SEPTEMBER 2019
Vol. 42, No. 9

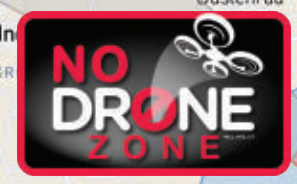
ASSOCIATION OF OLD CROWS

JED

www.crows.org

The Journal of Electronic Defense

Counter-UAS In Europe



Also in this issue:

- The DOD's Vision for EMBM
- Monitor: DARPA's Electronics Renaissance
- The EM Domain is an Integrated Domain

STRENGTH ACROSS THE SPECTRUM

ELECTRONIC WARFARE

Raytheon's modular EW capabilities demonstrate our proven ability to innovate and rapidly field effects that help ensure special mission success.

RAYTHEON.COM/SPECTRUM

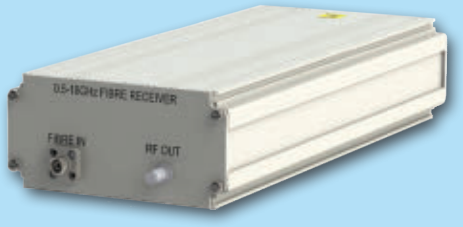
Raytheon

New for 2019

RWR Tester

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

RF Photonic Link



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

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

EWST | Ultra ELECTRONICS

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

ASSOCIATION of OLD CROWS
www.crows.org
September 2019 • Volume 42, Issue 9
JED
The Journal of Electronic Defense

A British Army AW159 Wildcat scout helicopter lifts off during Spring Storm 19, Estonia's largest annual military exercise, which took place from April 28 to May 10. Roughly 9,000 soldiers from Estonia, other NATO Allies and partner nations gathered near the town of Jõhvi, Estonia to participate in the exercise. NATO

News

Features

Departments

COVER PHOTOS COURTESY OF WITOLD WASCHUT, GABRIEL GARCIA MARENGO, RENÉ JACOBS, DON MCCULLOUGH, USAF AND DENNIS JARVIS

MAKE THE FIRST MOVE

NAVAL ELECTRONIC WARFARE SUITE

ALL-IN-ONE EW SUITE WITH ESM/ECM/SELF-PROTECTION ELEMENTS
CAPABILITY TO PERFORM SIGINT OPERATIONS
ENTIRELY SOLID STATE TECHNOLOGY
OFFLINE DATA ANALYSIS TOOLS

www.aselsan.com / aselsan

WHY DO WE WAIT?

This month's issue features an interesting cover story from Andrew White about counter-unmanned aerial system (C-UAS) developments in Europe. *JED* first wrote about C-UAS in October 2015 ("Going Small: Jamming the Mini-Drones") after noticing quite a few vendors at DSEI that year who were offering C-UAS solutions. What caught our attention was that industry had noticed the proliferation of mini-drones (by 2015, it seemed like just about every kid wanted one for their birthday), and it was anticipating that demand for C-UAS solutions would grow. Despite the proliferation of the drones and the growing number of C-UAS solutions, demand for C-UAS was still sluggish relative to the threat. Government leaders (at all levels of government) weren't willing to anticipate the problem.

What really stimulated the C-UAS market in Europe, however, was the drone incident at Gatwick Airport last December. Over a three-day period, 1,000 flights were disrupted because of drone activity detected near the airport. Afterward, the UK and other governments across the world became more serious about protecting the air space around their airports and the C-UAS market really heated up as a result.

Why was the C-UAS market stimulated by an event rather than a trend? As I mentioned, commercial mini-drones had been proliferating in the UK and just about every other country for several years before the Gatwick incident occurred. With millions of unlicensed drone users spread throughout the world, the collision between drones and airports was inevitable. Yet authorities and government leaders did not take the drone problem seriously and begin procuring C-UAS systems in large numbers until a major airport was shut down for several days. Why did they wait? The financial cost of procuring and operating a relatively small number of counter UAS systems to protect its major airports was far less expensive for the UK than the economic and political costs of disrupting 1,000 flights at Gatwick. The cost of the mini-drone that caused all the disruption was probably somewhere between $500 and $1,500.

In the military EW market, governments and military forces react to threats in two phases. When Russia, China or Iran begins to develop a new threat radar, for example, this usually stimulates a corresponding development in EW technologies to counter that threat. Yet it is only when this new threat becomes operational and maybe proliferates to other countries that military and political leaders transition their EW technology development into EW system procurement. They wait, even at the risk (and cost) of playing "catch up" if the threat proliferates quicker than we anticipated. The question remains, why do we wait and put ourselves in a reactive mode when the cost of doing this is so high? How can we get better at matching the pace of the threat, especially those threats that exploit fast-paced commercial technology? Our EW solutions cannot remain competitive against new threats if we develop great EW capabilities but they arrive too late to be useful. So, how should we adapt? – *J. Knowles*

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

SEPTEMBER 2019 • VOL. 42, NO. 9

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

COVER PHOTOS COURTESY OF WITOLD WASCHUT, GABRIEL GARCIA MARENGO, RENÉ JACOBS, DON MCCULLOUGH, USAF AND DENNIS JARVIS.

PUBLISHED AUGUST 2019/JED-M0919/4574

SM200A

Spectrum Analyzer

AVAILABLE FOR
$11,900
US RETAIL
Includes Software

High-performing, low-cost RF analyzers. Spectrum analyzer software and flexible low-level API included in the cost of the device. Powerful analysis modules continually added at no cost, and continual free software updates – it's time to break away and try a Signal Hound.

- *100 kHz to 20 GHZ range*
- *Sub-octave preselector, 20 MHz to 20 GHz*
- *160 MHz of instantaneous bandwidth*
- *1 THz sweep speed*
- *110 dB of dynamic range*

30-day money-back guarantee | 2-year warranty | Rental options

Signal Hound

SignalHound.com

Made in the USA

SEPTEMBER

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

8th Annual AOC Pacific Conference
September 9-12
Honolulu, HI
Arthur.N.Tulak.ctr@pacom.mil

SPIE Security+Defence
September 9-12
Strasbourg, France
www.spie.org

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

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

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

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

Kittyhawk Week 2019
September 25-26
Dayton, OH
www.kittyhawkaoc.org

European Microwave Week 2019
September 29 – October 4
Paris, France
www.eumwa.org

OCTOBER

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

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

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

Precision Strike Symposium
October 22-24
Laurel, MD
www.precisionstrike.org

56th Annual AOC International Symposium and Convention
October 28-30
Washington, DC
www.crows.org

NOVEMBER

Electronic Warfare South Africa (EWSA 2019)
November 4-6
Pretoria, South Africa
www.aardvarkaoc.co.za

MILCOM 2018
November 12-14
Norfolk, VA
www.milcom.org

Dubai Airshow 2019
November 17-21
Dubai, UAE
www.dubaiairshow.aero

DSEI Japan
November 18-20
Tokyo, Japan
www.dsei-japan.com

Defence & Security 2019
November 18-21
Bangkok, Thailand
www.pandci.com

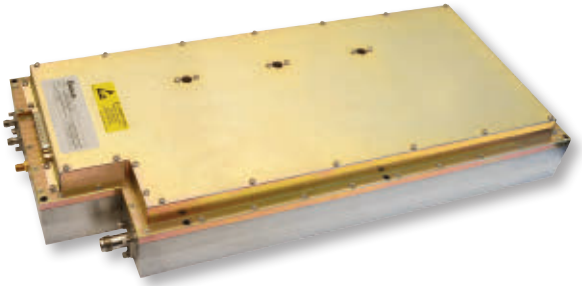
AOC conferences are noted in red. For more info or to register, visit www.crows.org. Items in blue denote AOC Chapter events.

Above and Beyond

Our newest low voltage, integration friendly, solid state HPA's have more benefits to offer over TWT's and MPM's.

Model BME69189-100
6-18 GHz, 100 Watts
Solid State Power Amplifier Module

- Full Power Across the Entire Bandwith
- Maintains Output Power, Gain, and Efficiency with Real World Load Conditions
- Superior Harmonics *and* Low Noise Floor
- Compact, Lightweight, and Usable in the Harshest Environments
- 28 VDC GaN Technology
- High Speed Blanking
- Operating Temperature: -40° C to 55° C
- Also Available in 20 & 50 Watts



Model BME2969-200
2–6GHz, 200 Watts
Solid State Power Amplifier Module

- High Efficiency Over the Entire Bandwidth
- RF Input/Output Sample Ports
- Internal DC to DC Converters
- External T/R Switch Available
- Maintains Output Power with Real-World Load Conditions
- Operating Temperature: -40° C to 55° C
- Also Available in 100 & 300 Watts

Contact our sales & marketing department today to discuss your exact project needs.

Comtech...*meeting needs, exceeding expectations.*

COMTECH POWER SYSTEMS TECHNOLOGY™

Comtech PST • 105 Baylis Road, Melville, NY 11747
Tel: (631) 777-8900 • Fax: (631) 777-8877 • www.comtechpst.com • sales@comtechpst.com

Control Components Division • 417 Boston Street, Topsfield, MA 01983
Tel: (978) 887-5754 • Fax: (978) 887-7244 • www.comtechpst.com/hill • sales@hilleng.com

SEPTEMBER

AOC Live Professional Development Web Course: Space EW
September 4-20
8 sessions, 1300-1600 EDT
www.crows.org

AOC Virtual Series Webinar: Introduction to Machine Learning for EW
September 5
1400-1500 ET
www.crows.org

Radar Fundamentals
September 9-11
Canberra, Australia
www.unsw.adfa.edu.au

Fundamentals of Radar Signal Processing
September 9-12
Winter Garden, FL
www.pe.gatech.edu

Digital Radio Frequency Memory (DRFM) Technology
September 10-13
Atlanta, GA
www.pe.gatech.edu

Signals Intelligence Fundamentals
September 17-18
Winter Garden, FL
www.pe.gatech.edu

Basic EO-IR Concepts
September 17-19
Winter Garden, FL
www.pe.gatech.edu

Introduction to Open Systems Architecting Solutions for Decision Makers
September 18
Atlanta, GA
www.pe.gatech.edu

AOC Virtual Series Webinar: Achieving SWAP-C Benefits in EW Systems using Positive Gain Slope MMIC Amplifiers
September 19
1400-1500 ET
www.crows.org

Software-Defined Radio Development with GNU Radio: Theory and Application
September 24-27
Atlanta, GA
www.pe.gatech.edu

OCTOBER

AOC Virtual Series Webinar: RAF 100 Group and its EW Legacy
October 3
1400-1500 EDT
www.crows.org

AOC Live Professional Development Web Course: The World of Airborne Expendables & Small Unmanned Aircraft Systems (sUAS)
October 8-17
4 sessions, 1300-1600 EDT
www.crows.org

Radar Principles
October 14-18
Swindon, UK
www.cranfield.ac.uk

NATO Joint Electronic Warfare Course
October 21-25
Oberammergau, Germany
www.natoschool.nato.int

AOC Live Course: Fundamental Principles of Electronic Warfare
October 26-27
0800-1700 EDT
www.crows.org

AOC Live Course: Machine Learning for EW
October 26-27
0900-1700 EDT
www.crows.org

