ASSOCIATION OF OLD CROWS
Advancing Electromagnetic Warfare TOGETHER
crows.org

April 2022
Vol. 45, No.4

JED

Journal of Electromagnetic Dominance

NATO Rethinks Air Survivability

Also in this Issue:

- Training US Army AMSOs
- EW 101: Jamming 5G Signals
- Tribute to Lt Col (Ret.) Stephen "Muddy" Watters

Enhance platform survivability
with the RSS8000 from Ultra

Recreate realistic EW threat scenarios to prove the operational performance of your self-protection systems.

The Ultra RSS8000 replicates realistic, high-fidelity radar signals from EW threat systems to create a complete electronic warfare environment. The system replicates different receiver antenna modulations to accurately model the direction-finding system on the platform. The RSS8000 is tightly integrated with the actual aircraft avionics including the RWR, ELINT, and Emitter Location systems.

With the new RSS8000 automated test feature, EW specialists can greatly reduce the time to deploy accurate radar profiles to fielded systems.

For more information about Ultra Specialist RF solutions, visit **ultra.group/intelligence-communications.**

ULTRA

Ultra Intelligence & Communications

www.ultra.group

JED
Journal of Electromagnetic Dominance

CONTENTS

April 2022 • Volume 45, Issue 4

US AIR FORCE

COVER PHOTO COURTESY OF GERMAN AIR FORCE

SrA Aaron Wadyko, USAF, 755th Aircraft Maintenance Squadron Crew Chief, marshals an EC-130H Compass Call in from its final flight at Davis-Monthan Air Force Base, AZ, on February 28. The 55th Electronic Combat Group will replace all of its EC-130H aircraft with new EC-37B Compass Call aircraft. The EC-37B made its first flight in September 2021. US AIR FORCE PHOTO BY SRA ALEX MILLER

Departments

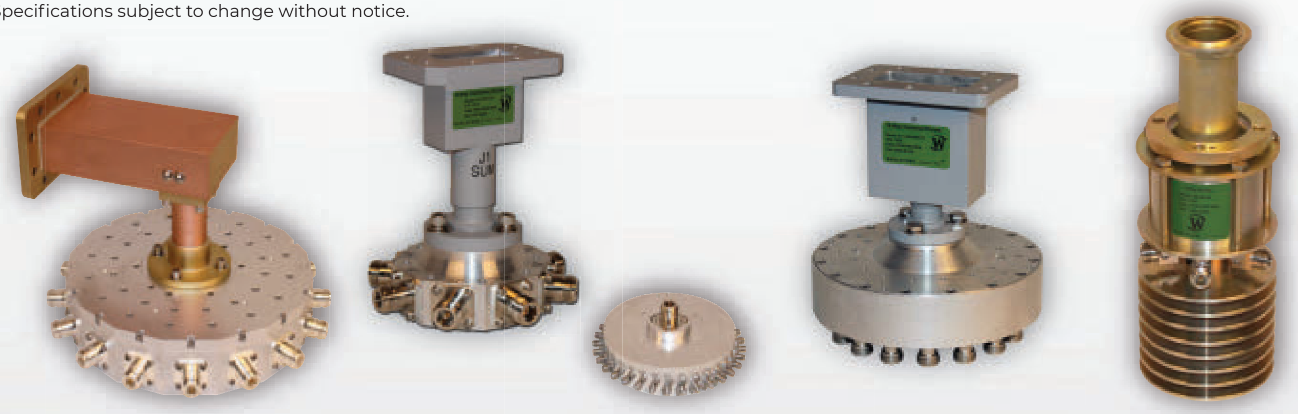
WERLATONE®

RADIAL COMBINERS

Multi-kW Power Levels ✦ **Low Loss Circuits** ✦ **Custom Designs Available**

Model	Type	Frequency (MHz)	Power (W CW)	Peak Power (W) 10% DC	Insertion Loss (dB)	VSWR	Connector Type
D9816	8-Way	330-530	10,000	50,000	0.25	1.30:1	3 1/8” EIA, N-Female
D8454	8-Way	370-450	10,000	50,000	0.25	1.30:1	3 1/8” EIA, N-Female
D5320	12-Way	470-860	500	5,000	0.30	1.30:1	All N-Female
D10119	4-Way	700-4200	2,000	15,000	0.30	1.35:1	13-30 DIN-Female, N-F
D10603	32-Way	900-925	50,000	150,000	0.15	1.25:1	WR975, 7/16-Female
D10795	32-Way	900-930	25,000	150,000	0.25	1.20:1	WR975, 4.3-10-F
D9710	8-Way	1000-2500	2,000	10,000	0.30	1.40:1	1 5/8” EIA, N-Female
D8182	5-Way	1175-1375	1,500	25,000	0.40	1.35:1	1 5/8” EIA, N-Female
D6857	32-Way	1200-1400	4,000	16,000	0.50	1.35:1	1 5/8” EIA, N-Female
D11896	4-Way	2000-2120	4,000	50,000	0.25	1.40:1	WR430, 7/16-Female
D11828	8-Way	2400-2500	3,000	25,000	0.20	1.25:1	WR340, 7/16-Female
D10851	8-Way	2400-2500	8,000	50,000	0.20	1.25:1	WR340, 7/16-Female
D11433	16-Way	2700-3500	2,000	20,000	0.30	1.35:1	WR284, N-Female
D11815	16-Way	2700-3500	6,000	40,000	0.30	1.35:1	WR284, N-Female
D12101	6-Way	2750-3750	2,000	20,000	0.35	1.40:1	WR284, N-Female
D9582	16-Way	3100-3500	2,000	16,000	0.25	1.50:1	WR284, N-Female
D12102	6-Way	5100-6000	850	4,500	0.35	1.35:1	WR159, N-Female
D12484	6-Way	8200-8600	600	700	0.35	1.25:1	WR112, SMA-Female
D12485	6-Way	9000-11,000	500	700	0.40	1.35:1	WR90, SMA-Female

Specifications subject to change without notice.



Werlatone, Inc. 17 Jon Barrett Road Patterson, NY 12563 845-278-2220 sales@werlatone.com www.werlatone.com

IS THE PEACE DIVIDEND (FINALLY) OVER?

As Russia's invasion of Ukraine drags on (as of mid-March), many European nations are taking a long and serious look at their respective security postures. Thirty years ago, the end of the Cold War caught NATO by surprise. As geopolitical analysts George Friedman described it, NATO and the Warsaw Pact were in a tug or war. When the Soviet Union collapsed, it let go of the rope, which threw NATO off balance, too. Most NATO members enjoyed "peace dividend" over the following decade and take advantage by trimming their defense budgets, shrinking defense forces and encouraging defense industry consolidation in several key sectors, including EW and SIGINT. During the post-9/11 conflicts in Afghanistan and Iraq, many European NATO countries increased their military spending, but only for those select units that were supporting expeditionary operations.

After Russia invaded Ukraine in 2014, however, most NATO members responded by increasing their defense expenditures as a percentage of GDP and grew their procurement spending as the alliance sought to rebuild its conventional deterrent. In 2014, only 7 of 29 NATO members spent more than 20% of their defense budgets on equipment (a NATO target). By 2021, that number had increased to 24 nations (and each of the remaining five were above 15%).

While governments can grow their defense budgets and buy new equipment within a few years, it can take more than a decade to build (or rebuild) an industrial technology base in specialized areas, such as EW and SIGINT. This type of technological and human capital investment is the real indicator that shows if European governments are truly making strategic pivots in response to Russia.

It's too early to say if European countries are going to grow their cadre of EW and SIGINT technology experts, but there are some positive signals (please forgive the pun). In Germany, for example, the new government has reversed a decision by the pervious Merkel-led government to buy US-made F/A-18E/F Super Hornets and EA-18G Growlers with Next-Gen Jammer pods. (See news story on page 14.) Germany has recently indicated that it will buy Typhoons – equipped with European EW suites and German-made jamming pods – to meet part of its requirement. This announcement was not a surprise, (the bigger surprise was Germany's earlier decision *not* to buy European fighters), but it does indicate how Germany is investing to maintain its domestic EW and SIGINT expertise.

In this month's *JED,* Richard Scott's cover story about NATO Air Survivability shows how the Alliance is rethinking its approach to self-protection EW and Airborne Electronic Attack. Ultimately, this will serve as a demand signal for European governments to develop the industrial base (including technology, operational and training expertise) they will need for these programs as they come on line. Let's hope that NATO members' response to the Russian threat runs deep and lasts long enough to influence its strategic investments.
– J. Knowles

JED
Journal of Electromagnetic Dominance

Journal of Electromagnetic Dominance is published for the AOC by
NAYLOR
ASSOCIATION SOLUTIONS
1430 Spring Hill Road, 6th Floor
McLean, VA 22102
Tel (800) 369-6220
www.naylor.com

COVER PHOTO COURTESY OF GERMAN AIR FORCE
PUBLISHED MARCH 2022/JED-M0422/9322

Three Ways

to Analyze RF Data from Signal Hound

1

SPIKE™

Spectrum analysis software, included with Signal Hound analyzers.

2

API

Your custom RF data, your way.

3

THIRD-PARTY SOFTWARE

Use a Signal Hound as a receiver for specialized software.

Signal Hound®

SignalHound.com/**Software-Options**

Made in the USA

SCAN HERE

Calendar *Conferences & Trade Shows*

APRIL

AAAA Mission Solutions Summit
April 3-5
Nashville, TN
www.quad-a.org

Navy League Sea-Air-Space
April 4-6
National Harbor, MD
www.seaairspace.org

37th Space Symposium
April 4-7
Colorado Springs, CO
www.spacesymposium.org

SPIE Defense + Commercial Sensing
April 5-7
Orlando, FL
www.spie.org

FIDAE 2022
April 5-10
Santiago, Chile
www.fidae.cl/en

Annual Directed Energy S&T Symposium
April 25-29
Mobile, AL
www.deps.org

MAY

Cyber Electrometric Activities (CEMA) 2022
May 3-5
Secret/US Only, TS/SCI
Aberdeen, MD www.crows.org

AOC Europe
May 10-12
Montpellier, France
www.aoceurope.org

Electronic Warfare Capability Gaps and Emerging Technologies
May 10-12
Crane, IN
www.crows.org

Special Operations Forces Industry Conference (SOFIC)
May 16-19
Tampa, FL
www.sofic.org

JUNE

Eurosatory
June 13-17
Paris, France
www.eurosatory.com

AOC Kittyhawk Week
June 14-16
Dayton, OH
https://kittyhawkaoc.org

Electronic Warfare Technical Conference
June 14-16
Shrivenham, Swindon, UK
www.cranfield.ac.uk

International Microwave Symposium
June 19-24
Denver, CO
https://ims-ieee.org

JULY

Farnborough International Air Show
July 18-22
Farnborough, Hampshire, UK
www.farnboroughairshow.com

AUGUST

TechNet Augusta
August 15-18
Augusta, GA
www.afcea.org

Defence & Security 2022
August 29 - September 1
Bangkok, Thailand
www.asiandefense.com

