103 and 104 by Dave Adamy, co-translated with her ex-colleagues in Mitsubishi Electric. These are the first and the only EW technical book series in Japanese, and printed over 10,000 copies overall. They enlightened Japanese people on EW as a defense science.

She believes that the importance of Asia is increasing and that an additional board member from Asia helps collaboration of allied countries in and out of the district to make AOC truly international. She also believes that every member of AOC should find one's interest in AOC activity regardless of background (industry, academia, government), technical areas (EW, communication), life stage, gender, international areas. If elected, she will seek to represent diverse opinions.

LTC Gary M. Lyke

LTC Gary M. Lyke, USA, currently serves as the Operations Branch Chief at the Joint Electromagnetic Preparedness for Advanced Combat (JEPAC) at Nellis AFB, NV. Prior to his joint assignment, he served as the Military Deputy and Chief of Operations, TCM-EW, Cyber Center of Excellence; the Chief of Cyberspace Electromagnetic Activities for the US Army Pacific (USARPAC); and as the Division Electronic Warfare Officer for the 25th Infantry Division at Schofield Barracks and 1st Armored Division in Iraq.

He was commissioned as a Field Artillery officer in the United States Army upon graduation from the University of South Alabama in 1997. He holds a Master's Degree in Civil Engineering from the University of Missouri – Science and Technology.

Lieutenant Colonel Lyke became an AOC member shortly after joining the Electronic Warfare Community in 2009. Since joining, he has served as an appointed director on the board, assisted in establishing two chapters and a scholarship program, assisted in the coordination of the annual AOC STEM exhibit and participated in various AOC committees. As a former president of the Diamond Head Roost, he assisted in the development and sponsoring of four AOC PACOM conferences. Gary currently serves on the AOC Board of Governors

His goals as an At-Large Director include but are not limited to:

- Partner programs with industry and academic institutions,
- Outreach to middle and high schools to encourage STEM, and
- Support to partner associations such as AFCEA and TechNet

Lieutenant Colonel Lyke has been married to Nichole since 1997.

Darin Nielsen

Darin Nielsen received his commission through NROTC in June 1989 at the University of Utah. He received his Naval Flight Officer wings in July 1992. He completed Replacement Bombardier/Navigator training at VA-128 upon which he received orders to the Green Lizards of VA-95. He completed two cruises with CVW-11 aboard the *USS Abraham Lincoln*. Darin transitioned to the EA-6B and received orders to VX-9. As an Operational Test Director, he was the HARM Project Officer on the HARM Block IIIA/V and HARM Block VI programs. He also participated in operational testing to support the introduction of the UEU, Band 9/10 transmitter and Block 89A. As a Naval Reservist, he served as OIC of NR MOCC EPAC 0176, as an IO Planner with NR NIOC San Diego, and as a staff planner with NR CNFK HQ, before retiring in July 2009.

Since leaving active duty, Darin has worked in the Electronic Warfare Data Systems (EWDS) lab as a sensor engineer supporting reprogramming requirements for the ALQ-99 and ALQ-218. He was a principal designer of the ETIRMS NG, which eventually became the basis for the ETIRMS UPC. Later, he was the ICAP II Block III Assistant Block Lead and Software Project Manager for the OFP development at the EA-6B WSSA. From 2005 to 2013, he worked as part of the Jammer Technique Optimization (JATO) Fleet Liaison Team, supporting EA technique testing and development, and technical TTP documentation. He is currently the Pacific Region Director on the AOC Board of Directors, serving as Education and then Communications committee chair. He is currently the San Antonio Operations VP/Site Lead for Elbit Systems.

Kenneth "Kilo" Parks

Kenneth "Kilo" Parks has been actively engaged in the Electronic Warfare, EMS and Information Operations communities for over 33 years. He is a recognized leader both in and out of uniform.

With his EW/IO background, his previous and current work with Industry, and his previous work as a member of the AOC Board of Director and Treasurer, Ken is most qualified to serve the needs of the members of the AOC as an At-Large Director.

Ken has led three EW/IO military commands with increasing EW/IO/Cyber responsibilities. He has worked numerous EW/IO issues at the Operational, OPNAV, SYSCOM and TYCOM levels.