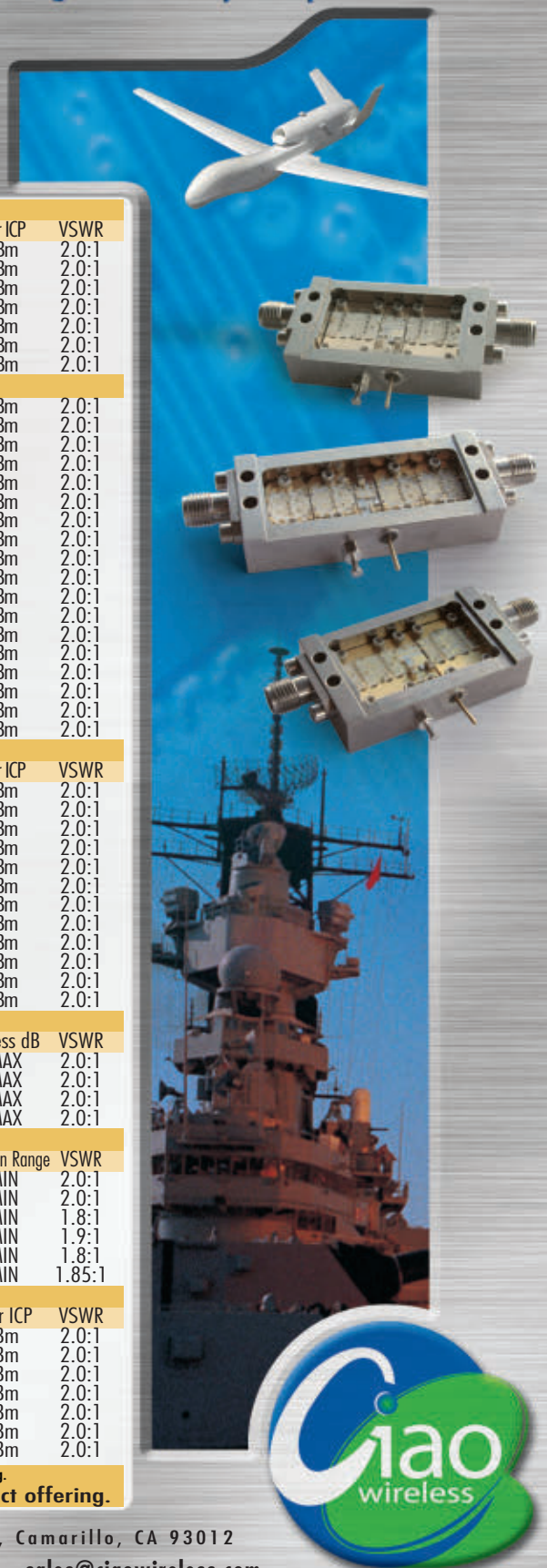
AOC courses are noted in red. For more info or to register, visit www.crows.org. Items in blue denote AOC Chapter courses.

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

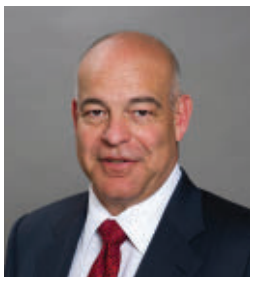
Model No.	Freq (GHz)	Gain (dB) MIN	Noise Figure dB	Power-out @ P1-dB	3rd Order ICP	VSWR
CA001-2110	0.01-0.10	18	4.0 MAX, 2.2 TYP	+10 MIN	+20 dBm	2.0:1
CA001-2211	0.04-0.15	24	3.5 MAX, 2.2 TYP	+13 MIN	+23 dBm	2.0:1
CA001-2215	0.04-0.15	23	4.0 MAX, 2.2 TYP	+23 MIN	+33 dBm	2.0:1
CA001-3113	0.01-1.0	28	4.0 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, Inc. 4000 Via Pescador, Camarillo, CA 93012

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



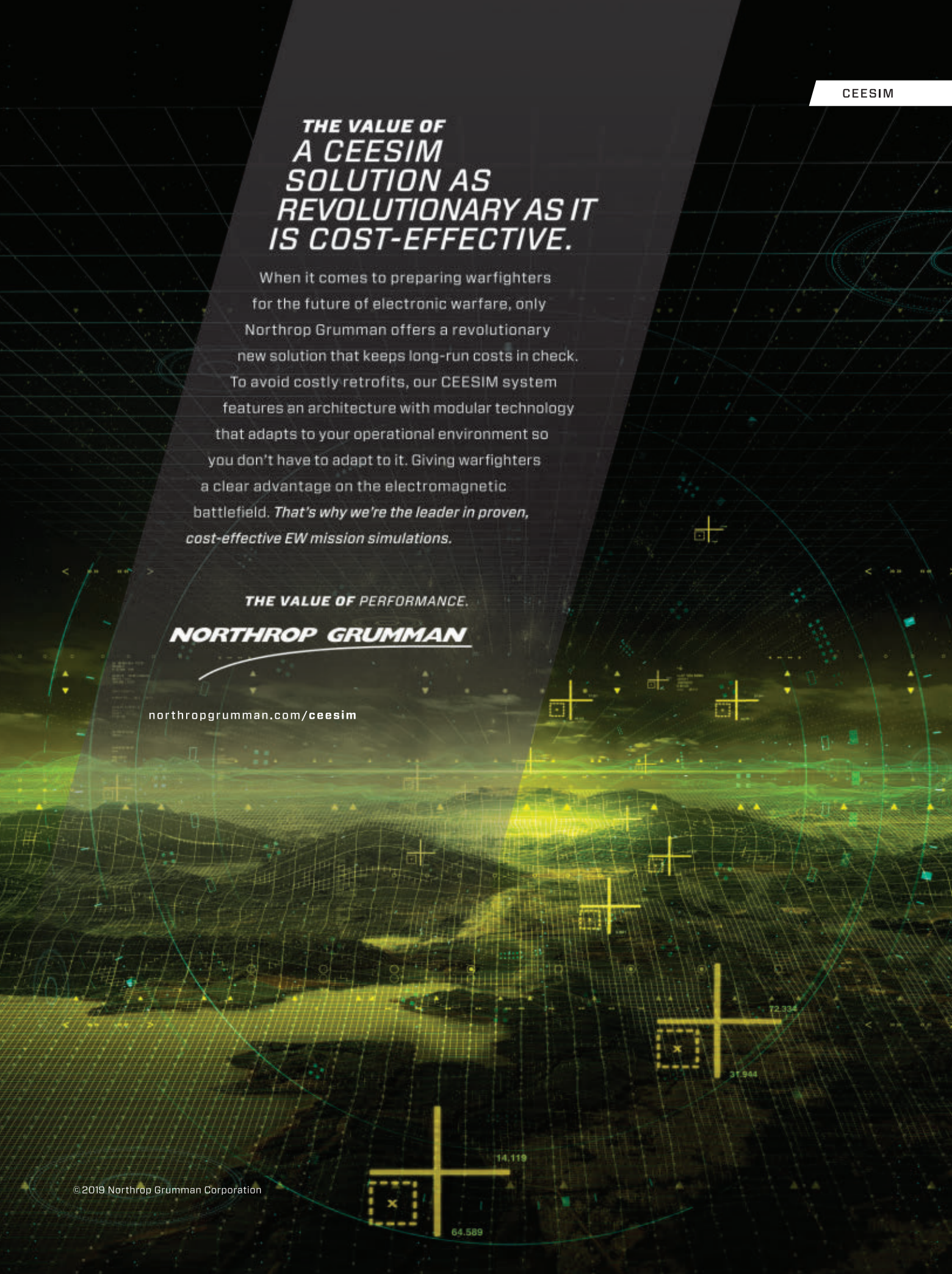
THE EM OODA LOOP

Working at the Joint Improvised Explosive Device Defeat Office (JIEDDO) for eight years beginning in 2006, I learned the meaning of "contested and congested" Electromagnetic Environment (EME) first-hand. We built approximately 35,000 RCIED jammers, deployed them to theater and then experienced the collision in the EME caused by insufficient spectrum management, spectrum management tools, non-compatible systems and intel loss-gain decisions, just to name a few. As we were establishing an EW Coordination Cell (EWCC) for CENTCOM at the Combined Air Operations Center (CAOC), you could walk on the floor of the CAOC and see the screens with a complete picture of the air campaign. We had nothing that came close to that for the electromagnetic battle (primarily Blue on Blue) that was taking place. What emitters were radiating, where they were, who they were?

You can take that simplistic environment based on our CREW systems, EA-6Bs and Compass Call, where no real Red EW and Cyber threat was directed against us, and compare it to today's environment. We now face peer and near-peer competitors in the EME who command organized and well-equipped EW and Cyber forces. Consider the number of emitters and the mix of systems that have "EW" capabilities in a Joint or Coalition environment, add to that the enemy's command and control structure and their dedicated EW and Cyber assets focused on denying, disrupting and deceiving our operations. How do we sense and project what is happening in the EME in real time or near real time? How do we ID and precision locate emitters, and, just as important, how do we de-conflict and put the best asset on the target at the right time?

We currently have weaknesses in the observe phase, orient phase, decide phase and act phase of the OODA Loop. One of the most pressing deficiencies in recent joint operations has been trying to achieve coordinated and cohesive operations within the EME. DOD, the COCOMs and Coalition Partners are recognizing the EME as a maneuver space, and they are beginning to aggressively pursue solutions for Electromagnetic Battle Management (EMBM). Building an effective EMBM capability will require changes across DOTMLPF to mitigate this capability gap and coordinate with coalition partners to enable the collection and sharing of data in a timely manner.

Technology development and training environments are essential to successful development of EMBM capabilities and bolstering our EM OODA Loop. Sensor integration, prioritization and data fusion will form the underlying baseline for EM awareness and asset availability (observe). Large data correlation and filtering, supported by machine learning, will provide higher fidelity situational awareness (orient). Technology advancements in Artificial Intelligence will provide robust, autonomous decision making. Finally, technology advancements in resilient command and control will enable EM systems to pace and negate the threat (act). EMBM will be the key contributor to achieving strategic advantage in future conflicts, and I hope you enjoy the article, "DOD's Broad Vision for Electromagnetic Battle Management," on page 36. – *Muddy Watters*



THE VALUE OF A CEESIM SOLUTION AS REVOLUTIONARY AS IT IS COST-EFFECTIVE.

When it comes to preparing warfighters for the future of electronic warfare, only Northrop Grumman offers a revolutionary new solution that keeps long-run costs in check. To avoid costly retrofits, our CEESIM system features an architecture with modular technology that adapts to your operational environment so you don't have to adapt to it. Giving warfighters a clear advantage on the electromagnetic battlefield. *That's why we're the leader in proven, cost-effective EW mission simulations.*

THE VALUE OF *PERFORMANCE.*

NORTHROP GRUMMAN

northropgrumman.com/**ceesim**

Ministry of Defence
Thailand

Defense & Security 2019

18 - 21 November 2019

IMPACT Exhibition and Convention Center
Bangkok, Thailand

Tri-Service Asian Defense & Security Exhibition
Conference and Networking Event

Held in Conjunction with:
ADMM
ASEAN Defence Ministers' Meeting

For more information please contact:
Ms. Yaowalak Chuvichien, Senior Sales Manager
+66 (0) 2036 0500 ext 212 Yaowalak@asiandefense.com

Official Publication:
Official Show Daily:
ADJ

Official Bilingual Show Daily:
ARMADA INTERNATIONAL
ASIAN MILITARY REVIEW

Official Exclusive Media Partner:
GBP AEROSPACE DEFENCE

Supporting Publications:
MILITARY TECHNOLOGY, DEFENCE REVIEW ASIA, JED, KANWA ASIAN DEFENCE, DEFENSE, SHEPHARD, ARMS JOURNAL, Jane's By IHS Markit, AVIATION & MILITARY NEWS, DSA, DEFENCE, European Security & Defence, NEW DEFENCE ORDER, AVIATION WEEK

Strategic Partner:
USA 2020 17th DEFENCE SERVICES ASIA EXHIBITION & CONFERENCE SINCE 1988
NATSEC ASIA 2020
20 - 23 APRIL 2020
KUALA LUMPUR, MALAYSIA

Officially Supported by:
TCEB

Organised by:
GML

+66 (0) 2036 0500 info@asiandefense.com @DefenseThailand #DefenseThailand2019

www.asiandefense.com

the monitor news

DARPA'S ELECTRONICS RESURGENCE INITIATIVE SETS GENERATIONAL GOALS FOR MICROELECTRONICS INDUSTRY

The Defense Advanced Projects Agency (DARPA) held its second Electronics Resurgence Initiative (ERI) Summit from July 15-17 in Detroit, MI. To define the purpose of the Summit and the mission of the ERI, Dr. Mark Rosker, newly appointed Director of DARPA's Microsystems Technology Office (MTO), opened the event by quoting Dr. George Heilmeier, who at the time of the quote in 1984 was the Chief Technology Officer of Texas Instruments (Dallas, TX), and had been a former and highly-regarded director of DARPA. "The startling rate of change that microelectronics is creating in world societies has caused organizations to ponder how long this rate of change can endure and at what level of performance it might end."