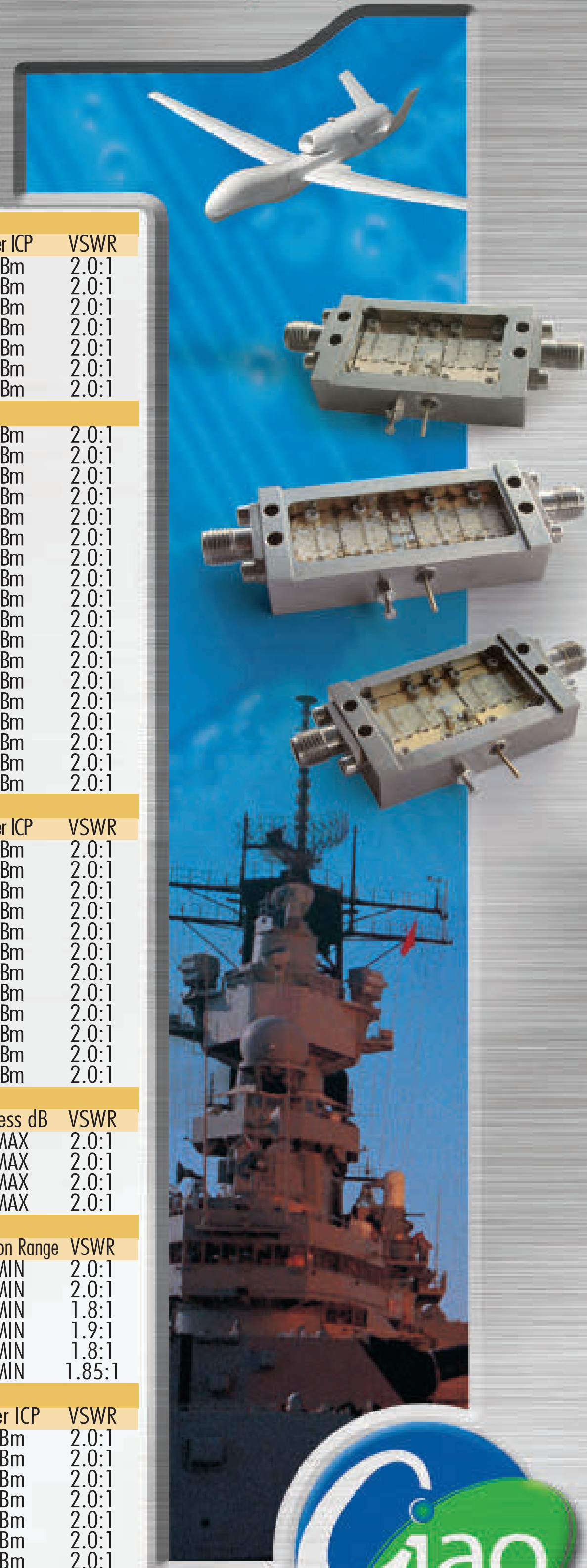
*AOC conferences are noted in **red**. For more info or to register, visit crows.org. Items in **blue** denote AOC Chapter events.*

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

Calendar *Courses & Seminars*

APRIL

AOC Live Virtual Professional Development Course: Tactical ISR Principles, Systems, and Techniques
April 4-27
8 Sessions, 3hrs. each
www.crows.org

AOC Virtual Series Webinar: EW and the Moscow Criteria
April 7
2-3 p.m. EST
www.crows.org

Basic RF Electromagnetic Warfare Concepts
April 12-14
Atlanta, GA
www.pe.gatech.edu

Infrared Countermeasures
April 12-15
Atlanta, GA
www.pe.gatech.edu

AOC Virtual Series Webinar: Space EW
April 21
2-3 p.m. EDT
www.crows.org

MAY

AOC Live Virtual Professional Development Course: EW Against a New Generation of Threats
May 2-25
8 Sessions, 3hrs. each
www.crows.org

AOC Virtual Series Webinar: Solutions for Quantum Computing and Communications
May 5
2-3 p.m. EST
www.crows.org

Electromagnetic Warfare Data Analysis
May 10-11
Atlanta, GA
www.pe.gatech.edu

Military Electronic Warfare
May 16-20
Shrivenham, Swindon, UK
www.cranfield.ac.uk

Modeling and Simulation of Phased Array Antennas
May 17-19
Online
www.pe.gatech.edu

Adaptive Arrays: Algorithms, Architectures and Applications
May 17-20
Atlanta, GA
www.pe.gatech.edu

JUNE

AOC Virtual Series Webinar: Development of Cognitive EW Datasets
June 16
2-3 p.m. EST
www.crows.org

Basic RF EW Concepts
June 28-30
Las Vegas, NV
www.pe.gatech.edu

Cyber Warfare/EW Convergence
June 28-30
Las Vegas, NV
www.pe.gatech.edu

AOC Virtual Series Webinar: Electromagnetic Battle Management
June 30
2-3 p.m. EST
www.crows.org

JULY

AOC Virtual Series Webinar: Low SWAP Multifunctional Electronic Warfare System Development
July 14
2-3 p.m. EST
www.crows.org

*AOC courses and webinars are noted in **red**. For more info or to register, visit crows.org.*

Cyber Electromagnetic Activity (CEMA) 2022

ASSOCIATION OF OLD CROWS

MAY 3-4 Belcamp, MD

The Invisible Battlefield: Deterrence During Competition, Dominance Throughout Conflict

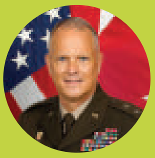
Join us for the CEMA 2022 Conference, where key Army leaders, decision makers, and industry partners will discuss how to achieve information dominance to seize and maintain the strategic initiative during any phase of conflict.

This conference will be Unclassified Distro A

Register now!
In-person spots are limited.

FEATURED SPEAKERS

MG Neil S. Hersey
Deputy Commanding General (Operations)
U.S. Army Cyber Command (ARCYBER)



MG Robert M. Collins
Program Executive Officer
U.S. Army Command, Control, Communications-Tactical

BG Jeth B. Rey
Director, Network Cross Functional Team

Mr. Joseph Welch, SES
Director, DEVCOM C5ISR Center

Mr. William B. Nelson, SES
Director, Assured Positioning, Navigation and Timing/Space Cross-Functional Team
U.S. Army Futures Command

Sponsorship opportunities available.
Contact Sean Fitzgerald, fitzgerald@crows.org, to learn more.

For more information, visit crows.org/CEMA2022

EVERYONE IS AN EMS OPERATOR

As this month's *JED* looks at NATO EMSO, and with the Russian invasion of Ukraine in late February, we are witnessing the how important the EMS is to military operations.

As Russian forces crossed the border into Ukraine, I was expecting to see an overwhelming Russian EMSO effort directed at Ukrainian forces. Surprisingly EMSO did not form a big part of the initial phase of Russia's invasion. While there definitely was military EMSO, and there were pictures and videos of aircraft dispensing expendables and destruction of Ukrainian IADS elements, I did not see or hear of a major EMSO campaign against Ukraine. What I did see was an effective information campaign, that seemed more *ad hoc* than fully planned.

When I began my term as AOC President, I discussed how EW and EMSO had larger pieces than just the military, and that commercial and civilian usage of the spectrum would continue to grow and interweave with military and government use. All EMSO tools and capabilities are key to any campaign, whether military or commercial, and must be considered and included in plans.

In Ukraine, we saw that individual communication tools (cellphones, computers, videos, pictures, texts, etc.) were essential for Ukrainians to send information out across the globe. Russian governments and military forces could not control Ukraine's entire network. Nor could Russia succeed in widely spreading it's message that Ukraine posed a threat to their sovereignty. Normal media outlets and social media enabled more information to flow across the EMS; and when Russia shut down the networks it controlled, it was a commercial network, Starlink, that enabled continued communication across Ukraine and the globe.

One challenge with the merging of all these networks and communication links across the EMS is determining what is fact and what is fiction, what is propaganda and what is real news. Another challenge is knowing how to separate military and commercial/civilian links at the appropriate times, when using the same frequencies in the spectrum, just like distinguishing a commercial shipping radar from a naval radar; knowing that in today's world, the commercial radar could feed information to the naval radar.

What used to be black and white in the EMS is now at best gray, and the "Kill Chain" is definitely a "Kill Web" as the EMS is truly an interwoven domain. It is highly complex and dynamic, and all who use it are in one form or another a spectrum operator. The EMS crosses international boundaries and cannot be controlled by one nation and is truly a domain that must be used effectively to operate and control the other domains.

Conferences: The AOC is hitting its stride in activities and is gearing up for in-person conferences (CEMA, Crane and AOC Europe in May) and we are moving on to normal times once again. My fellow Crows, stay safe out there, spread the news, welcome new Crows, mentor young Crows and look to help the AOC grow and improve. – *Glenn "Powder" Carlson*

EUROFIGHTER ECR IN LINE FOR LUWES ROLE

A major about-turn on the modernization of Germany's fast jet fleet means the Luftwaffe will now switch horses on its future airborne electronic attack (AEA) capability.

Under plans laid out by the Bundeswehr on March 14, the Lockheed Martin F-35A Lightning II has been selected to fulfil its Tornado replacement requirement. In addition, a new twin-seat Electronic Combat Role (ECR) variant of the Eurofighter will be developed to meet the Luftgestützte Wirkung im Elektromagnetischen Spektrum (luWES) AEA requirement for NATO.

The decision of the Social Democrat-led coalition government in favor of the F-35A and Eurofighter ECR overturns the policy of the previous Merkel administration, which had in April 2020 selected the Boeing F/A-18E/F Super Hornet as a partial Tornado replacement, and the Boeing EA-18G Growler to satisfy the luWES requirement. It is anticipated that the Luftwaffe will now buy up to 35 F-35As plus 15 Eurofighter ECRs.

The Eurofighter ECR concept has been developed by Airbus Defence and Space, in collaboration with Hensoldt, MBDA, Rolls-Royce, BDSV, MTU, BDLI and Aerotec, to confer the Eurofighter Typhoon with a capability for a full range of AEA missions: escort jamming (targeted at high and medium-frequency emitters); suppression of enemy air defenses/destruction of enemy air defenses (SEAD/DEAD); and delivery of stand-in jammers.

An artist's depiction of the Eurofighter ECR variant developed to meet the AEA requirement for the Luftwaffe and for NATO. Note the wing-tip receivers, anti-radiation missiles and Kalætron *support jamming pods.* EUROFIGHTER GMBH

Hensoldt is expected to take responsibility for the development of the podded escort jammer payloads equipping the Eurofighter ECR. Derived from the company's Kalætron product family, the multi-band pods feature DRFM-based architecture and GaN-based active electronically-scanned arrays.

Variants of MBDA's SPEAR family are also included as part of the Eurofighter ECR concept: the SPEAR 3 mini-cruise missile is seen as a kinetic effector for SEAD/DEAD, while SPEAR EW would serve as a stand-in jammer. – *R. Scott*

UK LAUNCHES BRIGHT CORVUS PROJECT

The UK Ministry of Defence (MoD) has launched a competitive effort, under its Defence and Security Accelerator (DASA), that seeks to identify and mature advanced distributed radio frequency (RF) technologies, techniques and effects.

Known as the Bright Corvus project, the research theme is intended to explore innovation applicable to the delivery of intelligence, surveillance and reconnaissance (ISR) and position, navigation and timing (PNT) in the future electromagnetic environment (EME). The primary focus of the competition is multifunction, distributed RF sensing (including radar and electronic surveillance in both the communications and radar bands) to support ISR and the targeting, delivery and post-action assessment of integrated RF effects.

The Bright Corvus project has an initial four-year timeframe (from mid-2021) with potential for follow-on work. According to DASA's synopsis, the initiative is intended to address the challenge of achieving pervasive, full spectrum, multi domain ISR. "In an increasingly congested and complex electromagnetic spectrum (EMS), it is essential to develop capabilities for situational awareness and affecting the adversary systems that are reliant on the EMS," it said. "As a result, a move away from large monolithic RF sensors, towards spatially distributed solutions that exploit autonomy and integrate with RF effectors will be part of delivering a step change in capabilities."

The DASA call is open to a broad range of platforms, ranging from dismountable or man-portable systems through to unmanned vehicles and elements that could be mounted on manned platforms. It is also designed to address various different scenarios and environments, such as dense urban environments with congested or disrupted EME, littoral coastal defenses, operations at significant range from a mission base, and operations in mountainous/valley areas.