Ken has worked at various levels within local Roosts, from member to Chairman of committees to President of the Tidewater Chapter. His accomplishments included increasing membership in the Tidewater Chapter and re-engaging various EW/IO commands locally and on the national scene.

Ken's platform includes continued focus on the financial stability of the AOC, increase the AOC's ability to enhance membership status at the local level and continued expansion of the AOC worldwide. Additionally, he will work to broaden the membership base of EMS practitioners and specifically EW within the various services. Elevating the Association's status within the Department of Defense and Industry, he will strive to increase value to the membership. Recognition of those whose efforts deserve special attention will remain at his core. If elected, he will work to increase and broaden membership in the AOC, much like he has achieved at the local level and in other associations.

Greg Patschke

Col Greg "Patch" Patschke, USAF (Ret.), has 29 years in the Electronic Warfare field. He brings a unique perspective, having worked on EW efforts for each military Service while on active duty and in industry. During his 25 years in the Air Force as a career Electronic Warfare Officer (EWO), he contributed to EW in multiple capacities: EW operations as B-52 EWO; test and evaluation of Joint EW systems; Commander of the 36th Electronic Warfare Squadron; Combatant Command EW planner; USAF EW Requirements on the Air Staff; Director of USSTRATCOM's Joint Electromagnetic Preparedness for Advanced Combat (JEPAC); and lastly, a Brigade EWO for the US Army during Operation ENDURING FREEDOM.

After retirement, he was hired by Lockheed Martin to lead their spectrum protection and denial research area within their Advanced Technology Laboratories. Greg is currently a director at L3 Technologies working on SIGINT- and EW-related customer solutions. Over his career, he engaged EW experts within government, academia and industry to solve the tough EW issues. In 2015, Greg received the 2015 AOC Executive Manager of the Year Award. Over the last three years, Greg has been a member of the AOC Board of Directors; in 2017, he was elected as the AOC Treasurer and sits on the HQ Executive Committee. In this role, he ensured the AOC maintains sound fiscal responsibility in order to deliver quality products to our membership. During this time, Greg oversaw both the sale of the HQ Building and a period of impressive growth within the AOC.

Mike Ryan

Mike Ryan has been an Army EW professional for most of his 34-year civil service career. In the early and mid-90s, he worked special laser-based electro-optic countermeasure programs mounted on combat and tactical vehicles. Through the late 1990s and beyond, Mike held several leadership positions in HQs PEO Intelligence, Electronic Warfare & Sensors. Beginning in 2003, he had the privilege to serve as the first CREW Product Director in charge of fielding life-saving ECM jammers. From 2008 to 2017, as the senior civilian in PM EW & Cyber, Mike helped architect the reintroduction of much needed Cyber Electromagnetic Activity (CEMA) capabilities into Army formations for the first time since the Cold War ended. He understands the value of Electromagnetic Spectrum Operations and its game-changing effects. Today, he continues to work those challenges as an EW professional in the Defense industry.

Since becoming a card-carrying member of the AOC, Mike has tried to "give back." As the APG Susquehanna Chapter president, he stood up the CEMA conference, which is now going on its 5th year. Its attendance is only second to the AOC Convention. He also stood up his chapter's Young Ravens program to energize our young professionals. For the past several years, he has held positions on the AOC National BOD with increasing responsibilities, including Conference Committee Chair, Senior Advisory Board (Army rep) and currently as the EXCOM Director of Strategy.

If elected to the BOD, Mike's focus will be outreach to local chapters and give them a voice in shaping the future AOC strategy.

PACIFIC REGION

Vince Battaglia

Vince Battaglia is an aerospace technical and business leader with a 30-plus year proven record of military platform Survivability systems design, development and deployment.

As an AOC Chapter President and former BOD member, Vince is very aware of the contribution that the AOC makes to our chosen field and is committed to ensuring that the AOC and its members remain at the forefront of the ever-evolving Electromagnetic Spectrum Operational (EMSO) structure.