Rosker elaborated that Heilmeier was concerned about what he called "the stagnation of innovation," and, in particular, its impact on the US defense strategy. "Using superior weapon performance to offset the numerical advantages of potential enemies could lose much of its validity."

Today, says Rusker, the stakes are even higher, as many worry that we're approaching the end of microelectronics innovation, especially in the US. At DARPA, however, Rusker says "We disagree. In fact we believe that we stand at the beginning of a new wave of innovation in microelectronics and that is why we are here today."

Reflecting on Gordon Moore's 1965 "law" that the number of components per integrated circuit seems to double at a constant rate – in fact, annually – Rosker observes that "this progress has actually been sustained through a series of 'waves' of technological progress, each one building upon those that preceded it." He also noted that "in each one of these waves, DARPA has played a key role in working with the commercial semiconductor industry to tackle the hard problems threatening to derail progress in technological innovation."

Rosker says that today we've reached the 4th wave in this process where we face new challenges that must be overcome if we wish to avoid the stagnation of innovation that Heilmeier warned of. These challenges include "finding new ways, other than physical device scaling, to drive circuit performance to higher and higher levels; overcoming the skyrocketing cost of IC design, which will limit innovation to the dwindling few that can afford it; and addressing the explosion in data being digitized and moved onto and off of chips which leads to latency, cost and enormous complexity in system design." In addition, Rosker emphasized the criticality of "safeguarding the accessibility and security of our microelectronic supply lines, which has become an imperative both to industry and to government."

The innovations ERI is championing for the 4th wave, says Rosker, lie in four areas: New Materials for Devices – "ERI is developing new concepts in semiconductor devices physics that go beyond traditional silicon CMOS to achieve higher levels of performance in both computation and memory, that offer advantages to silicon as well as approaches that can be combined with and complement current technologies;" Specialized Functions – "ERI is supporting a shift away from generalized von Neuman computing to new approaches to achieve circuits that are highly optimized for performance for specific kinds of tasks, including a focus on hardware implementations of artificial intelligence (AI);" Design and security – "ERI is enabling the next generation of automated design (EDA) tools to exploit the power of specialization in new and more complex architectures. In addition we are providing tools to build security into the design process;" 3D Heterogeneous Integration – "The 4th wave and ERI will exploit the third dimension in electronics to make a shift from coarse board-level and chip-level integration to much finer, higher density, more-interconnected microsystems that are composed of heterogeneous elements. This involves the development of new assembly methods, interconnect technologies as well as overcoming associated challenges such as thermal management."

Throughout the three-day conference, senior speakers from government, academia and industry gave presentations on the progress, accomplishments and promise of many of the technology initiatives already being pursued or planned as part of the 4th wave of innovation. One overarching message that became clear from learning about this widely diverse range of work covering incremental improvements to revolutionary new approaches and innovations was that choices are going to have to be made.

From an industry perspective, Dr. Lisa Su, CEO of AMD (Santa Clara, CA)

directed her discussion toward high-performance computing applications, noting that "when you're goal is to push the envelope of technology, you often have to make bets ahead of what you know will actually happen. In the semiconductor industry, those bets often have to be made five years, or even ten years or more in advance, when you're really thinking about the next wave of computing. When you're talking about the use of things like advanced triplets or heterogeneous technologies, those bets have to be made many, many years in advance."

Another, perhaps obvious, message from the conference was that commercial applications and the specific processing demands of those applications will necessarily drive much of this decision making. As a result and, in fact, the whole reason behind the ERI in the first place, is that the DOD through DARPA must find the best ways to anticipate, help direct, and leverage those decisions and innovations toward its own unique needs.

Dr. Lisa Porter, Deputy Under Secretary of Defense for Research & Engineering, began her presentation by stating just that, "Microelectronics are absolutely fundamental to essentially every technology and capability in the DOD." Referencing next-generation cellular technology (5G), Porter observed that "5G is not just a mere extension of 4G and in fact it ultimately will not look very much like 4G at all. 5G is all about ubiquitous connectivity, which means a transition from discrete to fully-distributed computation, communications, and data curation and management." Noting that this will demand dramatic advancements in microelectronics technology, Porter also pointed out that "the DOD's own IoT (Internet of Things) applications and machine learning inference engines at the edge will also demand leading edge technology to meet very stringent power and performance requirements, and we at the DOD cannot afford to be shut out of those capabilities and more."

Porter also emphasized, however, that "we can't just focus on performance improvements, we must now focus on security as well, and IoT, 5G, and distributed interconnected devices in general present significant security challenges." To achieve both objectives she says "we must develop data-driven security techniques and protocols that are complementary to advanced commercial flows." – *J. Haystead*

ALIGNING COMMERCIAL INNOVATION WITH DARPA'S NEEDS AND DESIRES

One of the takeaways from DARPA's Electronics Resurgence Initiative (ERI)

US ARMY STTR SOLICITATION TO FOCUS ON EMS-RELATED EFFORTS

The US Army announced that it will list seven topics as part of the DoD Small Business Technology Transfer (STTR) 19.C Broad Agency Announcement (BAA). Most of the research topics address operations in the EM Domain.

The Intrinsically Interference- and Jamming-Resistant High Frequency (HF) Radios project (Topic A19C-T001). The goal of the topic is to develop HF radio receivers based on recent technical developments in areas such as GaN low-noise amplifiers; high resolution analog-to-digital converters; and digital-signal-processing (DSP) and mixed signal techniques employing machine learning and artificial intelligence for signal filtering with extremely low signal-to-noise ratio. The aim is to achieve uninterrupted operation under high power interference and jamming attacks.

The Tactical Edge Sensor Processing project (Topic A19C-T004) seeks to develop "…efficient sensor edge processing in the Internet Battlefield of Things (IBoT). Data from these devices should be processed and interpreted locally over hardware systems in extremely small form factors in terms of size, memory and power." Potential applications include autonomous cyber recognition, target recognition and electromagnetic spectrum awareness.

The objective of the Adaptable Tactical Communications effort (Topic A19C-T005) is to enable optimal operation regimes for tactical radios in contested spectrum conditions. The system will "use information such as terrain data, data from sensors, and network management records to identify the occurrence and the principal cause of network impairments [i.e., jamming and interference] using machine learning techniques. Then, using dynamic adaptation techniques for making optimal decisions, such as reinforcement learning, the system should identify the optimal course of action for the user."

Finally, the Electronic Standoff Denial project (Topic A19C-T007) seeks to "develop a directed energy system capable of disrupting, disabling or destroying the electronics on a remote target within milliseconds of detection." This effort seeks to develop laser solutions solutions that "eliminate threats through the disruption of a target's electronic control systems rather than destroying the target by directing enormous amounts of power onto it as quickly as possible. For example, the coupling between electromagnetic radiation and electrons in solids suggests that short, high-intensity laser pulses rather than high-energy continuous wave lasers or microwaves may provide this alternative solution. Even without reaching the electronics directly, the interaction between a laser pulse and a material can generate broadband radiation that may disrupt nearby electronics… Any DE system able to remotely disrupt naturally packaged electronics in a realistic target in less than a few milliseconds is of interest, especially if the solution may be scaled to neutralize targets more than 1 km away." Army STTR program officials plan to hold an Industry Day at the University of North Carolina (Chapel Hill, NC) in September (a date had not been set when this issue of JED went to press). The point of contact is M. John Smith, e-mail usarmy.rtp.ccdc-arl.mbx.sttr-pmo@mail.mil. – *JED Staff*

Summit held in Detroit last month (see accompanying story – "DARPA's Electronics Resurgence Initiative Sets Generational Goals for Microelectronics Industry.") is that both the commercial semiconductor industry and the DOD must work very hard and very closely together in order to make future generation semiconductor technology suitable and compatible with each segment's requirements. It's also clear that this will be no easy task.

A number of commercial applications and markets will play a role in determining the direction of future innovation, but none more so than the emergence of 5G mobile technology and associated AI applications and features requirements. As described by Mr. Steve Mollenkopf, CEO, Qualcomm Inc. (San Diego, CA), "Due to its scale and particularly with 5G increasingly growing the amount of data it's processing, as well as the nature of what needs to be done, and where it needs to be done, 5G will tend to pull architectures in its direction."

This obviously has ramifications for the DOD and the role of DARPA going forward. Says Mollenkopf, "What we've seen in the semiconductor industry from the foundry perspective is that mobile tends to set the direction for the semiconductor industry, in terms of what node you're using, who is going to the node first, and even the structure of the foundry industry itself, including the design of transistors. This will probably never change."

Mollenkopf also sees mobile devices becoming the most pervasive AI platforms. "Among future trends, the mobile industry will increasingly need to focus on more and specific AI engines to allow you to make decisions on the data right where the data is. In terms of 5G and AI, 5G will allow a number of new industries to really make use of cellular technology for the first time, and it also means that the future of AI will really be determined by the coupling of AI and 5G together. In the future, what you're going to see is a lot of these heterogeneous engines being applied to AI, but you have to have 5G right next to it." he says.

One particularly interesting point made by Mollenkopf is that, "With 5G, the RF guys are really back in charge. Because we have basically reached the Shannon limit (the theoretical maximum information transfer rate of a communication channel, for a particular noise level), on everything else, the only way to get additional gains is to have some really awesome antennas and use them exactly right." Mollenkopf credits DARPA's work in this area which has "really benefitted us in terms of making this possible."

One particular ramification of this increased reliance on antenna technology, says Mollenkopf, is that "these smart antennas require a lot of processing to manage, and that processing has to be done in real time and directly at the antenna. So it's another ramification of how mobile is pulling computing and the semiconductor industry toward its unique requirements."

Another point is that, "Not all data will go to a processing cloud, and we'll see a lot of processing done at the wire-

less edge. This will require cloud players and device manufacturers to coordinate how to architect how big data and AI work. Factors like, low-power requirements, lower latency demands, privacy issues, on-device security and less bandwidth, will all need to be architected in chips, and this means that the transition to this mobile design point of AI will require the design architecture of the engines that perform the AI to change, with power and thermal efficiency being major considerations." Ultimately, Mollenkopf doesn't see there being any one-size-fits-all solution, at least at the device level, with more specialized AI engines for specific classes of applications or sets of data. As a result, he expects to see partnerships, collaborations, and joint development efforts forming over the long term to address these issues.

As pointed out by Qualcomm's Mollenkopf, foundries will also have a large role in the specific directions of future innovation as well. But, says Dr. Thomas Caulfield, CEO, Global Foundries (Santa Clara, CA), "As a foundry we have a little bit of a different perspective on where things are going. "

Noting that they serve a broad range of customers and market segments together with a broad range of technologies, Caulfield says their approach is to develop solutions not only at the node platform level, but to create feature-rich solutions around those nodes.

To accomplish this, as described by Caulfied, "Last August, we called a 'pivot' – where instead of continuing to chase leading-edge technology, along the lines of a strict interpretation of Moore's law, we would focus on achieving additional advances through other approaches, such as embedding different functionality and creating the ability to make systems-on-chip."

Caulfield says the new business model was adopted in recognition of the fact that, "even at our scale, we could no longer afford to spend $3 billion per year on R&D and $10 billion in capital expenditures to enable enough scale and volume at the leading edge. Instead, we chose to have a business strategy that was consistent with our scale and industry realities. We redefined technology leadership and differentiation. It doesn't have to be smaller features and faster devices, it can also be integration of a feature rich capability, through such approaches as multiple chiplets integrated onto a common substrate with advanced connectivity."

Referencing that the percentage of the total market at the leading edge (< 12 nm today is 20% and, while this is expected to grow, is still only projected to be at 25% in 2022), Caulfield says, "We chose to participate more broadly in the larger, more attractive market segments."