Five specific "challenge" areas have been identified: distributed RF sensing (seeking innovations that detect, recognize and identify entities of interest, as well as locate and track them in complex physical and EM environments); integrated sensing and effects (advancing integration of sensing with RF effect delivery at range or within challenging environments); integrated sensing and effects enablers (including antenna/front-end technologies, power technologies and modular system approaches applicable to future systems); PNT as a Service (enabling distributed RF sensing and effector concepts through novel PNT technologies, fusion and dissemination techniques, and resilience to or detection of disruptors); and novel concepts and architectures for advanced RF sensing and effectors (developing secure, autonomous coordination of sensor/effector units across multiple platforms to maintain continuous sensing, tracking or effect delivery in a deployed scenario).

Up to £2.8 million is available, with DASA expecting to fund 15-20 proposals. While the competition is open to proposals from as low as fundamental technical principles and concepts (TRL 1 or TRL 2), it is envisaged that outputs should achieve between TRL 3 and TRL 6 at the end of the project. – *R. Scott*

NEW DECEPTION TECHNIQUES DEMONSTRATED IN BRITECLOUD DECOY

Leonardo and the UK Royal Air Force (RAF), working in cooperation with the Italian and Danish air forces, have proved the insertion of new software-based airborne radio frequency (RF) deception techniques into the BriteCloud active expendable countermeasure device. Trials undertaken at a UK range have demonstrated the ability of BriteCloud to stay ahead of new and evolving threats.

Developed by Leonardo's UK-based electronic warfare business, BriteCloud is a second-generation expendable digital radio frequency memory (DFRM) jammer designed to provide fast jet aircraft with effective "end game" protection against advanced RF-guided missile threats and/or tracking radars. After ejection, the BriteCloud decoy searches and locks onto the highest priority threat; the DRFM's coherent response prevents the threat from detecting the deception as the decoy separates, so generating large miss distances and breaking the target lock.

Two fast jet variants have been developed: BriteCloud 55 is a cylindrical expendable active decoy (EAD) store designed for compatibility with standard 55-mm chaff and flare dispensers; while the BriteCloud 218 EAD adopts a "square" form factor designed to be compatible with 2x1x8-inch countermeasure dispensers, such as the ALE-47.

Leonardo has now revealed details of trials conducted last year to demonstrate the ability of BriteCloud to embody new waveforms, and so increase the repertoire of techniques that can be employed against threat radars. The trials, undertaken in partnership with the RAF's Rapid Capabilities Office, the Air and Space Warfare Centre, and the Defence Science and Technology Laboratory (Dstl), saw an Italian Air Force Tornado strike aircraft release BriteCloud 55 EADs, while a Royal Danish Air Force F-16 fighter dispensed BriteCloud 218 rounds. "The new techniques proved highly effective at the trials range and the positive results will be presented to other NATO nations in an operators' forum," said Leonardo.

The new countermeasures techniques demonstrated were developed as part of ongoing work to "futureproof" BriteCloud against future RF threat developments. This activity reflects wider Dstl work towards a sovereign air platform protection enterprise aligned to UK and NATO Next Generation Air Survivability plans. – *R. Scott*

MILDS BLOCK 2 MISSILE WARNER FIT CONFIRMED FOR LUFTWAFFE HERCULES

Hensoldt (**Taufkirchen, Germany**) has revealed that it is supplying self-protection equipment for installation on new Lockheed Martin C-130J/KC-130J Hercules aircraft being delivered to the German air force (Luftwaffe).

AFRL SELECTS LEIDOS TO DEVELOP MJÖLNIR HPM PROTOTYPE

The Air Force Research Laboratory (AFRL) has contracted Leidos (Albuquerque, NM) to develop and build the new Mjölnir high-power microwave (HPM) weapon system prototype under a $26.9 million award.

Leveraging from AFRL's first-generation Tactical High-Power Operational Responder (THOR) HPM demonstrator, Mjölnir (the name recounts the hammer of the mythical Norse god Thor) is intended to demonstrate advances in HPM technology for the counter-unmanned aerial systems (C-UAS) mission. HPM weapons provide non-kinetic defeat of targets using bursts of high-power microwaves.

Leaders from the Army Rapid Capabilities and Critical Technologies Office (RCCTO) enter the portable control center of AFRL's THOR C-UAS demonstrator, Feb. 11, 2021 at Kirtland Air Force Base. The follow-on Mjölnir system will be developed by Leidos. AFRL

The THOR system was originally developed by BAE Systems in partnership with Leidos, Verus Research and AFRL. Designed to be able to disable the electronics in multiple unmanned aerial vehicles, so providing a capability against UAS swarm attacks, the system is housed in two standard 20-ft containers that can be deployed by air and assembled by a crew of just two.

According to the AFRL, Mjölnir prototype development will use the same basic technology to address the C-UAS threat, but will introduce advances in capability, reliability, and manufacturing readiness to enable future transition to a program of record. Delivery of the prototype Mjölnir weapon system is scheduled for 2023.

Leidos has long experience in supporting the AFRL Directed Energy Directorate, resident at Kirtland AFB, NM. The company led the design, development and testing of the HPM source for the THOR system, as well as providing support for source operation and maintenance. – *R. Scott*

Germany in 2018 ordered three C-130J-30 tactical transport aircraft and three KC-130J-30 aerial refuelling variants under a Foreign Military Sales (FMS) contract with the US Air Force. The aircraft, which will operate from Évreux-Fauville air force base in France as part of a bi-national Franco-German air transport squadron, have been procured to fill a tactical airlift gap left by the retirement of the C-160 Transall from Luftwaffe service at the end of 2021.

While the original FMS case included US-supplied AN/AAR-47 missile approach warner equipment, the German Bundeswehr in 2020 elected to equip all six aircraft with Hensoldt's latest-generation Missile Indication and Launch Detection System (MILDS) Block 2 ultra-violet (UV) missile warning system. As well as alerting aircrew to the launch/approach of IR-guided missiles, the MILDS Block 2 variant also enables hostile fire indication and in-sensor data recording.

Hensoldt is supplying MILDS Block 2 units to Danish company Terma, which is in turn managing the integration of the systems at Lockheed Martin through its US subsidiary Terma North America (Warner Robins, GA). Functional integration into the aircraft is managed through Terma's AN/ALQ-213A EW controller.

Each C-130J/KC-130J aircraft is receiving five UV sensor heads, with one further aircraft set (five UV sensors) being delivered for lab use. A total of 20 sensors had been delivered as of mid-March, according to Hensoldt; the remaining 15 are due for handover by January 2023.

The first C-130J-30 aircraft (55+01) made its maiden flight in November last year, and was delivered to Évreux-Fauville in February 2022. Other aspects of the platform self-protection fit for both C-130J and KC-130J variants also includes the BAE Systems ALR-56M radar warning receiver and the same company's AN/ALE-47 countermeasures dispenser system. – *R. Scott*

IN BRIEF

The Swiss Army has ordered Maske 76 smoke/obscurant cartridges from **Rheinmetall Protection Systems** (Bonn, Germany). The Maske 76 cartridges, which will replace older Maske C rounds, will be used to protect the Swiss Army's ground vehicles against EO/IR- and laser-guided threats and targeting sensors. Rheinmetall did not disclose the quantity of cartridges or the contract amount – only noting that it was in the "mid-two-digit million-Euro range." Initial deliveries are scheduled for November, with the final lot expected in August 2027. Rheinmetall's plant in Neuenburg am Rhein in Baden-Württemberg will manufacture the cartridges.

The Naval Air Warfare Center – Weapons Division (Point Mugu, CA) awarded a $376,444 contract to **Tevet LLC** (Greenville, TN) for a portable radio frequency (RF) recorder system for the Multi-Spectral Defensive Electronic Warfare Systems Support Activity (MDEWSSA) Integrated Product Team (IPT). The RF recorder system will be used in the Electronic Combat Simulation and Evaluation Laboratory (ECSEL) to record, analyze, playback, store, and output RF waveforms for jammer and threat simulators.

The **Air Force Research Lab's Directed Energy Directorate** (Kirtland AFB, NM) will hold a virtual industry day on April 14 to provide potential contracts with an overview of its Directed Energy Technology Experimentation Research (DETER) Advanced Research Announcement (ARA) plans for 2022 and beyond. The point of contact can be reached via e-mail at AFRL.DETER.ARA@us.af.mil.

Vectrus Mission Solutions Corp. (Colorado Spring, CO) has won a $3 million contract from the Office of Naval Research (Arlington, VA) to support the Navy's Spectrum Dependent System (SDS) Data Synthesis (SDSDS) effort. The objective of the SDSDS program is to develop concepts, algorithms and software prototypes to access, harness, utilize and synthesize data from combat systems and other SDS to demonstrate the usefulness and feasibility of accessing, sharing and mining this data to identify threats in the RF spectrum with the goal of improving ship survivability.

The US Air Force Life Cycle Management Center's Fighters and Advanced Aircraft Directorate (Wright-Patterson AFB, OH) exercised a contract option with **Northrop Grumman** to continue development of the F-16 Integrated Viper Electronic Warfare Suite (IVEWS). Specifically, the company received an Unpriced Change Order (UCO) in advance of a contract modification award expected later this year. According to an Air Force news article, "Over the next 18 months, Northrop Grumman will complete IVEWS – also referred to as AN/ALQ-257 – development and install the system on several F-16s for flight testing. Additional development, integration, hardware qualification testing, and Engineering and Manufacturing Development (EMD) asset procurement will support the IVEWS Developmental Test/Operational Test (DT/OT) and Operational Assessment (OA) in early 2023." It further stated, "IVEWS provides a next generation EW system that is internal to the F-16 and interoperable with the on-board APG-83 Active Electronically Scanned Array (AESA) radar. It is designed to Open Missions Systems requirements and provisioned for long-term growth capability to support future upgrades such as the Fiber Optic Tow Decoy, Adaptive/Cognitive Processing, and Open System Architecture compliance." IVEWS production is expected to begin in 2024.

The US Army's **Program Executive Office for Simulation, Training and Instrumentation (PEO STRI),** Project Manager Cyber, Test and Training (PM CT2), Threat Systems Management Office (TSMO) has issued a Sources Sought Notice to help identify potential suppliers that can provide BQM-167A, MQM-178A, or equivalent subscale aerial targets. The targets will be used to carry a variety of payloads, including DLQ-9 jammers, Luneberg Lens, TOW Target Launcher Assembly and Towed Targets (JCHAAT, POT-A-TOW, and TRX-4) – and possibly ALE-47 chaff/flare dispensers – to test and evaluate air defense weapons systems. The contracting point of contact is Rebecca Gonzalez, (407) 384-3968, rebeca.a.gonzalez.civ@mail.mil.

ASSOCIATION OF OLD CROWS

Apply for an AOC Scholarship

Advance your career and apply for scholarship programs developed to assist future crows in their career goals.

Current Programs

Undergraduate Scholarship for Sophomores and Juniors

AOC currently provides two scholarships to students currently in their sophomore or junior year of college. Each year one male and one female student studying in engineering or engineering technology and interested in working in the aerospace and defense industry is awarded a scholarship. A generous donation from Raytheon Intelligence & Space funds these scholarships. We are seeking other industry partners to participate as well to grow our program further.

Accepting Applications February 15 – April 1

Cyber Corps Warrant Officer Scholarship

AOC is exceptionally proud of The Cyber Corps Warrant Officer Scholarship established by the Laurie Buckhout Foundation in August 2020 under the Association of Old Crows Education Foundation incorporated and registered as a Non-Profit status under 501(c)(3) of the Internal Revenue Code. The Cyber Corps Warrant Officers Scholarship Foundation is a non-profit organization dedicated to providing support to U.S. Army Cyber Corps (i.e., 170A, 170B, and 170D) warrant officers by allowing them to apply for financial assistance in gaining various levels of formal higher education.

Accepting Applications April 1 – May 30

Find out more at **crows.org/scholarshipprogram**

Support AOC's Education Programs

Donate to these important programs developed to assist future crows in their career goals.