His professional accomplishments span from singular engineering design projects to providing overall hands-on leadership to the design and development of large integrated electromagnetic systems. Vince has demonstrated management skills for small, large, domestic and offshore efforts, providing state-of-the-art technologies for military, including space, air and sea platforms. His experiences include responsibility for building successful businesses, directing avionics design and development teams, as well as establishing operating strategies to restructure faltering organizations. He has proven corporate and program team leadership capabilities, including: growth strategies, financial, technical, people and risk management skills, as well as establishing required facilities and human resource teams. He currently provides technical and business management consulting services for defense- related organizations.

Vince's professional experience is rooted in a bachelor's degree in electrical engineering, a master's degree in applied physics and an executive MBA.

He is dedicated to assuring that related organizations are committed and prepared to work in an inclusive and mutually supportive way while building on lessons learned.

Rick Lu

Rick Lu respectfully submits his application to serve on the AOC Board with youthful exuberance and vigor...to bring in new fresh ideas and help the AOC grow in prestige, influence and membership. Originally a communications systems engineer, Mr. Lu started and ran his first Silicon Valley high tech startup at the age of 29, three years after graduating with two Masters Degrees from Stanford and getting steeped in entrepreneurship. For the last 20 years, he has successfully built some of the most innovative and fast-moving companies in the EW/SIGINT Industry, utilizing the Silicon Valley style of focusing on speed and technology innovation. He would like to bring those "startup" techniques to help the AOC have accelerated growth and get more new young members involved.

An active member of the AOC since 2001, Rick was the Co-Chairman of the AOC's 54th Annual International Symposium, a Session Chairman for a number of AOC conferences, and currently supports the AOC GIR Committee. For over 12 years, he has been actively briefing Congressional members on the EW Industry's concerns and issues. He can thus effectively represent the AOC's and Industry Partners' interests on Capital Hill for the future.

He would like to bring his new ideas, highspeed business skillsets and youthful energy to serve on the AOC Board to make us all more successful. His current work combines Army, Navy and Air Force EW programs. Thus, he can bring a fresh and balanced perspective to the Board that is truly Tri-Service.

INTERNATIONAL REGION

Sue Robertson

For Sue Robertson, it is a great honor to serve the AOC as the current International Region 1 Director. She has really enjoyed interacting with the chapters in the region, visiting most of them and taking part in their meetings and conferences. She is also a director of the UK AOC Chapter and enjoys her role as visits co-ordinator. She has chaired technical sessions at EW Europe conferences and has participated in conferences organized by AOC chapters all over the world.

Sue's technical experience includes all aspects of EW systems development. She is an expert on airborne surveillance systems, and she has developed trials programs and provided advice on system improvements for a variety of airborne platforms. She believes an understanding of the RF environment is essential to successful EW Operations; her work has included the analysis of complex data sets from airborne mission systems recorded during trials.

She has written hundreds of reports during her time as a Defence Advisor, and she has contributed evidence to UK Parliamentary Committees on EW. She recently completed a book on ESM analysis and has written articles for defense publications on topics such as AESA radar, electronic attack and maritime EW.

She has been fortunate to work in multi-national teams comprising both military and civilian participants at all levels of seniority. Sue believes that diversity in the AOC should be encouraged and, if re-elected, would continue to seek engagement with EW and Cyber professionals, young and old, male and female, from all parts of the globe.

2019 Online Voting Instructions

Beginning June 1, AOC members can visit the AOC homepage, www.crows.org, where they will see election information and a link to Elections On-Line, the independent vendor that will conduct the online election. You will receive an email with login instructions shortly before the elections start. The website will direct you to your ballot, where you can make your selections. Your AOC dues must be current as of May 20th in order to vote. As with past AOC elections, your ballot is secret.

Elections On-Line will hold all completed ballots, tabulate them and send the results to the AOC when the election is complete. Once you have cast your online vote, Elections On-Line will send you an email confirming that they have received your completed ballot.