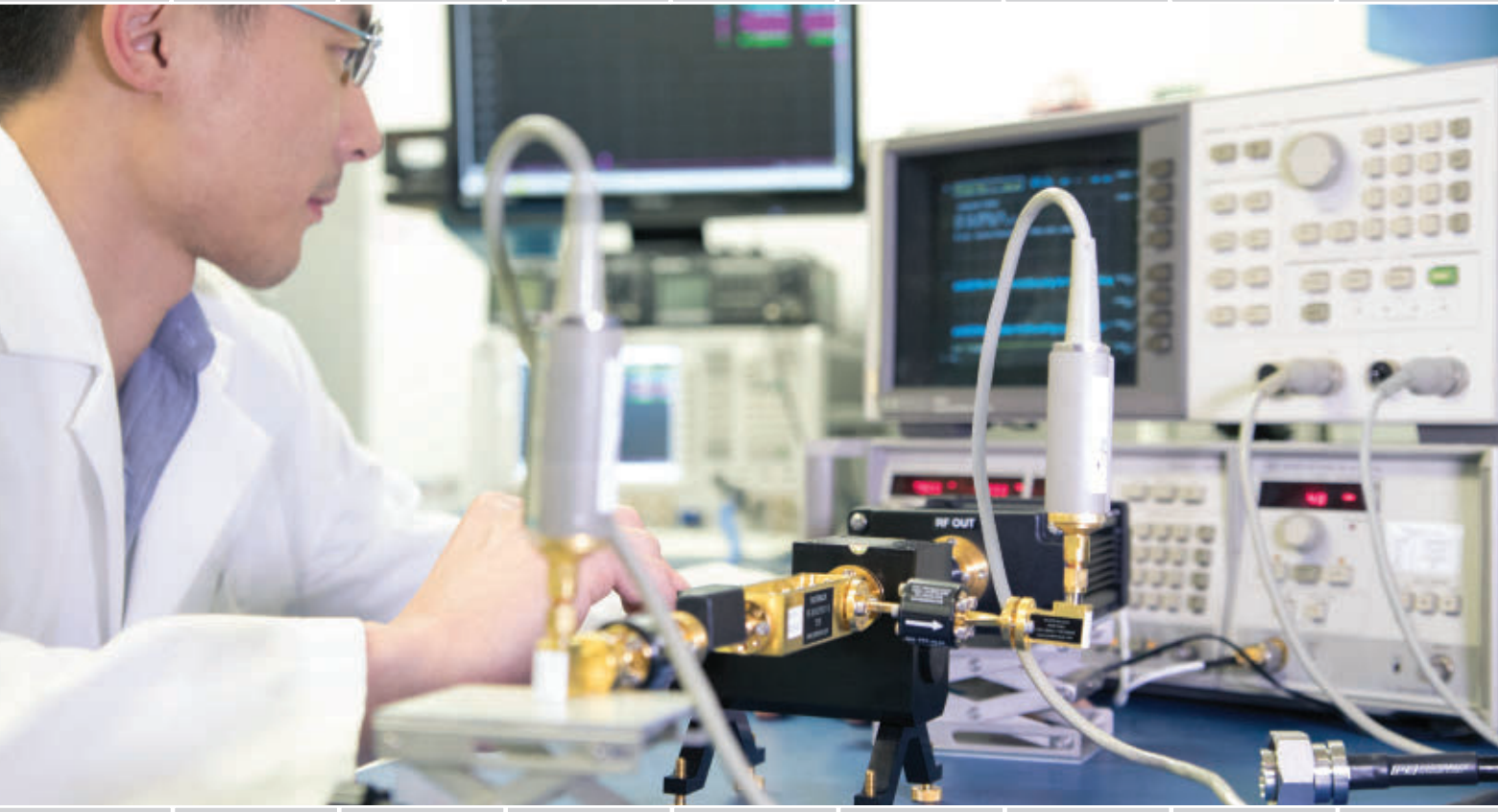
In terms of how their approach will relate to meeting future DOD requirements, Caulfield says that Global Foundries is very much aligning itself with DARPA's three ERI pillars – materials and integration; architectures; and designs. "In the materials and integration area, a key element is to use memory as a 'compute accelerator.' In terms of architecture, the key is to recognize that locality matters more than processing power and will be critical to achieving the performance required for the demands of AI applications of the future. In the final, design pillar, the driving point is that AI-at-the-edge has to be adaptable for both hardware and software." Observing that today there are essentially only five players remaining in the independent foundry sector in the world, Caulfield concluded by stating that, "We're looking forward to future programs and partnerships with DARPA." – *J. Haystead*

IN BRIEF

The US Air Force's **53rd EW Group, 36th Electronic Warfare Squadron,** has issued a Request for Information (RFI) for their upcoming Rapid Acquisition of RF Threat Simulator (RATS) effort. Under the RATS procurement, the 36th EWS wants to buy a "near commercial of the shelf" solution suitable for ALR69A digital RWR mission data testing, as well as testing the ALQ-213 EW Management System. The simulator will be installed at a laboratory facility being designed for the 36th EWS at Eglin AFB, FL. The contracting point of contact is Craig L. O-Neil, (850) 882-5070, e-mail craig.oneill.2@us.af.mil.

The Army Rapid Capabilities and Critical Technologies Office (RCCTO) is hosting an Innovation Day in McLean, VA, on September 17 to quickly target and acquire promising new technology – identifying solutions that could be in the hands of soldiers within a 1- to 3-year timeframe. Among the areas of focus is an advanced tactical SIGINT system featuring advanced wideband antennas, GP/GPU based ruggedized server hardware and artificial intelligence/machine learning based microservice capability modules. Another area of interest is "JEMSO/EW – Spectrum awareness, visualization, understanding to inform operational planning and execution." This effort aims for the "prototype and establishment of an intuitive sensing grid that delivers cooperative sensor operations across the depth and breadth of the Multi-Domain Operations battlespace. The integrated sensor architecture is built upon common, open standards, is managed by the MDC2 integrated tasking order (ITO) process based on collection and targeting requirements of collective C2 nodes." In the counter-UAS area of interest, the RCCTO seeks "innovative approaches to detect, Identify, Track, Engage and Defeat small UAS or a swarm of small UASs." Engagement mechanisms can utilize directed energy or kinetic effectors. Another project is "Multi-Domain Task Force Capabilities to Counter A2/AD – (EW, Space, Cyber, LRPF, New Kill Chains)," which could include EW, space-based capabilities, offensive and defensive cyber capabilities and new approaches to long-range precision fires and their kill chains. In the area of tactical cyber, the RCCTO is seeking "a cyber solution that provides the capabilities to deny, degrade, disrupt, destroy, and manipulate electronics (e.g., through the means of sensing and emitting Radio Frequency (RF) signals). Capabilities should provide the means to rapidly deliver lightweight (small packet size) effects in a tactical environment." The contracting point of contact is Paul Kemp, (703) 545-8224, e-mail paul.a.kemp5.cov@mail.mil.

You Engineer the Future.
We'll Supply the Components... Today!



Largest Selection ✓ Same-Day Shipping ✓ Expert Technical Support ✓

Armed with the world's largest selection of in-stock, ready to ship RF components, and the brains to back them up, Pasternack Applications Engineers stand ready to troubleshoot your technical issues and think creatively to deliver solutions for all your RF project needs. Whether you've hit a design snag, you're looking for a hard to find part or simply need it by tomorrow, our Applications Engineers are at your service. Call or visit us at pasternack.com to learn more.

866.727.8376
Pasternack.com

PASTERNACK
an INFINITE brand

world report

UK STARTS SEARCH FOR FUTURE EWCM SOLUTIONS

Industry has been asked by the UK Ministry of Defence (MOD) to provide information on electronic countermeasures systems and technologies that could potentially meet the Royal Navy's (RN's) needs for future soft-kill anti-ship missile defense.

Established as the second component of the overarching Maritime Electronic Warfare Programme (MEWP), the so-called Electronic Warfare Counter Measures (EWCM) project is investigating trainable launcher systems, off-board delivery mechanisms/vehicles and electronic payloads.

In a request for information (RFI) released in early July, the Maritime Combat Systems team within the MoD's Defence Equipment and Support (DE&S) organization advised that its market research was seeking "to gain a better understanding of the current marketplace and level of technology maturity," adding, "This RFI encompasses Technology Readiness Levels (TRLs) of TRL 5 and above and is primarily interested in commercial and military off-the-shelf (COTS/MOTS) trainable decoy launchers available now or the very near future." In addition, DE&S said it was also interested in "potential maritime off-board active decoy technologies (TRL 3 and above) for delivery vehicles expendables/unmanned air systems [UASs] and electronic payloads as a system."

As part of its market research, DE&S has advised its desire to view potential launcher solutions and, subsequently, potential active off-board decoy technologies (expendables, UAS and payloads). This engagement activity is planned to conclude toward the end of November 2019.

The MEWP program is looking to recapitalize the RN's shipborne EW capabilities in two phases. The first phase, known as the Maritime Electronic Warfare System Integrated Capability (MEWSIC), is planned to deliver improvements in electronic surveillance, EW command and control, and EW operational support. EWCM, which forms the second phase, is intended to introduce a new suite of decoys and expendables. – *R. Scott*

RHEINMETALL AND MBDA TO COLLABORATE ON HIGH-ENERGY LASER FOR GERMAN NAVY CORVETTE

Rheinmetall and MBDA Deutschland are set to build a high-energy laser onboard a German Navy corvette. This marks the first time the German Navy has pursued the development of operational laser technology for one of their ships.

The two German defense contractors will partner for the construction, integration and testing of a laser demonstrator to be installed on a Braunschweig K130, Germany's latest class of corvettes.

Werner Krämer, managing director of Rheinmetall Waffe Munition GmbH, said in a press release: "We're going to be cooperating very closely to put the military potential of laser technology to work for the Bundeswehr, boosting its operational readiness and combat effectiveness…Lasers offer new tactical possibilities on land, at sea and in the air. In partnership with the German Navy, we want to press ahead with this new technology."

Peter Heilmeier, head of sales and business development at MBDA Deutschland GmbH, said, "Cooperation between Rheinmetall and MBDA will be particularly beneficial for the Bundeswehr. Both companies will be leveraging their respective special strengths to make this German Navy project a resounding success."

The production timeline and allocation of project responsibilities has not yet been announced. More information will follow from Germany's defense procurement agency, the Federal Office for Bundeswehr Equipment, Information Technology and In-Service Support. – *H. Swedeen*

BRITISH ARMY TO RE-ORGANIZE FIELD ARMY UNITS

The British Army has outlined plans to restructure the Field Army's primary formations in an effort to meet modern challenges of a constantly competitive warfighting environment. Among the changes will be the reformation of a Division 6 (6 (UK) Div) that has historically led electronic warfare (EW), information operations (IO) and cyber efforts.

Though no changes will be made to the Army's operational focus, three separate divisions of the Field Army forces will be rebalanced to improve effectiveness, including Division 1 (1 (UK) Div), Division 3 (3 (UK) Div) and 6 (UK) Div.

In describing division priorities, Lt Gen Ivan Jones CB, Commander Field Army (CFA), said, "The Field Army must build on the strong foundation of the 3rd Division's world class war-fighting force. 1st Division provides specialist soldiers and equipment to develop other nations' armies, deal with disaster and humanitarian crises worldwide and enable our war-fighting division. 6th Division focuses on Cyber, Electronic Warfare, Intelligence, Information Operations and unconventional warfare through niche capabilities such as the Specialised Infantry Battalions."

The 6 (UK) Div will include: 1st Signal Brigade, 11th Signal Brigade, 1st Intelligence Surveillance and Reconnaissance Brigade, 77th Brigade and the Specialist Infantry Group.

Jones said, "The character of warfare continues to change as the boundaries between conventional and unconventional warfare become increasingly blurred. The Army must remain adaptable and evolve as a fighting force. The three complementary British Army Divisions harness the wide range of British Army capabilities, providing choice to the Government in defense of the UK's interests." – *H. Swedeen*

The world's leading tactical airborne ELINT/ESM system

EAGLE ATES System
0.5 to 18 GHz Antenna Head Unit

EAGLE ATES System
Single 1-ATR Package Option

Ultra Electronics is pleased to announce an upgraded ALR-510 ELINT/ESM system for use on manned and unmanned aircraft, called the EAGLE Airborne Tactical ELINT/ ESM System (ATES). Flight proven and fully qualified, the EAGLE ATES has industry leading performance and has achieved significant flight hours, demonstrating its capabilities on multiple platforms.