AOC distributes over $250,000 annually, through the AOC Educational Foundation (AEF) and affiliated chapters, for scholarships and grants to assist military enlisted personnel and U.S. undergraduate students in electrical engineering, physics, mathematics, and related disciplines. We welcome your contributions to these essential programs.

AOC FOUNDATION

Find out more at **crows.org/AEF**

Freedom of Action: NATO Rethinks Air Survivability for a New Threat Landscape

By Richard Scott

A decade ago, with NATO nations heavily committed to counter-insurgency operations in Afghanistan, the EO/IR-guided man-portable air defense system (MANPADS) threat was foremost in the mind of the air platform protection community. While operations over Libya during 2011 had reminded allied air arms that the RF threat had not disappeared, activity in the air survivability realm was overwhelmingly focused on defeating MANPADS that may have reached Taliban forces via Iran and Pakistan.

Fast forward to 2022, and the threat landscape has changed almost beyond recognition. Potential adversaries – with Russia and its acolytes writ large – have been investing in long-range, highly integrated, multi-layered integrated air defense systems (IADS) that draw Red "threat bubbles" well beyond home borders. These complex "systems of systems" present particular challenges with regard to their increasingly broad coverage of the electromagnetic spectrum – and the expansiveness of their surveillance volumes and engagements envelopes.

For example, radar systems operating in low bands outside of conventional radar frequencies have eroded many of the advantages hitherto enjoyed by low-observable aircraft. Passive radar systems that exploit signals of opportunity are proliferating, as are a new generation of software-defined radars designed for rapid adaptation and upgrade with new and novel waveforms. And the latest generation of mobile surface-to-air missiles advertise multi-target tracking and simultaneous engagement capabilities at ranges measured in hundreds of kilometers.

Thus, NATO freedom of action in the air is no longer a given, as it was in the 1990s and 2000s. Today, operational planners and aircrews alike recognize that the future operations are likely to take place in heavily contested airspace. Forfeiting the ability to operate freely at the tactical and operational level has potential strategic-level impacts, as the emergence of increasingly sophisticated and highly resilient IADS has fundamentally changed the risk calculous in the minds of campaign planners and operational analysts.

A Royal Air Force Chinook dispenses decoy flares during operations over Afghanistan. A decade ago, NATO's air platform protection focus was on defeating MANPADS. The threat environment has since changed beyond recognition in its composition and complexity.

ROYAL AIR FORCE/CROWN COPYRIGHT

Faced with this growing challenge, NATO is moving quickly to change its approach to air survivability. Alongside ongoing modernization initiatives at both platform and mission levels, the subject matter expert community within the NATO Air Force Armaments Group (NAFAG) has promulgated a Next Generation Air Survivability (NGAS) framework designed to ensure that alliance air power can stay ahead of the threat in increasingly complex and contested air environments.

Acknowledging that the variety, capability and proliferation of threats is increasing, NGAS has a number of strands. For example, it enshrines a move away from a threat-specific focus, and instead seeks to deliver more proactive and agile airborne electronic attack (AEA), suppression of enemy air defenses (SEAD) and self-protect countermeasures solutions designed to defeat generic threat technologies. The concept also emphasizes greater use of model-based synthetic evaluation environments to overcome constraints affecting the scale and fidelity of live test events.

Equally important, it is recognized that the ultimate success of NGAS will require broader and deeper partnerships with industry: the objective is to better cohere research and development investment with frontline priorities, and to expand the "community of interest" beyond traditional electronic warfare

Advertorial

LAB TESTING OF MULTIPORT RADAR WARNING RECEIVERS UNDER REALISTIC CONDITIONS

Radar warning receivers often use multiple phase coherent receive paths to determine the signal angle of arrival. In order to test these receivers, the test system must be able to simulate a complex signal environment for all receive ports simultaneously.

Modern radar warning receivers (RWRs) usually have multiple ports in order to determine the direction of incoming signals. Airborne RWRs form part of an automatic self-defense system. They detect radars in the environment, and they identify and classify these radars based on signal characteristics such as frequency, pulse duration and interpulse/intrapulse modulation. In order to also precisely determine the direction of incoming signals, advanced RWRs are often equipped with phase coherent receive ports. To achieve 360°coverage of receive directions, the RWR antenna systems (e.g. individual antennas or antenna arrays) are distributed over the platform.

Direction determination methods

To determine the direction of an emitted signal, the following signal differences between the signals of the receive antennas are evaluated (Fig. 1):

- Time difference of arrival (TDOA)
- Amplitude differences
- Phase differences (interferometry)

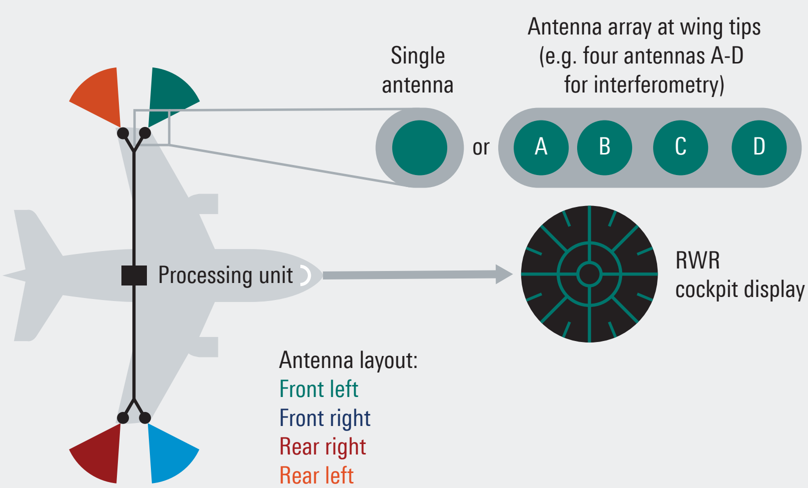


Figure 1:
Aircraft with a multiport radar warning system consisting of multiple receive paths, a central processing unit and a display. Source: Rohde & Schwarz

Requirements for the test system

Radars use RF frequencies up to 40 GHz, depending on the task, so radar warning receivers must be able to cover the same frequency range. This also applies to test systems for radar warning receivers.

To provide a radar warning receiver with signals that are as realistic as possible, the test system simulates an extremely complex RF signal environment with many radar signals on all receive ports at the same time. So the test system must have an independent signal source for each antenna input port of the receiver. Each generated signal at the receive antenna inputs can also contain many different radar and interference signals at the same time.

Plus, the test system must support long simulation times, moving transmitters and receivers, and a large number of antenna patterns and antenna scans. Multiport interferometric receivers additionally require a test system that can calculate the relative phase angles between the receive ports (antenna outputs) for each pulse as a function of the signal frequency, antenna arrangement and the positions of the emitter and receiver in three-dimensional space, and configure them with suitable precision. For this it is essential that the phase relationships between the generated signals remain stable during the simulation period (phase coherence).

The radar signal simulator from Rohde & Schwarz generates all required signals using multiple coupled, identical COTS vector signal generators. Thanks to the modular and software defined approach, this system provides extremely high scalability and flexibility. If a six-port RWR needs to be tested, the test system must be equipped with three R&S SMW200A two-path signal generators (Fig. 2). The RF Ports Alignment software from Rohde & Schwarz enables automatic calibration of the entire test system at the RF interfaces of the receiver. This is necessary in order to ensure the required precision in the relative amplitude and phase differences between the ports.

If necessary, a high-end R&S SMA100B analog signal generator can provide the shared LO signal for the vector signal generators.

Webinar: Efficient testing of multiport EW receivers

Generating real-life test signals in the lab is still the top goal when evaluating EW receivers. The presenters demonstrate challenges and solutions to overcome the complexity of test scenarios and signals. Starting with the requirements of testing basic pulse processing in Radar Warning Receivers (RWR), this webinar discusses and demonstrates the generation of phase coherent multi emitter signals without pulse dropping (pulse-on-pulse).

Find out more information and how to register at www.rohde-schwarz.com/radar

Embedding in a hardware-in-the-loop (HiL) environment

Radar simulators for multiport applications are often operated in an HiL environment, with the radar simulator embedded in the test system. It receives signal updates in the form of pulse descriptor words (PDWs) and updates the RF signals accordingly. Extremely high signal update rates and low latencies are usually essential. To achieve this, a fast computer streams PDWs to the signal generator in order to simulate the required radar scenario in real time. In technical terms, this is implemented using LAN-based high-speed PDW interfaces on the signal generators. With two installed RF paths per signal generator, update rates as high as 6 million PDW/s per path can be achieved this way. This allows an HiL environment to generate a high-density, realistic RF environment with many simultaneously simulated radars.

If necessary, additional RF ports or simulation features can easily be added by purchasing hardware components or software licenses.

Author: Robert Vielhuber

Figure 2:
A six-port radar signal simulator consisting of three R&S SMW200A two-path vector signal generators and an R&S SMA100B analog signal generator for the LO signal.
Source: Rohde & Schwarz

(EW), defensive aids systems (DAS) and countermeasures suppliers.

THREAT CHANGE

Briefing the EW community at last October's AOC Europe 2021 conference in Liverpool, the UK principals leading NATO's Sub-Group 2 on EW Protection Measures for Joint Services Airborne Assets (SG/2, a subgroup of NAFAG) detailed this new approach. "The threat continues to advance at pace," Mark Elson, fellow within the Electromagnetic Protection Group of the UK Defence Science and Technology Laboratory (Dstl), explained. "Potential adversaries are looking at what we do, and responding to how we operate. We now need to break their OODA [observe-orient-decide-act] loop, and we need to stay out in front.

"We've made some inroads, and we've got some really good capabilities [with legacy approaches]," he added. "But we have to think and act differently going forward."

As chair of SG/2, which has responsibility for EW protection measures for NATO's joint airborne assets, Elson's current focus is on rolling out the NGAS model across both the UK – working in close concert with Air Command – and the wider alliance. "NGAS is a framework to allow NATO to stay ahead of the threat," he told the AOC Europe attendees. "So we're going to think proactive, we're going to think system-level, we're going to think threat-agnostic [and] it's got to be agile, reprogrammable, and it's got to scale to the mission level."

Being proactive and agile is very much about "futureproofing," with SG/2 very much emphasizing the need to adapt and evolve to meet developments in the threat environment through-life – not just at entry into service. Scaling to mission level means multiple platforms working together to provide an overall integrated capability that maximizes all available resources.

What is driving this new mindset is a recognition that the reactive, threat-led posture that conditioned airborne countermeasures development for the past 70 years is no longer fit for purpose. Threat capabilities are able to use software defined architectures to evolve much faster than in the past, and EW systems developers must do the same. Both operational practitioners and the defense scientific community recognize that the EW development paradigm needs to adapt to this reality.

An Italian Aeronautica Militare Tornado ECR from 50° Stormo, 155° Gruppo ETS, departs on a training mission during the a "Blue Flag" exercise. NATO is developing an AEA/SEAD roadmap that is looking to rebalance and update the capability available to the alliance. USAF

This is where NGAS comes in. According to Wg Cdr Chris Greenwood RAF, Protection of Air Operations staff officer within Air Command's Air Capability Strategy team, the new framework – already endorsed as core to the UK air platform protection strategy – has been formulated to meet the challenge of operations in complex, non-permissive air environments. "We're looking to stay ahead of 'Red,' and work closely with industry and international partners to ensure we're providing spirally upgradable solutions to our platforms and warfighters when they need them," he told AOC Europe 2021. "We've been sharing this work with NATO so we can be aligned with threat landscapes and understandings, and work coherently towards future solutions."

The task, Wing Commander Greenwood continued, was to transition from a reactive, threat-specific approach to a new and more proactive model better suited to countering the threats of today and tomorrow. "If we think of a MANPADS, we can't be putting a new flare on a platform every time we come up against a new [threat]," he said. "We've got to be looking at these threat technologies [and] grouping them together. The aspiration for the future is to be truly threat-agnostic."