Paper Ballots

For those AOC members who cannot vote online, the AOC has provided a paper ballot below. Members may cut out the paper ballot, mark it – including your member number (available on the front label of your *JED*) and your name and contact information – and mail it back to the AOC. Paper ballots must be postmarked after June 1, 2019, and before June 30, 2019, and be addressed to:

AOC
1555 King St 5th Floor
Alexandria, VA 22314

Campaign Rules

Campaigning or electioneering on behalf of any candidate for AOC International office, with or without their knowledge or consent, is prohibited.

2019 AOC Election Ballot

Ballots accepted June 1-30, 2019.

Name ....

AOC Member Number ....

Email address ....

PRESIDENT *(Vote for 1)*

- ☐ Glenn "Powder" Carlson
- ☐ Craig Harm
- ☐ Rich Wittstruck

PACIFIC REGION DIRECTOR *(Vote for 1)*

- ☐ Vince Battaglia
- ☐ Rick Lu

INTERNATIONAL REGION *(Vote for 1)*

- ☐ Sue Robertson

AT-LARGE DIRECTOR *(Vote for 2)*

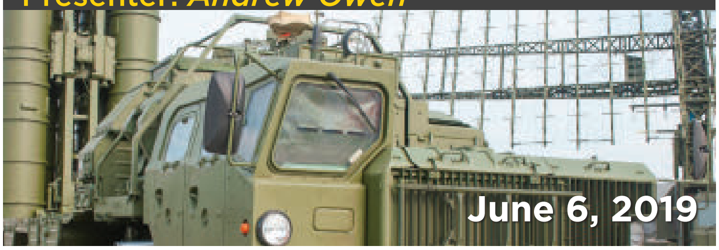
- ☐ Nino Amoroso
- ☐ Brian Hinkley
- ☐ Dr. Haruko Kawahigashi
- ☐ LTC Gary M. Lyke
- ☐ Darin Nielsen
- ☐ Kenneth "Kilo" Parks
- ☐ Greg Patschke
- ☐ Mike Ryan

2019 AOC Virtual Series

AOC VIRTUAL SERIES

AOC Virtual Series has been a tremendous asset providing the AOC's audience with learning, advocacy, and the exchange of information. Register today to hear from subject-matter experts on all things EW!

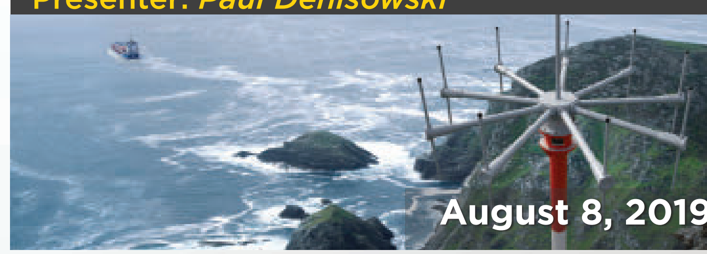
ELINT & RESM, Getting the Facts Straight
Presenter: *Andrew Owen*



Space EW 2.0
Presenter: *Dave Adamy*

Understanding Tracking Radars
Presenter: *Kyle Davidson*

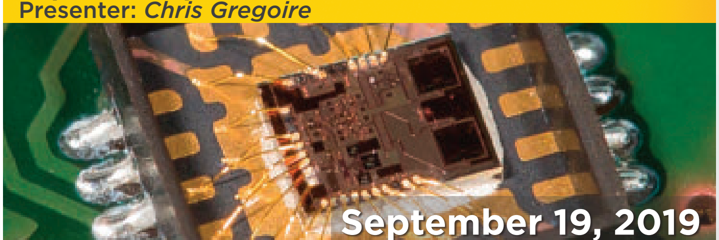
An Introduction to RDF Methodologies
Presenter: *Paul Denisowski*



Evolving to the Next Generation of Multifunctional EW - Part II
Presenter: *Matthew Orr*

Intro to Machine Learning for EW
Presenter: *Kyle Davidson*

Achieving SWAP-C Benefits in EW Systems using Positive Gain Slope MMIC Amplifiers
Presenter: *Chris Gregoire*



RAF 100 Group and its EW Legacy
Presenter: *Thomas Withington*

For more upcoming AOC Virtual Series Webinars, visit crows.org

ASSOCIATION OF OLD CROWS