Meet the EAGLE ATES System

- Meets or exceeds typical ELINT and ESM system performance requirements
- Flight proven on multiple platforms
- Qualified to MIL-STD-810G (Environmental), MIL-STD-704F (Power), DO-160E/G (EMI/EMC)
- World leading Instantaneous Field Of View with best in class Direction Finding accuracy
- Supports both Direction Finding and emitter polarization detection
- Single platform or multi-platform co-operative geolocation
- Designed and used with low and medium capacity datalinks
- Scalable training simulation (embedded or classroom) systems
- Expandable to deal with the emerging threat of V/UHF radar based systems

Ultra ELECTRONICS

ITAR FREE - Made in Canada

www.ultra-tcs.com

Ultra Electronics
TCS, EW Group
88 Hines Road
Ottawa, Ontario
Canada K2K 2T8
Tel: +1 613 592 2288

Counter-UAS: European EW Companies

By Andrew White

The proliferation of commercially available unmanned aerial systems (UASs) in the civil sector and their increasing employment in the military domain continues to force governments around Europe to pursue a series of counter-UAS (C-UAS) solutions and strategies to protect armed forces and critical national infrastructure.

Whether it be the employment of UASs by violent extremist organizations (VEOs) to deploy airborne improvised explosive devices (ABIEDs) in Iraq and Syria, electronic warfare (EW)-equipped UASs disrupting communications networks in eastern Europe, or "hobbyist" UASs operated by unknown persons to aggravate operations at international airports, the demand for mature, cost-effective and deployable C-UAS solutions has never been higher.

As the market continues to mature, European industry is offering up scalable solutions that can be operated in a system-of-systems approach to support armed forces, law enforcement and civil customers alike. In December 2018, for example, London Gatwick airport was closed for 33 hours following UAS activity which saw airport and government authorities drafting in multiple types of C-UAS equipment to prevent any further disruption.

As Danish C-UAS system manufacturer, MyDefence, explained in its "Protecting Airports Against Drones: How to protect airports against unauthorized use of drones" white paper, published in February 2019, "airborne collisions between drones and airplanes could introduce a significant burden to aircraft operators, not to mention a potential loss of life and additional legal liability to airlines and airport facilities."

"Technology exists, and combining different sensors in a system is considered the ultimate drone de-tection solution. Therefore, utilizing a combination of radio frequency (RF) sensors with optical sensors and/or radar would provide the most accurate overview, while also being a more expensive solution," the white paper suggested.

However, it also warned of difficulties in conducting C-UAS operations in airport and other congested and cluttered environments, such as urban areas: "Net capturing a drone is not realistic and jamming is illegal. When it comes to mitigating the threat, the only realistic thing at present is to develop a set of procedures that separate departing and landing air traffic from the rogue drones entering the protected area," the white paper concluded. Similar issues are being witnessed by armed forces seeking to integrate C-UAS technology into wider Integrated Air Defense Systems (IADS) to protect main and forward operating bases from the threat of ABIEDs through to larger surveillance and EW platforms.

Discussing some of the protective measures being undertaken in Europe, Northrop Grumman Innovation Systems (NGIS) portfolio director, Jay Annis, described the current C-UAS marketplace as "ambiguous and volatile." Highlighting the relative ease with which a lone, small and low-flying UAS could be detected on a battlefield, Annis warned how C-UAS technology would be severely challenged when threats inevitably escalate into swarms of UASs operating in already cluttered environments. "Then it starts to get really hard," Annis said, before suggesting that a "9/11" type incident would trigger significant developments in C-UAS technology. "It's easy at the moment to detect and defend, but no event has yet taken place to drive a real sense of urgency," he said. "Gatwick clearly identified challenges. In a cluttered urban environment, most systems are extremely challenged, including EW-defeat systems which cannot be turned on all the time and someone must be in the loop and watching a screen 24/7. Equally, unmanned capabilities are growing exponentially, not just in the asymmetric and IED role, but also in intelligence and information gathering, as well as communications. So a drone crashing into a formation is the least of our worries," Annis added.

COMMERCIAL SOLUTIONS

One of the industry partners drafted in to assist with C-UAS operations at Gatwick Airport in 2018 is Italian company Leonardo, which has already supplied elements of its Falcon Shield solution to the UK's Royal Air Force. Leonardo Electronics' sales and marketing manager, Andy Roberts, describes how the C-UAS market is currently "very strong," with demand being witnessed from both military and civil customers, such as airport operators. "We've actually seen a major uptick in interest over the last few months in response to well-publicized incidents of malicious drone activity, such as the multi-day closure of Gatwick Airport just before Christmas," he explained. "Prior to these incidents, malicious drone activity was seen as a risk, but only really 'on-paper.'"

"Now that the danger has actually manifested," Roberts said, "we're seeing many organizations looking to mitigate this risk. Because the Leonardo Falcon Shield was the system operated by the

Compete Against Drones

C-UAS solutions continue to be employed to protect critical national infrastructure including international airports in addition to ongoing support of expeditionary armed forces. ADAM MOREIRA

Royal Air Force at Gatwick Airport (and later at Heathrow airport) to help bring about an end to the crises, we're seeing interest from civil operators in addition to our traditional military market."

"Right now, we're at a relatively early stage as regards the uptake of C-UAS systems," he explained, "so the capability gap for most operators is between having nothing at all and having an effective C-UAS system. But the technology is there, it's just a case of getting the kit into the hands of operators."

Nonetheless, Roberts also warned that UAS technology was developing so fast, it was critical that C-UAS system providers did not "stand still" in upgrading capabilities. "Our experts are constantly evaluating the latest drone technologies, modes of operation and usage, so that Falcon Shield can evolve to stay current as the drone threat evolves," Roberts stated, before explaining how it was becoming increasingly difficult to use jamming technology to halt a drone which is flying an automated path (i.e., without any reference to its environment such as GPS) due to a lack of control signals directing its movement. "Of course, even in this case, we can still jam and/or trace a video feed going back to the drone's operator, but this may not be enough. So we're always looking at new ways to address the threat."

Leonardo's Falcon Shield, which currently lies at Technology Readiness Level (TRL) 9 and claims to be capable of detecting any commercially available drone, has been designed as a modular system which can be adapted to the specific operational requirements of the end user, Roberts explained. "A military customer is likely to have a different set of needs to a large airport operator, which will in turn have different needs (and budget) to the operator of a small airport…" Modular building blocks in the Falcon Shield solution include command-and-control software and operator workstation; radio-frequency (RF) detector and/or a 3D radar to detect drones; Nerio Ultra-Long-Range (ULR) electro-optical system, which includes a thermal imaging (TI) camera to track and identify UASs; and Leonardo's Guardian jammer to defeat threats.

Highlighting the Guardian jammer as a differentiator in the Falcon Shield solution, Roberts described it as an "electronic sniper rifle" designed to avoid transmitting indiscriminate barrage jamming, which can have "unintended effects on other signals in the area, such as mobile phones".

In Germany, a triumvirate of companies – comprising Rohde & Schwarz, ESG and Diehl – are offering the Guardion C-UAS solution to support emerging operational requirements across the continent. Director of C-UAS Detection and Counter Solutions at Rohde & Schwarz, Götz Mayser, explained how the past several years had seen commercially available and easy-to-use drones becoming a "tool of choice for anyone with sinister plans." "There is increasing concern about the intended or unintended misuse of drones, ranging from invasion of privacy, covert delivery of drugs and weapons, to the endangerment of public figures and terrorist attacks. With the proliferation

of small rotary-wing UASs that are easily available, the age of the UAS-threat has become a reality, and defending against it will require considerable effort and resources from both industry and the military," Mayser stressed. As a result, he believes C-UAS technologies will continue to emerge as the "go-to technology" for homeland security, law enforcement agencies, private security and other government entities, with an abundance of systems becoming available to customers across Europe. However, Mayser warned that legislation supporting UAS and C-UAS operations remained "scarce" across Europe and the world as a whole, differing from country to country: "It is not clear whether industry can provide sufficient safeguards to deal with new challenges and threats," he said.

The Guardion solution comprises a combination of electronic sensors and countermeasures systems. Within the sensor suite, Rohde & Schwarz's Ardronis radio-monitoring solution detects and identifies UAS control uplink signals at a very early point. "It can take the bearings of the remote controller

Guardion comprises a joint effort between Germany's Rohde & Schwarz; ESG; and Diehl, which manufactures the HPEM soft-kill effector to neutralize UAS. ROHDE & SCHWARZ

even before the drone takes off and can help bring an offending unmanned aircraft to a halt," Mayser explained while describing how the Ardronis monitors remote control uplink and drone downlink signals (typically in the 433-MHz, as well as the 2.4- and 5.8-GHz frequency bands). The system is capable of detecting and locating threats out to a range of 1.5 km in urban and highly congested frequency bands, and at ranges as far as 5-7 km under optimal conditions. The system is also supported by a library of UAS control signal profiles in order to classify the type of UAS, or at least its command and control system.

"Thanks to automatic online hopper analysis capabilities," Mayser explained, "Ardronis analyzes technical radio parameters, such as hop length, symbol rate and modulation type, and then classifies the transmission system used. With this classification result, Ardronis can force the drone to fail-safe by disrupting the uplink control signal with a smart, adaptive, low power-jamming countermeasure." Mayser continued.

Guardion, which can also feature radar and electro-optical (EO) detection systems, can be networked to acoustic sensors to overcome any "blind spots," which are often prevalent in the urban domain. Sensors feed into ESG's Taranis command and control system; and Diehl's High Power Electro Magnetic (HPEM) effector as another soft-kill solution.

Guardion also features a data recording capability, which includes all command signals from the operator to the

Drone Guard

The Field Proven C-UAS Solution

Drone Guard: Modular Drone Detection, Identification & Interception System

Meet us at
DSEI 2019
Booth S7-330

- C-UAS with unique, integrated, multi-sensor, multi-layer architecture for complete protection.
- Robust search and track with 3D phased array X-Band RADAR; long range COMINT; and high resolution EOIR.
- Efficient neutralization with high accuracy directional jammer; or Take Over.
- Unified C2 for enhanced performance.
- Portable, fixed site, and On-the-Move configurations.
- Over 100 systems deployed worldwide.

ELTA Systems Ltd.
www.iai.co.il • market@elta.co.il

IAI
Where Courage Meets Technology

drone, as well as captured WiFi video footage transmitted to the drone operator. This information can be used as evidence in subsequent legal proceedings against the drone operator. In addition, the collected signals are used to update the Ardronis system's threat library. "Everything the system intercepts can be archived, from individual detection results to entire RF scenarios," Mayser confirmed. "The ever-growing user-friendly drone profile archive lists all types of common drone uplink signals with their critical parameters. The [Guardion] operator can black-and white-list certain drone profiles and can train in new drone signal types on their own. We are furthermore working on new features that allow interconnection of distributed multiple sensors, as well as improved jamming capabilities."

In the UK, Liteye Systems' Anti-UAV Defence System (AUDS) continues to be developed on the back of its employment in Iraq to support coalition operations over the past several years. The AUDS, which includes Chess Dynamics' Hawkeye DS and EO Video Tracker, Blighter's non-rotating passive electronically scanned array A400 Series Air Security Radar, and Enterprise Control Systems' Directional RF Inhibitor in Ku- and L-bands, was mounted on board Oshkosh Defense's Family of Medium Tactical Vehicles (FMTVs) to provide force protection for US Army units.

According to a company spokesperson for Chess Dynamics, the C-UAS market remains a fragmented one. He described how the market continued to feature a series of companies specializing in one of the "detect," "track and identify" and "defeat" mission sets. "There are very few [companies] who are able to offer fully-integrated solutions that encompass multiple sensors," the spokesperson explained. "Equally, there are many people who claim that their single [mission set] solution equipment is the panacea and the best on the market. It clearly isn't because it has never been operationally tested in combat. That privilege is restricted to very few and cannot be understated." As a result, Chess Dynamics unveiled to the market two new C-UAS solutions in June – the AirShield and AirGuard systems.