While more exotic countermeasures, such as high-power directed energy and hard-kill "shoot-back" missiles, may offer potential solutions in the future, their lack of maturity means they are not yet an option. "In the near-term, there is definitely going to be a requirement for using currently available technology in novel ways – and through better integration – to defeat threats in the next 10-15 years," said Wing Commander Greenwood, adding: "We also need to make sure these solutions are reprogrammable. As well as the speed of updating the data on the platform, we also need to be able to spirally upgrade the solutions so we are not constantly having to change the black boxes [on board]."

The new NATO Defensive Aids System (NDAS) architecture (see related article in JED Online) exemplifies this thinking. "This will provide a 'spine' on platforms [using] a common Ethernet bus," Wing Commander Greenwood explained. "This will enable us to, firstly, software-develop black boxes as far as possible, but also swap modules out individually without change to the whole system."

He continued: "We also have to think about self-protection at the platform level – how do we integrate the sensors and effects on a platform to defeat future threats? And then we have to think about how we work at a mission level – how we use SEAD, cyber and all the assets at our disposal to maintain freedom of action in this future air threat environment?"

Wing Commander Greenwood also highlighted the importance of synthetic environments. "We'll be modelling future experimental ideas which we'll only be able to do in synthetic environments [and] we'll be modelling what we think the future threat environment will look like.

He added: "We will be using these new [synthetic] environments to not only develop new systems, but also to assure them. This will require a mindset change – rather than have an aircraft flying down a range, and watching flares come off, we will be saying to commanders 'that computer over there said to me that you're going to be ok'.

"It also means that those synthetic environments need to be shared with industry. And it means that the 'blue' models that industry develops can be used in our synthetic environments can be used to assure. So, we have to be talking about open architectures."

COMPLEXITY

The view in SG/2 is that the complex nature of the threat landscape that has made traditional approaches to air survivability obsolete. Modern IADS integrate widely distributed surveillance sensors, anti-air missile systems and command centers in network-based architectures to provide coordinated "defense in depth" over a wide area, while also enabling air defense forces to adopt unconventional tactics and novel engagement modes. At the same time, the key attributes of the modern IADS – disaggregation, federation, redundancy, synchronization and fusion – make such systems increasingly resilient to both kinetic and non-kinetic means of SEAD.

"Adversaries don't operate as individual threats, they operate as a threat environment that is increasingly interconnected and integrated," explained Mark Threadgold, another technical fellow from Dstl's Electromagnetic Protection Group. "Within that environment, we are seeing long-range surveillance assets with detection ranges measured in thousands of kilometers, missile engagement zones measured in hundreds of kilometers. The threat is using multiple [EO and RF] wavebands to derive the information it needs to deliver hostile effect. So you may defeat a particular part of the system, but that does not stop the system working."

Threadgold became chair of the SG/2 Planning Committee in 2018, assuming responsibility for delivering a coherent approach and roadmap for air survivability activities within SG/2. He told the AOC Europe 2021 audience that it was time to stop fixating over specific threat systems. "Our current approach to understanding a threat in enough detail to counter it, and then working out how we put a countermeasure on our platforms, needs to be reviewed," he said. "We need a new approach to focus less on the threat, and instead focus on generic threat technologies [and to] develop spirally upgradeable solutions to stay ahead of the threat.

"It's a completely different ball game now," continued Threadgold. "And as things evolve – and they are evolving rapidly – everything is much more software-defined as part of a networked laydown. That challenges the way we think about not just what the threat is, but what we might actually face on the first day [of an air campaign]. So anything that we develop, or are basing on our understanding on today, could be very different by the time we face it on day one."

LAWS OF PHYSICS

Trying to predict how the threat could develop and evolve may appear near-impossible. But according to Threadgold, the reality is that technologies and techniques remain governed by the laws of physics. "We have to think generically about the technologies these threats use, and how we think about the vulnerabilities therein," he said. "If we understand the physics, and it's the same generic technology, then we can defeat that technology regardless of what it's stuck on. This gives us the chance to stay ahead of where the threat is going.

"So we need a new approach to develop and assure survivability, and we need to be proactive to stay ahead of the threat – let's not wait until we've seen these things before we try to work out how to defeat them. We need to work out solutions before we see them for the first time. And we need to raise our game at both platform and mission-level."

Cognizant of this reality, SG/2 has adopted a 16-box grid schema that plots a specific capability or concept against the threat environment. "This articulates how we move from where we are – a traditional approach – to a new way of working," said Threadgold. "It's really focusing on how we move from what is component level – the analogy here might be a countermeasure waveform against a tracking algorithm – up through a whole subsystem, such as a missile warner, into the platform. So that's a fully integrated threat against a fully integrated platform."

Finally, the model scales up to mission level. "That is now about how we understand the IADS problem," Threadgold said. "How do we use third-party-delivered effects in a SEAD role to counter – or to provide sufficient suppression of – a fully integrated IADS complex."

DISRUPTIVE TECHNOLOGIES

Matthew Cook, the Air Protection Science Adviser at RAF Air Command, identified key technology areas that are seen to have particular importance to air platform survivability. "The first of these is 'big data'," he said. "And what I mean in a threat context is data fusion [involving] different sources from across the electromagnetic spectrum. Never mind multi-band RF threats, or multi-band EO threats – what happens when you start fusing data from electro-optical sensors and radars at the same time?"

Next comes autonomy and artificial intelligence. "They provide more opportunities for the threat to become much more automated," Cook told AOC Europe attendees. "For example, image recognition is pretty much everywhere now – if a human can work out the difference between a platform and a flare, then why couldn't a threat as well?"

Cognitive EW is part of this, added Cook. "The ability to adapt to a scenario [and] not relying on those pre-programmed algorithms in order to track targets, and react to changes in the environment when a countermeasure effect is produced." There are also new and different threat vectors to consider. "The EW frame of the problem is no longer

An A400M airlifter dispenses flares from a Saphir-300 dispenser. The NATO Defensive Aids System project has been established to develop a standardized open architecture and common message set to support the "plug and play" integration of threat warning sensors and countermeasure effectors onto operational platforms. MBDA

just the platform, and the missile coming towards you – it's much more complicated," Cook said. "For instance, swarming drones [and] uncrewed systems as well. Really, the key message on emerging and disruptive technologies in a threat context is the enhancement to situational awareness and target tracking."

NATO's Science and Technology Organization (STO) is already active in response to these developments, with one example being SCI-327. According to Cook, this three-year research task group, organized under the Systems, Concept and Integration (SCI) Panel, is exploring novel countermeasure concepts against dual-band EO/IR imaging seekers. "[SCI-327 is] the leader in a new way of predicting what the future threat is going to look like, and then producing countermeasures for those threats in a much more generic way," he said. "It means that regardless of what the future threat ends up looking like, we can have something ready on the shelf for when it becomes a problem."

Another activity, SCI-344, is focused on developing and evaluating approaches to defeating future multi-sensor (EO/RF) threat systems to increase the survivability of air and maritime platforms. A precursor exploratory team (SCI-ET-050) has already conceptualized a number of sensor-fusion based algorithms. The intention is that SCI-344 will be able to anticipate potential counter-countermeasure techniques being utilized by future multi-sensor threats in its development of candidate generic defeat concepts.

What should also be borne in mind, Cook added, is that the self-same technologies offering potential advantage to "Red" also provides exploitation paths for "Blue." "Cognitive EW, for instance, could provide an opportunity for us to step away from those all-important pre-programed parametric mission data sets," he explained. "A cognitive radar warning receiver that could detect the threat by virtue of some generic characteristic of its waveform would be incredibly useful."

NEW MODEL

The threat developments outlined by Cook demand that SG/2 also revises its organization. Previously, there has been a focus on separate EO and RF activities in single wavebands, a separation between detect and defeat, and an emphasis on trials events.

But no longer. "Given the threats we are facing, continuing in this way will not work," said Threadgold. "Our current approach does not scale to meet the challenges of the future."

SG/2 and its various communities of interest are being reoriented to reflect NGAS aims and objectives. This means taking an integrated project approach to detect and defeat, whether in EO or RF. "We're putting together a roadmap that no longer looks at [different] areas in isolation," Threadgold said. "Each of the activities we now deal with in SG/2 brings together the expertise needed from those sub-teams beneath to deliver fully integrated activities at either platform-level or mission-level.

"You still need to go through those component stages to get some underpinning evidence, but the output and the advice that we provide is now much more aligned to the platform and the mission level. That's what the operators care about."

Test and evaluation also require revisiting. Delivering live 'in air' testing that is truly representative of the integrated threat environment, at the required scale and fidelity is extremely challenging both technically and financially. Furthermore, this approach does not align well to the flexibility and agility mantra that underpins NGAS and the need to stay ahead of the threat. This is even before the sensitivities associated with exposing novel countermeasure solutions during live test events.

"Understanding how we develop the right synthetic environments, and what we use them for, and how we use live testing to collect that validation data we need, is a fundamental new approach that we are driving towards," said Threadgold. "The days of assuring platform survivability solely by testing on a test range against an example of a threat, to make sure it works, are gone.

"If we are going to assure through synthetic environments, we need to have confidence that the synthetic environment is up to the job we're asking it to do."

The challenge here is to be able to bring together all entities – software models, digital twins and real hardware – in a single evaluation tool that provides both complex threat emulation and comprehensive platform representation. "We want to deliver a fully integrated, multi-platform survivability solution against a complex mission-level threat," said Threadgold. "So, you need to understand the whole network, and how you operate and survive in that environment."

US Army Aviation Trai
Challenges of Changin

By John Haystead

US ARMY PHOTO

As is the case DOD-wide, the top objective today of America's military is rapidly transitioning its military capabilities from a focus on irregular or asymmetric warfare to the very real (and much more dangerous) threats posed by peer and near-peer adversaries. The path to accomplishing this means much more than the development and fielding of new and superior technology and system capabilities, however. First and foremost, it means major changes to doctrine, education and training. And, very specifically, it means concerted attention to revamping Service capabilities and tactics to gain and maintain operational superiority in the Electromagnetic Spectrum (EMS).

In the case of Army Aviation, this responsibility falls squarely on the shoulders of the US Army Aviation Center of Excellence (USAACE) at Fort Rucker, AL. USAACE is responsible for providing the Instructor Pilots (IPs) for all overall Army aviator training, including the next-generation of Aviation Mission Survivability Officers (AMSOs). The organization is currently in the midst of a major restructuring of its instructor training paradigm aimed at a much tighter linkage between pilots and AMSOs.

As described by Chief Warrant Officer 4 (CW4) Chris Crawford, AMS Training Developer, within USAACE Directorate of Training and Doctrine (DOTD) Survivability Branch, the transition really began with Army aviation's major shift in training's emphasis to operational tactics development as a means to greater survivability. "Thus, the big-picture goal of the Army Aviation Tactics Transformation Initiative is to increase tactical focus and competency in its aviators, increase readiness for large-scale combat operations while capitalizing on existing counterinsurgency operational expertise."

Says Crawford, "recognition of the critical role of role of the AMSO in this process, really dates back to the 1990s with the conclusion of Operation Desert Storm, when the position of Tactical Operations (TACOPS) Officer was formed out of the two-week Electronic Warfare Officer (EWO) course at Ft. Rucker. These TACOPS officers would later become AMSOs in the 2013 time period and really begin to take root around 2015 -2017 with additional elements added to the AMSO course where they receive training in the fundamentals of instruction, simulation for flying against a threat, and validation of the tactics which we actually fly."

Crawford explains, "The process really began in earnest in 2015 when strategic studies caused us to focus on near-peer and peer adversaries and the capabilities that they had developed. This led the Army Aviation Survivability Development and Tactics (ASDAT) team to write the first ever classified Army Aviation Survivability Guide. This guide has since evolved into the classified TC3-04.2 Aviation Combat Survivability and Tactics manual and formed the doctrinal foundation of our beginnings in tactics testing and validation. This process we call our Quick Reaction Test (QRT). We've done several of these QRTs to develop what we currently call our 2800 and 2900 series Aircrew Training Manual (ATM) tasks, and we are in the early stages of forming the next QRT. A major milestone was reached in 2017 with the completion of the first Quick Reaction Test (QRT), which would help result in the development of some of the tactics we now use to fly against today's threats and which continue to evolve."

In describing the thinking behind Army Aviation's plans for revamped pilot and AMSO training, Crawford references their heavy reliance on Dr. Robert Ball's book, *The Fundamentals of Aircraft Combat Survivability: Analysis and Design,* in helping to direct their efforts. Crawford says, "Dr. Ball points to two primary pillars – susceptibility and vulnerability – in his analysis. And for AMSO training, we focus on the susceptibility pillar and particularly susceptibility reduction through our own three pillars which are: fused

ning Evolves to Meet g Threat Dynamics

mission planning – taking in intelligence collection and fusing it into the aviation mission planning process; evasive flight tactics which is how we maneuver our aircraft in response to the threats we face; and greater understanding of the threat. In today's Combat Aviation Brigades (CABs), we now have both EWOs and intelligence officers, but the AMSOs are synchronizing those collection efforts and the understanding of the EMS and then taking that information and really filtering it down to the pilot level so it can be useful to reduce our susceptibility in the threat environment being faced."

As part of the changes, AMSOs will now be teamed with the new Aviation Tactics Instructors (formerly IPs). This transformation is going on right now. As explained by LTC Brian Silva, Brigade Operations Officer, 110th Aviation Brigade, the flight training brigade at Ft. Rucker, "The evolution of the IP course and the future vision for follow-on Aviation Tactics Instructor Course (ATIC) is to work much more closely in each of our formations with our AMSOs. The way we're pursuing this is by evolving the current IP course into a much more tactically-focused program. It's enabled by two other initiatives that USAACE is pursuing. By combining a training foundation from both the Aviation Warfighters Skills (AWS) program plus the Unit Trainer Evaluator (UT/E) program, these two pieces enable us to transform the formal instructor pilot training program that we're able to deliver here at Ft. Rucker."

AVIATION WARFIGHTERS SKILLS

As emphasized by Crawford, "Today, there is an entire paradigm shift in how we fight, including a focus on flying low and a renewed emphasis on tactics. This means major changes to the current professional military education and functional courses. Our aircrews must have a graduate-level understanding of the threats we face, how we understand and articulate tactical risk, and the manner in which we conduct mission planning to mitigate those risks."


US ARMY PHOTO

As a result, USAACE is reshaping its Professional Military Education (PME) curriculum to include classified training on threats, survivability and tactics. The latest example of this is the Aviation Warfighters Skills (AWS) course, which is replacing the Aviation Warrant Officer Advanced course. AWS focuses on warrant officers earlier in their career progression in order to train them at the classified level for mission planning, threat scenarios, survivability and tactics. Says Crawford, "The shaping of our PME earlier in the Warrant Officer career path helps build a strong foundation rooted in tactics from which to grow once they get ready to track. The AWS and UT/E programs will help to greatly enhance our lethality and survivability in future operational environments."

UNIT TRAINER/ EVALUATORS (UT/Es)

The UT/E program is a Directorate of Evaluations and Standardization (DES) initiative within USAACE. Says CW4 Jimmy Wilson, DES AMSO, "Although the UT/E initiative is not progressing as fast as we would like it to, it is really starting to kick in and gain traction, especially in the AMS community." Wilson says, that currently the most requested UT/E is for the AMS right now, where the AMSO in a unit starts training and evaluating the pilots and crew members in their units. "We're on the road constantly from DES and with roughly seven units scheduled in the next six months to include UT/Es. As of this date, we have 19 completed UT/E candidates and are tracking them closely to see how they're being utilized and their effectiveness within units. Units that are already utilizing them are seeing more and more benefits and really beginning to better understand how to fully utilize their potential and offload some of the more basic requirements from the IPs so that they can focus on bigger and higher-level training." Says Lieutenant Colonel Silva, "The focus of the training will be completely different from what our IPs currently receive. Whereas currently a lot of our IP preparation is really oriented on basic aircraft handling, really doing very basic maneuvers but making sure they're done very safely, we think we can offload a lot of this onto the UT/Es, which are developing in the units. As a result, our future tactics instructors will be able to focus much more on mission and tactical tasks, and advising their commanders on small unit employment probably up to platoon level."

Wilson says they're still in the validation phase of the progression of UT/Es, "but we're hoping that will change here shortly. Right now, Component 1 (COMPO 1) active units have been the primary beneficiary of UT/E, with our first COMPO 2 National Guard UT/E candidate starting next month, with more lined up over the next few months." As more UT/Es come on line, the hope is that the new ATI course will begin to stand up around the Fall of 2024 or just after the new year (FY2025).

MUCH EXPANDED ROLE FOR AMSOs

Currently, the AMSO course falls under the 1st Aviation Brigade at Ft. Rucker, but as a part of the new comprehensive

US ARMY PHOTO

training transformation, it is now moving into, and aligning under, the 110th Aviation Brigade where the ATIC will also be located. As outlined by Lieutenant Colonel Silva, "Fundamentally, we have two brigades at Ft. Rucker, as well as a third brigade that is not part of USAACE. The 1st Aviation Brigade has all of the flight students and has a lot of the professional military education courses that don't involve flight instruction. The 110th is where they receive all of their actual flying training through the IPs that we have in the brigade. The driver behind transferring the AMSO course from the 1st to the 110th Brigade is that there is now a greater emphasis on simulator instruction in the course. Because of the similarities between the two programs (AMSO and eventually ATIC), it's actually exactly the way we want AMSO and tactics instructors to function in the field, speaking a similar language and approaching problems from only a slightly different viewpoint." He says the move is tentatively expected to happen in April of this year.

QRT, ICTL AND METL

As part of the AMSO course restructuring effort, USAACE has been developing a new AMSO Individual Critical Task List (ICTL) to better meet the goals of a more tightly integrated AMSO/ATIC course program. Says Crawford, "When this effort first started several years ago, we went through an initial critical task site selection board. It really came down to seeing what the other Services did, with each doing things slightly differently, and we wanted to validate through testing and scientific methodology why we do what we do. So, we went out to the Naval Air Weapons Station at China Lake, CA, and conducted tactics validation testing (Quick Reaction Testing – QRT) to validate why we do what we do. Those lessons became the classified 2800 and 2900 Series tasks that we now train all of our aviators on."

The team is now about to go into the next phase of the process with a new critical site selection board and QRT just approved to review the critical tasks of the AMSO. Says Crawford, "What is unique about this next one, that will begin this summer, is that we will be involving the developers of the ATI course to ensure we align roles and responsibilities of the tactics instructors and the AMSOs moving forward. That will really codify this new synchronization effort and our path forward under the 110th Brigade, and we're extremely interested to see what comes out of this."

The AMSO ICTL differs from the Mission Essential Task List (METL), which is representative of what the AMSO's role is in terms of what they provide a unit commander. As explained by Crawford, "METLs are what the unit provides and what their role and responsibility is overall. They recognize that, while all Combat Aviation Brigades (CABs) are very similar in design right now, they are also all aligned to different regions and responsibilities, so they're not all exactly the same. The METL is really sort of the unit's core competencies – the reason that it exists in the Army. METL is the priwmary role of that unit and it is expected to perform, based on the way it is organized, the equipment that it has fielded, etc. whereas the individual CTL is tied to that officer's specific Military Occupational Skill (MOS)."

ASDAT TEAM

With the stand-up of UT/Es and ATIC training, the role of the AMSO is also necessarily taking on much greater importance. One aspect of this can be seen in the formation of the Aviation Survivability Development and Tactics (ASDAT) team. Also based at Ft. Rucker, the ASDAT team is composed solely of AMSOs, but falls under the Joint Combat Assessment Team (JCAT) which, in turn, falls under the Joint Aircraft Survivability Program (JASP) office. The primary function of JCAT is to serve as aviation 'combat forensic' officers, studying threats and maintaining close ties with forward-deployed units, so that in the event that an aircraft is brought down, they can rapidly deploy to perform a forensic investigation into the specific cause(s). Says Crawford, "because of their unique knowledge and unit placement at Ft. Rucker, they fall under the Requirements Directorate or what we call the

Army Capability Managers (ACMs). They work a lot in the test world and were a part of the original effort that led us to the QRT. In fact, they started it, but they weren't alone in this. It was a synchronized effort between DES, DOTD, and several other organizations here at Ft. Rucker. It's a unique expertise with close ties to the current fight, and so they're very much involved in tactics development and advising the force on what to do when something new pops up in the world and then advising the aviation enterprise on a direction to fix it through requirements writing."

GREATER EMPHASIS ON SIMULATION TOOLS

As mentioned earlier, one of the reasons that the AMSO course is moving over to the 110th Brigade is their greater use of simulation tools in training. Says Lieutenant Colonel Silva, "With the AMSO course that students are going through right now, you have students from all different platforms going through with extensive simulation training, especially involving the survivability maneuvers developed from the QRTs."

In particular, Silva points to the Reconfigurable Virtual Collective Trainer for Aviation (RVCT-A). Although not yet fielded, The RVCT-A will be a future collective trainer for the force. Silva says he's excited that Ft. Rucker will be on the leading edge of the fielding schedule. "RVCT-A will replace some of the older collective trainers that the Army has now and will be fielded to units in addition to training locations like here, at Rucker."

The RVCT includes aviation platforms (RVCT-A), ground platforms (RVCT-G), dismounted infantry collective maneuver training, collective gunnery training and mission rehearsal capability. The RVCT is described as a "mobile, transportable, modular and scalable training capability with the minimum hardware necessary to represent form, fit, and function for the user to execute collective tasks. The system will use the Common Synthetic Environment (CSE) platform enabler, which is comprised of three foundational capabilities: One World Terrain (OWT), Training Management Tool (TMT), and Training Simulation Software (TSS). The RVCT architecture and design will enable and support interoperability with the future Next Generation Constructive (NGC), Live Training Environment, and other Synthetic Training Environment (STE) and operation capabilities."

Lieutenant Colonel Silva says they're planning on using it extensively during ATIC training, with the culminating phase being an entire classified mission scenario that requires the students to plan, rehearse and execute their own missions in a mixed-airframe mission (Apaches, Black Hawks, Chinooks, etc.). "By doing a tactical mission in a classified collective trainer, we will be able to replicate high-threat enemy systems and allow the students to operate in that environment," he explains.

Across the entire USAACE team, Crawford says they stay in constant communication with each other, with regular meetings between all the entities involved to ensure that all of their different efforts are coordinated. "Although DES is necessarily on the road so much,

USMC PHOTO

when they come back, they do a data dump with us," he explains. "This is critical since they're out there connected to the field and seeing the implementation of the doctrine we're creating. We've been reliant on them to give us that feedback and help evolve the doctrine and make it better for the force based on what the force is telling DES. There is also the recent relationship with the 110th and the development of the ATIC course and the continued relationship with the AMSO course moving over into 110th is really solidified. At the end of the day, we're all trying to make Army aviation better and trying to prepare for the next fight of multi-domain, large-scale combat operations, that may be sooner than we think."