Leonardo's Falcon Shield has been designed as a modular system of systems, capable of accommodating platform-agnostic sensors and effectors dependent upon customer requirements.
LEONARDO

AirShield is a wide-area detect, track, identify and defeat solution incorporating radar, RF direction finding and EO sensors, as well as identification software that involves a degree of machine learning and a narrow-beam, software-defined RF inhibition system. According to Chess Dynamics' spokesperson, AirShield can be integrated into battle management systems and networked to hard-kill weapons, including medium-caliber cannons firing airburst ammunition. "It is based loosely on the original AUDS concept but, utilizing open architecture, is able to integrate different radars, different detect sensors (including acoustic sensors) and enhanced identification techniques," the spokesperson added.

Additionally, Chess Dynamics' AirGuard system is a "role-specific detect, track, identify and warn system" designed specifically for protecting the airspace around an airport. Featuring an EO camera (both daylight and IR) and a 3D narrow-band weapon tracking radar, AirGuard is able to identify the hostile UAS's velocity and trajectory to predict the point and time of impact with an incoming or outgoing aircraft.

Chess Dynamics continues to work on reducing the electromagnetic signatures of its systems, in order to minimize interference with other systems in an area of operations. The company is also very focused on developing open architecture solutions which, the spokesperson explained, must be standard across the industry to ensure all potential C-UAS solutions are scalable and adaptable.

In France, Thales is offering its ForceShield C-UAS solution, which can also be integrated into a wider integrated air defense system. At this year's Paris Air Show, the company's head of Airborne C4I, Thomas Got, described how the solution was designed to protect against the "proliferation of new airborne threats, such as missiles and UASs and the increasing complexity of the airspace." Got described how ForceShield formed part of Thales and Thales Raytheon Systems' wider Advanced Air Defence concept. Specifically, the ForceShield solution includes the GM200 multi-role 3D medium-range and short-range air defense engagement radar, and Skyview C2 weapon coordination software. The system is supported by a variety of hard-kill weapons including Thales' Lightweight Multirole Missile (LMM) and StarStreak, which can be fired from the Rapid Ranger Launcher for force protection and mobile solutions.

In February, Danish company MyDefence unveiled its latest C-UAS solution. The Knox system, so-called after the US Bullion Depository in Kentucky, was designed in response to the closure of Gatwick Airport and comprises a fixed-installation C-UAS capability to protect critical national infrastructure.

Advance with Cobham

Innovation Starts with the Building Blocks of Technology

Cobham Advanced Electronic Solutions designs and manufactures off-the-shelf and customized RF/microwave/millimeter wave components, assemblies, apertures and subsystems as building blocks for EW systems that provide detection, identification and countering of threats in an ever-changing Electromagnetic Spectrum Warfare environment.

Cobham Advanced Electronic Solutions

Advance with Cobham at: www.cobham.com/EW

COBHAM

INNOVATION THROUGH INSIGHT

www.cobham.com

2121 Crystal Drive, Suite 800, Arlington, VA 22202
T: +1 (703) 414 5300 E: CAES.BD@cobham.com

Thales's ForceShield C-UAS solution features the company's own SkyView C2 software allowing end users to view a common operating picture of the entire battlespace. THALES

Capable of detecting, locating, tracking and defeating smaller classes of UASs, Knox features a reactive smart jammer, a purpose-built UAS radar system and integrated EO/IR sensors. The sensor-agnostic solution also features an open architecture to enable integration of third-party technology dependent upon customer preference. According to a company source, "Knox allows customers the ability to integrate third-party sensors without being dependent on one type of C2 user interface, thereby providing a future-proof system which can continuously be upgraded as the threat evolves and new mitigation solutions are introduced."

The development of Knox follows efforts by MyDefence to provide C-UAS solutions down to the lowest tactical level. Other systems from the company include a mobile C-UAS solution which has been integrated on board a General Dynamics Land Systems Light Armored Vehicle (LAV) and demonstrated at the NATO Non-Lethal Technology Exercise (NNTEX-18) in Quantico, VA, in December 2018. This system uses passive RF sensors to detect threats out to a maximum range of 2km. Measuring a total of 10kg with a series of four antennas located on each corner of the vehicle chassis, the mobile C-UAS system operates in the 2.4- to 5.8-GHz frequency range. Sensors can be supported by any open architecture C2 solution, including MyDefence's own IRIS battle management system. The system's RF sensors can also be networked with MyDefence's 23-kg Eagle X-band radar and can detect UAS threats out to a maximum range of 1km within four seconds. According to company sources, NNTEX-18 provided MyDefence with the opportunity to "field-test" C-UAS technologies across a variety of exercise scenarios including swarms of UASs in the urban environment.

MyDefence also has been among the few companies to expand C-UAS solutions beyond vehicles and fixed sites. The company has designed a range of man-wearable C-UAS solutions for small units and Special Forces users. The company's Wingman 103 Drone Detector is a man-wearable 735-gram system that uses MOLLE straps to attach to a vest or back pack. The sys-

continued on page 34

WASHINGTON D.C.

56TH

AOC INTERNATIONAL SYMPOSIUM & CONVENTION

OCTOBER 28 - 30, 2019

DISCOUNTED REGISTRATION **ENDS SOON!**

56.crows.org

Host Sponsor

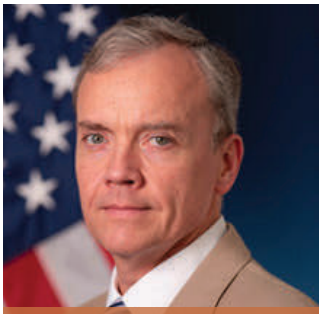
BAE SYSTEMS

SPEAKER SPOTLIGHT

The Honorable David L. Norquist
United States Deputy Secretary of Defense *(Invited)*

The Honorable Don Bacon
U.S. House of Representatives
NE-02 *(Invited)*

James A. Faist, SES
Director, Adv Capability,
OUSD Research & Engineering



Dr. Tim Grayson
Director, Strategic Technology Office (STO), DARPA

For a full listing of distinguished speakers, please see 56.crows.org

SYMPOSIUM INFORMATION

Building the EMS Enterprise

The 56th Annual AOC International Symposium and Convention will survey the EMS Enterprise across the *Technology, Readiness, Organization* and *Support* equities necessary to achieve EMS Superiority. Distinguished senior military and civilian leaders and subject matter experts will discuss how the global environment is fueling new opportunities in technology and operational concepts for military forces.

Registration Pricing

	~~By 7/31~~	8/1-10/4	10/5-OnSite
All Access Industry (Member)	~~$695~~	$795	$895
All Access Industry (Non-Member)	~~$895~~	$995	$1095
All Access Academia*	~~$445~~	$545	$645
All Access Young Crows*	~~$445~~	$545	$645
All Access Government Civilian*	~~FREE~~	FREE	FREE
All Access Military in Uniform**	~~FREE~~	FREE	FREE
Exhibition Only	~~FREE~~	FREE	FREE

*Must present proper ID for discounted price:
- Academia - faculty/staff/student ID.
- Young Crows (35 years old and younger) - photo ID with DOB.
- Government Civilian - government ID or civilian CAC card.

**Duty uniform must be worn each day. If not, a fee of $100 will be assessed.

Discounted pricing ends 10/4!

PROFESSIONAL DEVELOPMENT COURSES

Make the most of your trip! Sign up for a professional development course while you're here!

Machine Learning for EW
October 26 – 27, 2019
Presented by: Kyle Davidson

Fundamental Principles of Electronic Warfare
October 26 – 27, 2019
Presented by: Dave Adamy

ECM: Theory & Design
October 31 – November 1, 2019
Presented by: Kyle Davidson

Advanced Principles of Electronic Warfare
October 31 – November 1, 2019
Presented by: Dave Adamy

THE INNOVATION STAGE RETURNS!

We invite you to join us at the Innovation Stage presented by Keysight Technologies and Rohde & Schwarz. Talks will explore how state-of-the art ideas and technology applications come together to create a new reality, examine unconventional solutions to stay one-step ahead of emerging threats, and challenge us to rethink what we know about the "laws of physics."

INNOVATION STAGE
DYNAMIC DELIVERY. CAPTIVATING CONTENT.

The Innovation Stage offers a series of short, dynamic and fresh perspectives that build upon the conversation surrounding this year's Symposium theme "Building the EMS Enterprise." The ideas, aspirations, and knowledge shared on the Innovation Stage are intended to generate and exploit new ideas to solve problems and think differently about advancing our shared mission and common interests in EMS operations.

The Innovation Stage sessions are open to all badge types – all Access Pass, Exhibition Only Pass, and Booth Personnel.

Presented by: KEYSIGHT TECHNOLOGIES ROHDE&SCHWARZ

AOC CAREER FAIR

The Association of Old Crows is proud to announce the 2019 AOC Career Fair, held in conjunction with the 56th Annual AOC International Symposium & Convention. The industry's top employers will be showcasing their **current openings** to the largest concentration of **qualified candidates** in the Electromagnetic Warfare community! The Career Fair takes place all 3 days in the Exhibit Hall during official show hours.

CAREER FAIR
THE INTERSECTION OF TALENT & OPPORTUNITY

Job Seekers: Register for a complimentary "Exhibition Only" pass, or any other paid registration.

Employers: Contact **Jim Cook - jim.cook@communitybrands.com** or **727-497-6552** to reserve your space in the AOC Career Fair.

PROGRAM MANAGER BRIEFING SERIES

AOC is thrilled to launch our inaugural Program Manager (PM) Briefing Series which will be held during this year's International Symposium and Convention. The PM Briefing Series will offer a technology interchange in a series of **45-minute sessions** comprised of presentations from PM offices across the military services and audience Q&A. This program will be **open to only 2019 exhibiting companies.** Each company will receive the complimentary benefit of one transferable ticket to attend the series. During this program, exhibitors will **hear directly from their government customers** on the status of key programs and activities under their leadership, opportunities and milestones on the horizon, and how government and industry can strengthen collaboration.

5TH ANNUAL AOC STEM PROGRAM

GET INVOLVED!

The AOC is proud to host its 5th Annual STEM Outreach Program on the Exhibit Hall floor, but we need your help! Here are some ways you can help pour into future crows:

Display: Demonstrations & Interactive displays of EMS foundations & technologies are needed
Volunteer: Guide students through the displays *(10+ volunteer hours = FREE REGISTRATION)*
Donate: Companies and Individuals are encouraged to support - sponsor a student for $100

Contact **Blain Bekele - blain@crows.org** or **703-549-1600 x217** to take part.

EXHIBIT HALL SPACE IS NEARLY FULL!

Booth space on the convention show floor is almost gone! Don't let the opportunity to exhibit at the biggest Electromagnetic Warfare event of the year pass you by. Contact **Sean Fitzgerald – fitzgerald@crows.org** or **703-549-1600 x222** for more information. Learn more at **56.crows.org**.