In reflecting on the evolution of the AMSO training process over the past 15 years, "and seeing where we're going and where we're driving, and in particular from the feedback from the field," Crawford says, "I think the most important aspect of the transformation of the TACOPS into the AMSO and moving forward is that, a lot of times the AMSO or the TACOPS officer was referred to as a 'Jack-of-all-Trades,' or simply 'the kitchen sink,' whereas as an Army Warrant Officer, we are not that. We are masters of our technical and tactical areas; so the refinement of what the AMSO is and the further refinement that we're going to be doing in this next critical task site selection board with ATIC to align our roles moving forward is really solidifying what the job is, what capability we bring to a commander. It will no longer be a case of not really knowing what an AMSO does; it will be very clearly defined. And, commanders are being educated on how to use that tool of the AMSO to really increase their survivability in these large-scale combat operations."

5G Communications – Part 13

Jamming of 5G Signals *cont.*

By Dave Adamy

JAMMING A 5G SATELLITE LINK

Remember that to jam any link, you need to jam the receiver – not the transmitter. Thus, to jam a satellite uplink from the ground, it is necessary to transmit a jamming signal to the satellite. The good news (for the jammer) is that the satellite receiving antenna is pointed toward the ground; the bad news is that the satellite is far away. Back in February, we considered a mid-band 5G satellite uplink, jammed from the ground. Now we will consider a high-band uplink.

HIGH BAND SATELLITE UPLINK

Fig. 1 shows the desired signal and jamming links. For convenience, we will use the same physical situation we used for the mid-band satellite uplink in the February 2022 "EW 101" column. The satellite is 300 km high, directly over the ground station, and the jammer is far enough from the satellite ground station that the satellite is 10° above its horizon. In February, we just did the math to determine that the jammer-to-satellite distance was 1,151 km. For completeness, we now calculate that this would place the jammer on the Earth 1,090 km from the ground station. We calculated that the geocentric angle from the jammer to the ground station was 9.8°. That makes the earth surface distance 0.0272 times the 40,030-km circumference of the earth.

Next, use the same 28-GHz signal frequency and 64 element array antenna we used in last month's EW 101 column. That gives us 18 dB boresight antenna gain for both ends of the uplink. The satellite receiving antenna gain is still approximately 0 dB to the jammer (which is assumed to be far from the main beam). The J/S calculation is the same as that calculated last month, except the jammer is much farther away (1,151 km vs. 40 km) and the uplink distance is 300 km vs. 25 km.

This makes the space loss from the jammer to the receiver:

32.4 + 20 log(1151) + 20 log (28000) = 182.5 dB

And the loss from the uplink transmitter:

32.4 + 20 log(300) + 20 log (28000) = 170.8 dB

So the jamming-to-signal ratio is now:

J/S = ERPJ – ERPS – LJ + LS + GRJ - GR = 60 – 58 – 182.2 + 170.8 + 0 - 18 = -27.4dB

It is actually worse than that because the atmospheric attenuation (as shown in **Fig. 2**) is 2 dB from the jammer and negligible for the vertical uplink.

Last month, we looked at the situation in which the jammer is placed at the boresight of the target receiver's antenna to allow a more than adequate jamming-to-signal ratio of 6.2 dB. That won't work for this case, because the jammer would have to be at the ground station.

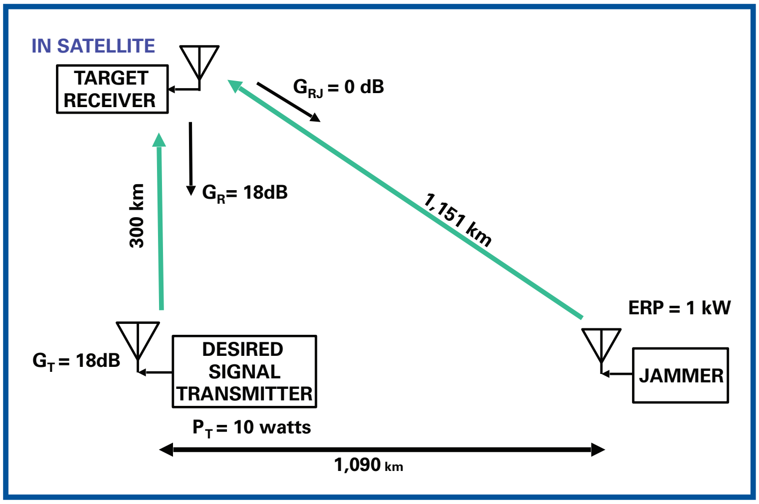


Fig. 1: *The target receiver is in a Low Earth Orbit satellite at 300 km altitude. A high-band (28 GHz) 5G link is used by a ground transmitter with an antenna elevation of 90°. The 1-kW jammer is on the earth's surface with an elevation to the satellite of 10°.*

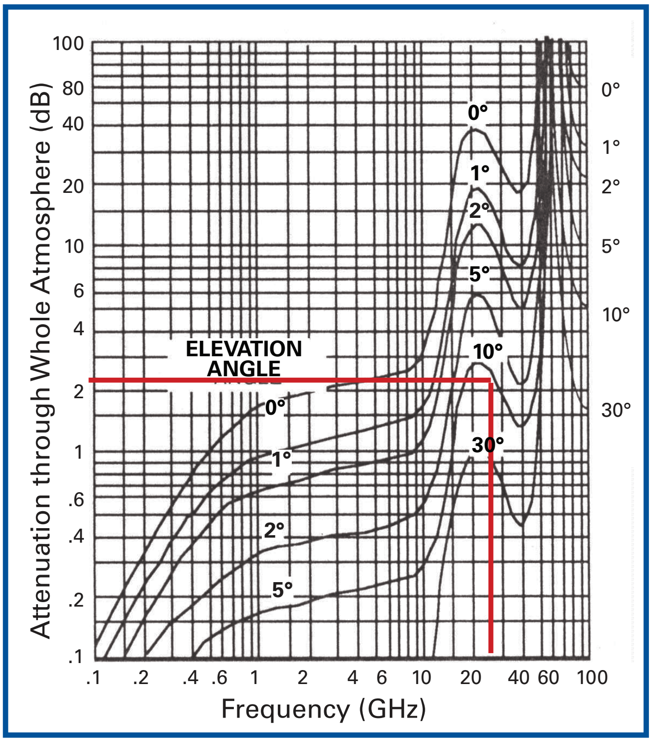


Fig. 2: *The atmospheric attenuation through the whole atmosphere at 28 GHz is 2 dB at 10° elevation, but negligible at 90° elevation.*

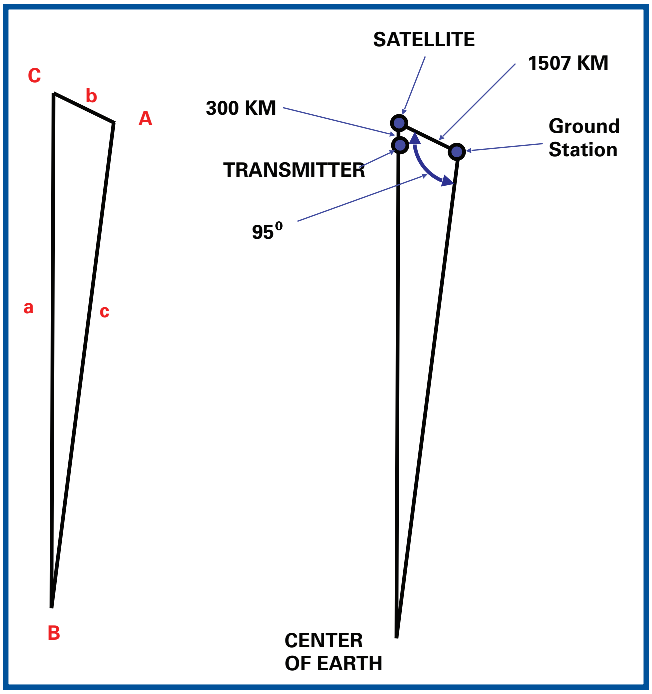


Fig. 3: This illustration shows the link geometry for a satellite in a 300 km high orbit when the satellite is 5° above the ground station's horizon.

WHAT IF THE SATELLITE IS ONLY 5° ABOVE THE HORIZON TO ITS GROUND STATION?

The worst-case jamming is when the satellite is closest to its ground station, but the best case is when the satellite is only 5° above the horizon. The satellite-to-ground-station geometry is shown in **Fig. 3,** for a satellite in a 300-km-high circular orbit when it is 5° above the horizon to its ground station. The satellite, the ground station, and the center of the earth form a plane triangle. The sides of the triangle (lower case) and the angles (upper case) are shown in the same figure. Side *a* is the radius of the earth + the satellite elevation (6,671 km), side *c* is the radius of the earth (6,371 km) and angle *A* is the elevation of the satellite above the center of the Earth (90° + 5° = 95°). The sine of 95° is 0.996. From the law of sines, we can calculate angle *C* to be:

arcsin (6371 x 0.996 / 6671) = 72.0°

Angle B is: **180° - 95 - 72.0° = 13°**
The sine of 13 degrees is **0.225**
Then, from the law of sines, side *b* is

6671 x 0.225 / 0.996 = 1,507 km

This is the distance from the satellite to the ground station., so the loss for the desired signal link is:

32.4 + 20 log (1507) + 20 log (2800) = 185 dB

Now the jamming-to-signal ratio is increased to:

J/S = ERPJ – ERPS – LJ + LS + GRJ - GR = 60 – 58 – 182.2 + 184.9 + 0 - 18 = -13.3dB

This is 14.1 dB better, but still nowhere near adequate jamming.

JAMMING THE DOWN LINK

Fig. 4 shows a 1-kW (ERP) jammer in an unmanned aerial vehicle flying at 2000 meters altitude and 50 km from the ground station of the above-described satellite. It is jamming the satellite's down link. This requires transmitting a jamming signal to the receiver, which is on the ground. To get a clear path to the receiver, it is necessary to have the jammer in the air.

The satellite is still directly over its ground station, but now the jammer is much closer to the target receiver than the desired signal transmitter, so a greater jamming-to-signal ratio is practical to achieve.

The loss from the link transmitter to the link receiver is the same as in the uplink:

32.4 + 20 log(300) + 20 log (28000) = 170.8 dB

The loss from the jammer to the link receiver is now:

32.4 + 20 log(50) + 20 log (28000) = 155.3 dB

The atmospheric loss is negligible in both links.

The jamming-to-signal ratio is:

J/S = ERPJ – ERPS – LJ + LS + GRJ - GR = 60 – 58 – 155.3 + 170.8 + 0 - 18 = -0.5 dB

This will do an adequate job of jamming, unless there is an electromagnetic protection measure in the link.

If the satellite is 5° above the ground station's horizon, the J/S is increased by 14.1 dB, to + 13.3 dB, which is excellent jamming (if there is no electromagnetic protection in the link).

If the jammer UAV can be positioned closer to the satellite ground station location, the jamming-to-signal ratio can be significantly improved. For example, if the jammer is in a side lobe of the ground station receiver, the J/S would be 4.5 dB better. If it is located at the boresight of the receiving antenna, the J/S would be 18 dB better. Either of these cases would allow a smaller UAV with a jammer transmitting a much lower ERP to be used. If there were a swarm of several small UAVs with low-power jammers, the jamming could be very effective.

WHAT'S NEXT

Next month, we will start a new series on electromagnetic protection. Dave Adamy can be reached at dave@lynxpub.com.

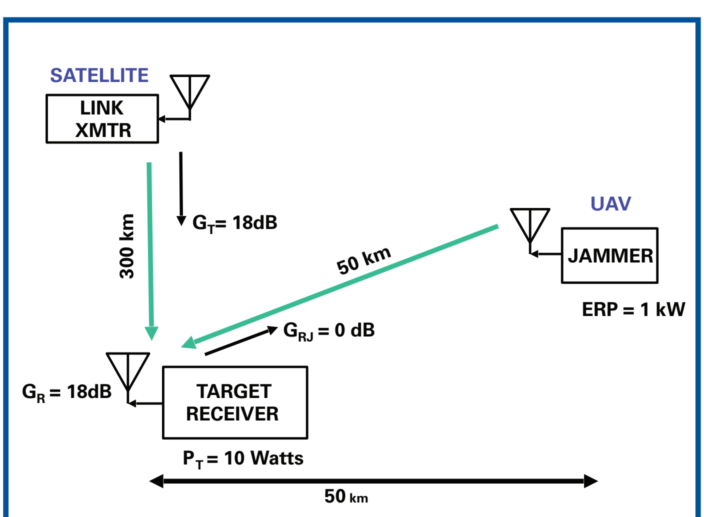


Fig. 4: The transmitter is in a Low Earth Orbit satellite at 300-km altitude. Its ground station (directly under the satellite) uses a high-band (28 GHz) 5G link. The 1 kW jammer is on a UAV flying at 2000 meters altitude, 50 km from the ground station.

TRIBUTE TO LT COL STEPHEN "MUDDY" WATTERS, USMC (RET.)

Muddy Watters, who served the AOC in many capacities and most recently as AOC President from 2018 to 2020, passed away on 5 March 2022. We say goodbye to one of the EW Community's staunchest champions.

After graduating from Western Colorado University in 1979, Muddy joined the US Marine Corps and embarked on a distinguished 35-year career in EW. He was an Honor Graduate and Outstanding Student of the 453d EW Course at Mather AFB, CA, and served as an EA-6B aviator in various VMAQ squadrons during his years of military service. He flew combat missions in Desert Shield, Desert Storm, Operations Deny Flight and Deliberate Force. His awards and accomplishments included nine Air Medals, three for valor in combat; lead briefer for Marine Corps Suppression of Enemy Air Defense Lessons Learned for Bosnia; US lead for NATO Suppression of Enemy Air Defense training and coordination; and Instructor of the Year – Instructor Hall of Fame Landing Forces Training Command Pacific. In 1996, he earned an MA in National Security and Strategic Studies (with honors) from the US Naval War College and later was selected as commander of Marine Tactical Electronic Warfare Squadron 3 (VMAQ-3) at MCAS Cherry Point, NC.

After retiring from the Marine Corps, Muddy held various industry positions and participated in several high-level EW studies for OSD and NSA, including the 2002 Airborne Electronic Attack Analysis of Alternatives (AEA AOA) study.

During the Iraq War, Muddy provided support to the Joint Staff J-65 for Counter IED (Improvised Explosive Devices) and also served as Director of the Technical Analysis Group at the Joint IED Defeat Organization (JIEDDO). RCIEDs were a relatively new threat to US troops, and Muddy was a strong advocate for developing a counter-RCIED strategy because he knew that EW systems could be effective at saving soldiers' lives. Muddy later served as the Senior Manager for Cyber and EW at Raytheon Advanced Missile Systems in Tucson, AZ, where he worked on advanced EW concepts and technologies.

During his career in Industry, Muddy became more involved with the AOC and was a strong advocate for STEM education. Muddy believed that students (future Crows) needed to be engaged at an early age, and he helped build the foundation for what the AOC STEM program is today. It was his vision to create the learning stations and the hands on "petting zoo," as he liked to call it, at the AOC's International Symposium and Convention.

Muddy's tenure as AOC President was very popular, and all 67 AOC chapters and over 14,000 members benefitted from his inspirational leadership. Every EW advocate, regardless of service or of company affiliation, counted Muddy as a fighter in their ranks. Muddy always handled himself with great competence and confidence, whether addressing congressional representatives, military and civilian leaders or young STEM students.

Muddy has earned our farewell salute for a job well done. He was one of our very best and brightest EW professionals, and we will miss him dearly. Semper Fi.

Glenn "Powder" Carlson
President, Association of Old Crows

AOC Members

SUSTAINING

BAE Systems
Bharat Electronics Ltd.
CACI International Inc.
Chemring Group PLC
Electronic Warfare Associates, Inc.
General Atomics Aeronautical Systems, Inc.
General Dynamics
Keysight Technologies
L-3 Harris
Leonardo
Perspecta
Raytheon Intelligence & Space
Rohde & Schwarz USA
Saab Sensor Systems Germany GmbH
SRC, Inc.

MILITARY UNITS

30 Cdo IX Gp RM
547 IS
57 IS/DOD
Air Command Denmark
Detachment-A 743d
Helicopter Wing 53
IWTG Norfolk
Japan Air Self-Defense Force
NASIC/AC
NIWTG SD
Zentrum Elektronischer Kampf Fliegende Waffensysteme

INSTITUTES/ UNIVERSITIES

Georgia Tech Research Institute (GTRI)
Mercer Engineering Research Center (MERC)
Riverside Research Institute
RVJ Institute

GOVERNMENT GROUPS

ACEASPO
Australia Department of Defence DIO
DE&S
Defence Science & Technology Agency
DOD
Los Alamos National Lab
New Zealand Defence Technology Agency
NGA – National Geospatial-Intelligence Agency
NLR – Royal Netherlands Aerospace Centre
Swedish Defence Materiel Administration T&E Directorate

GROUPS

3dB Labs Inc.
Abaco Systems
Ace Consulting Group
Ad hoc Research Associates, LLC
Aeronix, Inc.
Aethercomm Inc.
Alaris Antennas
Allen-Vanguard
Ampex Data Systems
Analog Devices
Anritsu
API Technologies
ApisSys SAS
Apogee Engineering
Applied Systems Engineering, Inc.
Armtec Defense Technologies
ARS Products
Aselsan A.S.
Atkinson Aeronautics & Technology, Inc.
Atlanta Micro, Inc.
Atrenne, a Celestia Group Company
Avix
Azure Summit Technology, Inc.
Babcock International Group
Beca Applied Technologies Ltd.
Black Horse Solutions, Inc.
Blue Ridge Envisioneering, Inc.
Booz Allen Hamilton, Inc.
Boyd Corporation
Cablex PTY Ltd.
CEA Technologies, Inc.
Centauri
Centro de Guerra EletrÃ³nica – PTAF
Clearbox Systems
Colorado Engineering Inc.
Communication Power Corporation
Communications & Power Industries LLC
Comsec LLC
Comtech PST Corporation
Crescend Technologies, LLC, Defense Solutions
CRFS Inc.
CRFS Limited
CSIR DPSS
Cubic Defense
D-TA Systems, Inc.
Daqscribe
Darkblade Systems
Dayton Development Coalition
dB Control
DCS Corp
Decodio AG
Defense Research Associates Inc.
Deftec Corporation
DEWC Group
Dreamlab Technologies AG
Eagle Sales Corp.
Elbit Systems of America
Elbit Systems of EW & SIGINT Elisra
Eldes S.R.L.
Electro-Metrics Corp.
Elettronica S.p.A.
Elite RF
Elmtek Pty Ltd
Empower RF Systems
Epiq Solutions
Esroe Limited
Evans Capacitor Company
Galleon Embedded Computing
GFD GmbH
Government Business Development
Hammer Defense Technologies LLC
Hasco
HawkEye360
Hegarty Research LLC
Hensoldt Sensors GmbH
Herrick Technology Laboratories, Inc.
IAI North America
IDS International Government Services
Indra
Intelligent RF Solutions
Interface Concept
Ispin AG
ITA International, LLC
IW Microwave Products Division
JT4, LLC
KBR
Key Bridge Wireless
Kihomac, Inc.
Kirintec
Kranze Technology Solutions, Inc. (KTS)
Kratos General Microwave Corporation
L3Harris TRL Technology
LCR Embedded Systems
Leonardo DRS
Leonardo Electronics-US
Liteye Systems, Inc.
Lockheed Martin Co.
MarServices GmbH
Mass Consultants Ltd.
Maxar-Ypsi-EW
MBDA France
MC Countermeasures, Inc.
MDA
MDSI
MegaPhase LLC
Meggitt Baltimore
Meggitt Defense Systems
Meta Mission Data Ltd.
Milpower Source, Inc.
Milso AB
Mission Microwave Technologies
The Mitre Corporation
Motorola Solutions
MTSI
My-Konsult
MyDefence System Integration
N-Ask Incorporated
Nagravision S.A.
NEL Frequency Controls, Inc.
Northeast Information Discovery Inc.
Northrop Grumman Defense Systems – Advanced Weapons
Novator Solutions AB
OCS America, Inc.
Parsons
Pentek
Penten
Peraton/Perspecta
Persistent Systems, LLC
Perspecta
Phasor Innovation
Photonis Defense Inc.
Physical Optics Corporation
Plath GmbH
PredaSAR
Procitec GmbH
QuantiTech
Rada Technologies LLC
Rafael Advanced Defense Systems Ltd.
Research Associates of Syracuse, Inc.
RFHIC US Corporation
Rincon Research Corporation
Rohde & Schwarz GmbH & Co. KG
Rohde & Schwarz Norge AS
Roschi Rohde & Schwarz AG
S2 Corporation
SciEngines GmbH
Scientific Research Corp.
SEA Corp.
Serpikom
Sierra Nevada Corporation
Signal Hound
Silver Palm Technologies
SimVentions
SMAG Mobile Antenna Masts GmbH
Smiths Interconnect
SOIO
Spectranetix, Inc.
Spherea GmbH
Spirent Communications
SR Technologies
Stellant Systems
Swisscom Broadcast AG
Sypaq
Systems & Processes Engineering Corp. (SPEC)
Tabor Electronics
TCI International, Inc.
Tech Resources, Inc.
Teledyne Technologies, Inc.
Telemus Inc.
Teleplan Globe Defence
Terma
Tevet LLC
Textron Systems
Textron Systems Electronic Systems UK Ltd.
Tinex AS
TMC Design
TMD Technologies Ltd.
Transformational Security LLC
Transhield Inc.
Trenton Systems
Trideum
Tualcom, Inc.
Ultra Electronics – EWST
Ultra Electronics Avalon Systems
unival group GmbH
Vadum Inc.
Valiant Integrated Services
Valkyrie Enterprises LLC
Verus Research
Viavi Solutions
Vigilant Drone Defense Inc.
Vitec
W.L. Gore and Associates
Warrior Support Solutions LLC
WGS Systems, Inc.
X-Com Systems
Zarges, Inc.
Zentrum Elektronischer Kampf Fliegende Waffensysteme

ASSOCIATION OF OLD CROWS

JED, Journal of Electromagnetic Dominance (ISSN 0192-429X), is published monthly by Naylor, LLC, for the Association of Old Crows, 1001 N. Fairfax St., Suite 300, Alexandria, VA 22314.

Periodicals postage paid at Alexandria, VA, and additional mailing offices. Subscriptions: *JED, Journal of Electromagnetic Dominance,* 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, Journal of Electromagnetic Dominance
c/o Association of Old Crows
1001 N. Fairfax St., Suite 300
Alexandria, VA 22314

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

JED Sales Offices

NAYLOR ASSOCIATION SOLUTIONS
1430 Spring Hill Road, 6th Floor
McLean, VA 22102
Tel (800) 369-6220
www.naylor.com

Project Manager:
Kira Krewson
Direct: +1 (770) 810-6982
kkrewson@naylor.com

Project Coordinator:
Alexandra Lewis
Direct: +1 (352) 333-3409
alewis@naylor.com

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

Robert Shafer
Direct: +1 (770) 810-6986
rshafer@naylor.com

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

NAYLOR (Canada) Inc.
200 – 1200 Portage Ave.
Winnipeg, MB R3G OT5 Canada
Toll Free (US): (800) 665-2456
Fax: +1 (204) 947-2047

Index of Advertisers

JED QuickLook


ApisSys
Direct sampling up to X-Band
AV Series
OpenVPX
"The Partner for Your Solution"
Visit us at
AOC Europe Montpellier 2022,
booth B12
The Leading Provider of High Speed Data
Conversion and Signal Processing Solutions
ApisSys
www.apissys.com