2019 Exhibitor Listing

COMPANY	BOOTH
412TW Benefield Anechoic Facility (BAF)	916
Advanced Test Equipment Rentals	221
Aethercomm	737
Alaris Antennas (Pty) Ltd	202
American Standard Circuits	240
Ampex Data Systems	316
Analog Devices	731
Annapolis Micro Systems, Inc.	911
Antenna Research Associates, Inc.	338
AOC EW Europe	210
API Technologies Corporation	207
ApisSys	502
Applied Thin-Film Products	212
ASELSAN A.S	334
Atlanta Micro, Inc.	437
Azure Summit Technology	410
BAE Systems	515
Boyd Corporation	503
Cobham	605
Communication Power Corporation	922
Communications & Power Industries LLC	302
Comtech PST	327
Conduant Corporation	239
CRFS	211
dB Control	500
Deepwave Digital	232
Digital Receiver Technology (DRT)	330
Directed Energy Professional Society (DEPS)	340
Dixie Crow Chapter AOC	406
D-TA Systems	633
Elbit Systems	817
Elite RF	241
Empower RF Systems	807
Epiq Solutions	318
ESROE Limited	224

COMPANY	BOOTH
FEI-Elcom Tech	816
Ferrite Microwave Technologies	918
General Dynamics Mission Systems	728
Georgia Tech Research Institute	404
Giga-tronics	323
Gowanda Components Group	820
Herrick Technology Laboratories, Inc	231
Interface Concept	815
iRF-Intelligent RF Solutions	732
Keysight	602
Kratos General Microwave	505
L3Harris	409
Leonardo DRS	908
Lexatys, LLC	238
Lockheed Martin	705
MC Countermeasures Inc.	332
Meggitt	504
Mercury Systems	623
Metamagnetics	914
Microwave Products Group	405
Microwave Specialty Company	719
Motorola Solutions, Inc.	818
National Instruments	304
Northrop Grumman	509
Ophir RF	723
Pasternack	204
Patria	631
Pentek	422
Photonis Defense Incorporated	426
Physical Optics Corporation	424
Planar Monolithics Industries, Inc	907
Plexsa Manufacturing	827
Procitec GmbH	501
PSI Cases	235
Q Microwave, Inc.	401

COMPANY	BOOTH
Qorvo	320
Raytheon Company	417
Research Electronics International	324
Rohde & Schwarz	611
Rotating Precision Mechanisms Inc	219
S2 Corporation	926
Saab Defense and Security	537
Schaefer Electronics Inc	216
Sierra Nevada Corporation	811
Signal Hound	722
Silver Palm Technologies	326
Spectranetix	600
SRC, Inc.	305
Syncopated Engineering Inc	230
Syntonic Microwave	208
TCI	725
TE Connectivity	638
Tektronix, Inc.	830
Teledyne Defense Electronics	711
Terma North America	823
TEVET	636
Texas Instruments	836
Textron	331
TMD Technologies, LLC	721
TrustComm	220
ULTRA ELECTRONICS - EWST	906
Vadum Incorporated	234
VectorNav	629
VIAVI Solutions, formerly Aeroflex	536
Wideband Systems	403

Space subject to change, accurate as of 8/6/2019

BATTLESPACE SIMULATIONS, INC.

Don't Settle for Only Part of the Battlespace

MODERN AIR COMBAT ENVIRONMENT (MACE)

BSI's MACE is a powerful yet easy to use full-spectrum computer generated/semi-automated forces (CGF/SAF) simulation.

PHYSICS BASED EW

MACE uses advanced physics-based models for all platforms, weapons, and EW signal propagation to include environmental conditions and terrain.

VIRTUAL EW EQUIPMENT SUITE

Existing emulations include: ALR-69 RWR, ALQ-161 Receiver/Jammer, ALE-47 Countermeasures System, USQ-113 Comms Jamming, ALE-50 Towed Decoy, DF Scope, & more.

EXTENSIBILITY

Enhanced 'no-code required' scripting engine allowing users to extend the MACE UI with custom tactics & behaviors. Developer API supports tight integration directly with MACE.

AND SO MUCH MORE...

Visit us at www.bssim.com to learn more.

Raising the Bar with 5th Gen Signal Generation and Processing Capabilities

BSI is proud to release the next generation of the Modern Air Combat Environment (MACE) with features that include:

- **Simulate advanced 5th generation radar systems such as Active/Passive Electronically Scanned Arrays (AESA/PESA)**
- **Rich modeling of the electromagnetic battlespace including advanced 2D/3D radar beam and scan visualization**
- **High-fidelity real-time threat simulation and emitter audio**
- **Self-protection, stand-off, and escort jamming**
- **Signal data generation to the pulse-level**
- **Third-party extensibility and integration via advanced script editing or the available MACE Application Programming Interface**

Battlespace Simulations, Inc.
"Don't Settle"

www.bssim.com **sales@bssim.com**

A-10 Scene Rendered by MetaVR's Virtual Reality Scene Generator

continued from page 28

tem, which features internally mounted directional antennas that cover 2.4- and 5.8-GHz, can detect C-UAS signals at ranges up to 1 km (line of sight). The AA100 external antenna, (9.2 inches and weighing 200 grams) provides 360-degree coverage of 433-MHz, 1.2 GHz, 2.4 GHz and 5.8 GHz signals. The system is powered by clip on batteries (providing 14 hrs of power) commonly used with AN/PRC-148/152 radios. On the countermeasures side, the company's Pitbull smart jammer can defeat drones at distances up to 1 km by jamming at 2.4 and 5.8 GHz, as well as GNSS frequencies. The 775-gram Pitbull provides an internally mounted antenna and can operate continually for 2 hours, or up to 20 hours on stand-by via a standard (AN/PRC-148/152) battery.

The PITBULL is a wearable counter-UAS system. MYDEFENCE

FUTURE DEVELOPMENT

Seeking to future-proof C-UAS technology to deal with emerging threats, particularly relating to swarms of autonomous systems, industry continues to consider the integration of machine learning and artificial intelligence algorithms into solutions.

For example, NGIS's deputy segment director for precision weapons, Robert Menti, says the major challenge facing the market remains determining the intention of threatening UASs as well as the ability to "rapidly classify red, blue, green or white threats" across congested and cluttered areas of operation. As a result, Menti says NGIS is looking to integrate "advanced data analytics and machine learning" into its systems-of-systems C-UAS solution which is designed to bring together technologies from across the market into a single capability as part of a systems integration approach.

Another industry source also described how machine learning and artificial intelligence could represent the "most important area of growth, and very clear markers have already been laid by the requirements setters that this has to be an integral feature of all 'future' systems."

Such upgrades are also being considered by Leonardo for its Falcon Shield capability, with Roberts explaining: "In most cases, it's not economically feasible for a commercial operation such as an airport to have a crew of dedicated operators manning C-UAS systems 24/7, so we're always looking to reduce operator workload. Artificial intelligence and machine learning could play a role in that, such as by automatically recognizing a drone type, alerting the relevant operator and suggesting an appropriate countermeasure.

"We're already some of the way towards this model. In normal circumstances, the Falcon Shield system can be incorporated into routine activities and effectively operated by one individual whose primary responsibilities will lie elsewhere, but artificial intelligence could improve this even further," he added.

Looking at the market holistically, industry continues to view the C-UAS domain as a rapidly expanding sector with demand signals from both governments and commercial entities in particular, enabling a series of significant requirements in the short-, medium- and long-term. As another industry source observed, "miniaturization, automation, and being able to defeat UASs operating outside the recognized ISM frequency bands, present some of the key development drivers moving forward across the marketplace. Effective countermeasures against fully autonomous BLOS [beyond line of sight] UAS operation should be seen as essential and needs to be accelerated."

Elsewhere, Leonardo's Roberts also described how the sector will see military organizations and larger airport operators leading demand for C-UAS solutions in the future. "Given the speed of acquisitions, I'd see this being the case for the next 2-3 years. Then, as drone technology evolves and becomes even more widespread, I'd see a bigger demand from operators worldwide, including smaller civil customers and even private individuals. However, much will depend on legal frameworks at national and international levels in respect of drones." For example, he notes that "there are big questions to ask such as should personal 'hobby' drones be regulated? And, should airport operators be allowed to jam potentially rogue drones? This is where the views of various governments will have a big impact on the market for C-UAS systems."

Finally, Rohde & Schwarz's Mayser believes the next five to ten years will see governments looking to develop new defensive capabilities in order to draw upon autonomous decision-making mechanisms and networked sensing systems capable of detecting, tracking, identifying and defeating hostile drones over complex and varied environments. "Homeland security, law enforcement agencies, private security and other government entities will put their trust into more multi-effector solutions and countermeasure that include control link jamming, GPS jamming, sensor blinding or disruption of electronics," Mayser explained, adding that, "UAS use will almost certainly continue to increase in the future, if only for the asymmetric advantage they offer as a comparatively low-cost, yet high impact, asset. In this respect, recent experiences in Israel and Syria in the military sphere, and Great Britain, Germany and Singapore – only to mention a few – in the civilian domain, may be dress rehearsals for the intensification of the dangerous uses of UASs in the future."

5th Annual Cyber Electromagnetic Activity (CEMA)

ASSOCIATION of OLD CROWS

8-10 OCTOBER 2019 Aberdeen Proving Ground, MD

"On the Road to Army of 2028 - Delivering Integrated EW, SIGINT and Cyber at the Tactical Echelon"

REGISTER NOW!

This year's event will continue to expand the CEMA discussion from a doctrine, operational, technology, and threat perspective and how to integrate electronic warfare, cyber, signals intelligence, information operations, and other forms of non-kinetic fires into operational formations. **Security clearances for all international participants are due by August 23! Requests for US participants are due September 17! Visit our website for all necessary information.**

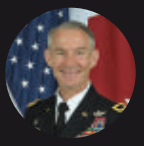
DISTINGUISHED SPEAKERS

GEN John M. "Mike" Murray *(invited)* Commanding General, US Army Futures Command

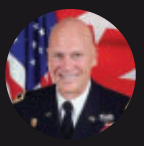
LTG Scott David Berrier *(invited)*, United States Army, Deputy Chief of Staff of the Army G-2 (Intelligence)

LTG Stephen Fogarty *(invited)*, USA, Commanding General, Army Cyber Command

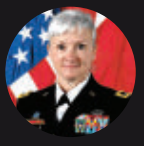
The Honorable Dr. Bruce D. Jette, Assistant Secretary of the Army for Acquisition, Logistics and Technology



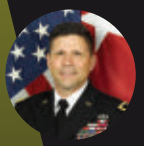
MG Neil Hersey, Commanding General, Cyber Center of Excellence and Fort Gordon



MG John Morrison *(invited)*, USA, Chief of Staff, US Cyber Command

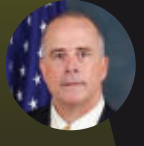


MG Laura Potter, Commanding General and Commandant, U.S. Army Intelligence Center of Excellence and Fort Huachuca, Fort Huachuca, Arizona



MG Joel K. Tyler, Commanding General, U.S. Army Test and Evaluation Command

BG Robert M. Collins PEO IEWS



Mr. Roy Fox, SES, U.S. Army, Capabilities Development and Integration Directorate

Sponsorship opportunities are going fast!

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

crows.org/page/CEMA2019

DOD's Broad Vision for Electromagnetic Battle

By Dr. Bill Conley, Dr. John Stine, Adam Miller and Brig Gen Lance Landrum

The Electronic Warfare Executive Committee (EW EXCOM) currently considers the Electromagnetic Spectrum (EMS) as a medium of maneuver for the Joint Force and recognizes that the EMS is essential for successful Command & Control (C2), maneuver and kinetic engagements. Through internal debates, the Department of Defense (DOD) has examined many issues involving the EMS, including software tools required to visualize and control it, why we need each tool, and how we intend to use the tools to expand the competitive space as described in the National Defense Strategy (NDS). The maneuver space mentality enables Unity of Command.

The capability that the Joint Force Commander exercises to manage the EMS is typically referred to as Electromagnetic Battle Management (EMBM). While this term has been used to refer to a tool, in fact EMBM is a much broader concept. Investment in any electromagnetic planning and battle management tool must anticipate enabling the broader concept. Further, the broader concept will affect how all Services implement the C2 of EMS Operations (EMSO) and how future spectrum-dependent systems (SDSs) are designed to respond to that C2. Physics, technology and the principles of maneuver warfare should drive the design of EMBM tools.

Through a two-year study funded by the Office of the Under Secretary of Defense for Acquisition and Sustainment and performed by MITRE in support of the EW EXCOM, we have identified visionary keys of how EMBM is a broader concept. DOD will build an EMBM tool to assist the Joint Force Commander in planning and understanding EMSO. To achieve the dynamic spectrum operations called out as an objective in the 2015 Defense Science Board study, "21st Century Operations in a Complex Electromagnetic Environment," it must be designed to enable the overall concept. This article describes the vision that the DOD has for this broad concept of EMBM.

VISION #1: EMBM will not only determine if a spectrum plan is acceptable, but will also enable the dynamic and real-time adaptation of EMS maneuver

Today, most EMBM activities occur in peacetime and involve evaluating the sufficiency of a spectrum plan. This sufficiency review determines if enough spectrum resources are available to support the Department's needs. This focus on static EMBM planning risks inadequate integration of EMBM into operations. Just as detailed, exquisite plans lack the flexibility to be rapidly modified during an operation and are too easy for an adversary to disrupt during conflict (much as the Schlieffen Plan of 1914's reliance on strict movement timetables proved too brittle), so EMBM does not exist solely to fill and deconflict spectrum assignments.

EMBM is a far-reaching concept that gives our commanders flexibility and extends to how we design all of our SDSs to enable unity of effort. As funded in the President's Budget for FY20, the establishment of Joint EMS Operations Cells at the Combatant Commands sets the expectation for real-time EMBM in wartime that can effectively support operational maneuver in the EMS during a conflict. Thus, EMBM will no longer be a planning function but a vital part of the commander's plan, enabling SDSs to synergistically maneuver in the EMS.

EMBM must be viewed as a concept that extends to all operators and to the way we do business in the EMS at all echelons, through all phases of conflict and within all Services. This perspective characterizes the EMS as a maneuver space as opposed to a utility. Treating the EMS as a maneuver space expands the operational competitive space – a goal of the NDS.

VISION #2: EMBM extends beyond the Joint Task Force headquarters, enabling multiple command echelons to make C2 decisions

Low-latency, high-capacity communication networks enable the centralization of operational decisions, improve spectrum efficiency and make spectrum interference easier to identify and address. However, complete centralization of decision-making is not a viable operational strategy. Centralized decision-making limits operational flexibility and prevents commanders from making necessary localized decisions, contrary to the doctrine of centralized control and decentralized execution. Commanders at all echelons must be able to optimize their use of spectrum and to execute EMS maneuver; during a communications-degraded operation, centralized C2 will likely prove ineffective, as the necessary feedback will not be

EMBM will no longer be a planning function but a vital part of the commander's plan, enabling Spectrum Dependent Systems to synergistically maneuver in the EMS.

Management

regularly and reliably available. EMBM seeks to provide visualization tools to commanders at all echelons, enabling them to control assigned forces operating in the EMS. The Services are already investing in tools to realize this vision. EMBM is not intended to centralize all decision making as a staff function; instead, it centers on enabling centralized planning and decentralized execution in the EMS. Distributing C2 will create opportunities for emergent dynamic behavior and enable commanders to exploit local opportunities. However, this comes at a cost, because distributed execution increases the complexity of deconfliction.

Using Marine Corps Doctrinal Publication 1: *Warfighting* as an illustration, attaining the goal of creating multiple dilemmas for an adversary results from giving mission orders with the commander's intent, which then allows subordinates to act on their initiative to achieve a collective objective in a way that overwhelms the adversary. To achieve this vision, the means used to execute EMBM must extend beyond tools exercised at senior command levels and become integrated with Service component capabilities.

VISION #3: EMBM enables the commander to proactively take action

There is a common understanding across the DOD that for commanders to respond to adversary actions in the EMS they must have the means to visualize the EMS, and several nascent EMBM tools are designed to provide this capability. Drawing on an understanding of the operational environment, commanders can respond (with maneuver, fires, etc.) to mitigate the effectiveness of an adversary's initiative. EMBM, however, should turn the equation from response to friendly initiative: to enable friendly force offensive maneuver that creates dilemmas for our adversaries.

Electronic attack (EA) creates problems for adversaries in the areas of escalation control, first strike capability and attribution. Yet, there are countless examples where Electronic Warfare Officers (EWOs) were constrained from acting by commanders who mistakenly believed that the EWO's activity would disrupt friendly C2 links. In these cases, visualization at the command level would have been helpful to resolve the perceived spectrum interference. To realize the NDS goal, commanders must empower their assigned EMS units and staffs to seize the initiative while minimizing the negative impacts on friendly forces (including our allied partners).

In a contested environment, supporting centralized understanding of the entire Electromagnetic Operating Environment (EMOE) in real time may not be feasible. Instead, a culture and doctrine of making decisions at the tactical edge is required. By defining EMS maneuver spaces and operational goals, lower echelons can initiate complex actions and produce emergent behaviors. Combined arms is an excellent historical example of emergent behaviors. Deception actions can result from emergent EMBM capabilities today.

VISION #4: EMBM combines the best of spectrum management and electronic warfare planning to enable dynamic maneuver

Spectral fratricide can occur when operational realities fail to match the commander's plan. Currently, joint spectrum interference resolution (JSIR) is a problem that stands out to spectrum managers, and DOD requires better capabilities to address its challenges. As the density of SDSs in the operational environment continues to increase, EMBM must improve the commander's ability to integrate maneuver in the EMS with maneuver in the traditional domains. must occur in the way we think about spectrum management: we should move away from envisioning it as obtaining control over a resource and move toward considering it as the way we protect and preserve our ability to shoot, maneuver, and communicate. This elevates the role of EMBM beyond that of a tool for deconfliction; it must support the integration of EMS maneuver with all other types of maneuver.

In Combatant Commands that work with multiple partner nations, the current process for requesting host nation (HN) spectrum approval is time-consuming and cumbersome. However, improving only the process is an example of the current mindset and fails to address the underlying issue; instead, we need to view the

Commanders at all echelons must be able to optimize their use of spectrum and to execute EMS maneuver; during a communications-degraded operation, centralized C2 will likely prove ineffective, as the necessary feedback will not be regularly and reliably available.

There is a common understanding across the DOD that for commanders to respond to adversary actions in the EMS they must have the means to visualize the EMS, and several nascent EMBM tools are designed to provide this capability.

EMS as a maneuver space. Systems with static assignments are more easily targeted, since their spectrum utilization can be discerned, anticipated and countered.

The future JSIR function must expand the competitive space, support dynamic maneuver, and deny adversaries any useful insight into the wartime operations of our SDSs. EMBM capabilities must bridge the maneuver strategy into the reality of numerous unique and diverse HN spectrum approval processes.

VISION #5: EMBM will control diverse, distributed system-of-systems devices

Complex combinations of capabilities developed during conflict such as combined arms, systems-of-systems, and, recently, multi-domain battle, will have an impact on military planning for future generations. In all of these cases, humans have integrated and performed C2. However, this approach is not sustainable in the future given the increasing complexity and technical variables available to an operator. We must standardize a common knowledge base and method for communicating operations occurring in the EMS to improve effectiveness and efficiency. EMBM will provide commanders insight into the real-time performance of the distributed system-of-systems.

Synchronizing our efforts in the EMS will require establishing interfaces and standards for EMBM as a concept before developing specific planning and management tools to execute EMBM. EMBM must take into account how orders are given, how plans are shared, how coordination is performed to avoid conflicts, and how control measures are used to mitigate interference and to specify desired effects. Therefore, a major outcome of EMBM will be the technical means of coordinating and conducting Joint EMS maneuver. EMBM is a system-of-systems concept, and the design of the Joint tool will influence how Service tools and SDSs across the DOD will be designed in the future to effectively maneuver in the EMS.

VISION #6: EMBM unites the EMSO community to improve effectiveness, integration and specialization

EMBM encompasses the planning & management tools and operational practices for all EMSO. While the missions are unique, the underlying physics and intuition are very similar for EW, radio communications and radar systems. Alignment around EMSO also creates overlap between technologists

specializing in EW, radio communications and radar design; the same is true for tactical operators and planners. This alignment allows fires through the EMS (better known as EA) to be used advantageously in the scheme of maneuver, including kinetic fires (either direct or indirect), as well as fires delivered through cyberspace.

Technical intuition, derived from years of experience in the art of maneuver operations in the EMS, produces insights that only experienced EMS maneuver practitioners can develop. Extended specialization of EMS units results in ideas for C2 tools, mitigation options and opportunities for obtaining advantage in the EMS.

VISION #7: EMBM will leverage our national means to improve situational awareness for the commander

Understanding adversary objectives and C2, including the presence of data networks and sensors, is a key responsibility of the commander in wartime. While peacetime exploitation is frequently a Title 50 intelligence activity, military commanders must train with, and integrate, these capabilities into their assigned forces. As a nation that values freedom, we must preserve data privacy while improving military readiness to deter adversaries. In the Information Age, with most data links encrypted, detecting a signal no longer reveals specifics about the user or content. Privacy concerns and risk management have resulted in many EMS survey tools being utilized under intelligence authorities instead of operational authorities. To implement the NDS, we must change our culture and processes to provide the operational commander with needed data. Ongoing efforts are improving data exchange between operational and intelligence units.

VISION #8: EMBM creates opportunities by producing situational awareness

Forming an accurate picture of the EMS is extremely difficult both operationally and technically. Producing situational awareness will be an activity of EMBM and not merely a product of the EMBM tool. Warfighters will decide where to place the sensors that detect the EM environment and will execute that plan as best possible. Warfighters will construct the current situation based on what those sensors provide. Further, only warfighters can provide the critical judgement on what the

The real change must occur in the way we think about spectrum management: we should move away from envisioning it as obtaining control over a resource and move toward considering it as the way we protect and preserve our ability to shoot, maneuver, and communicate.

anticipated activities of friendly and adversary warfighters will be, and so create the operating picture that drives many of the functions that EMBM must provide (e.g., deconfliction and synergistic maneuver).

EMBM must provide commanders with tools and data to enable them to visualize the EMS maneuver space in order to make decisions and seize the initiative. While all data can be made available to the commander, not all data results in valuable information, so the data gathered must be processed to focus on the most significant information and produce as accurate a common operating picture (COP) as possible. DOD must overcome many challenges to provide this type of COP, including placing sensors to cover areas of interest; supporting and maintaining the feeds in operational environments on overtaxed networks; and, finally, building confidence in the fused results.

Understanding the EMOE is technically challenging and will require visualization tools to enable humans to understand the battlespace. In gathering disaggregated data, DOD must build an EMBM architecture to add value when connectivity is intermittent, sensors are in disadvantageous locations and uncertainty abounds – Clausewitz called this friction. Advantage comes from what we are able to do as a result of our awareness of conditions in the EMOE and how effectively we can use maneuver in the EMS to support our objectives.

EMS sensing can capture the presence of electromagnetic radiation but usually not the source, reason or intent of a transmission. Understanding the meaning of what is sensed depends on metadata about the sensor and its environment – features that are dynamic and often uncertain. Capturing and consolidating this information is a data-intensive process that imposes high demand on our networks. Further, merely observing a negative event is not helpful by itself. Our real objective is to anticipate, mitigate and exploit adversary electromagnetic radiation. Sensing is helpful to the extent that it enables the identification of emitters so that models of those emitters become part of the EMOE estimate. This understanding supports the commander making maneuver decisions in all domains.

Alignment around EMSO also creates overlap between technologists specializing in EW, radio communications and radar design; the same is true for tactical operators and planners.

VISION #9: EMBM provides Battlespace Awareness

EMS battlespace awareness comprises knowing the current disposition of all friendly and adversary SDSs and the anticipated and potential interactions among those SDSs. (This is analogous in the land domain to knowing the location and direction of movement of an adversary tank column and anticipating how the column will engage friendly forces.) Individual sensors are capable of digitizing the environment at a particular location, but building full battlespace awareness will require many sensors and other intelligence assets collecting data on SDS maneuver and EMS usage over time and across the battlespace. EMBM provides a framework to consolidate this information and to display the disposition of SDSs, their current and anticipated use of the EMS, and, most important, the current and anticipated interactions that merit attention. Capturing the way SDSs interact in models and in how EMBM presents that information is a feature that differentiates EMBM from other battle management systems.

In the congested and contested EMOE, monitoring EMBM's display of blue, red and grey spectrum utilization, commanders can understand EMS patterns of life and identify how maneuver units avoid interference by the adversary, detection by adversary sensors, and engagement by adversary weapon systems, while minimizing the impact on neutral infrastructure. By capturing and understanding the nuances of interaction among SDSs, commanders can implement more technical deconfliction modes (e.g., those that multiplex use by temporal, spatial, directional, and behavioral methods) and execute more precise EA, which allows more use of EA because fratricide is mitigated.

Forming an accurate picture of the EMS is extremely difficult both operationally and technically. Producing situational awareness will be an activity of EMBM and not merely a product of the EMBM tool.

VISION #10: While existing data, models, and algorithms are useful, EMBM must enable timely decision making and execution

The ubiquity of networks, greater computing power, modern propagation models, better modeling of spectrum consumption, spectrum policy language, advanced signal processing algorithms, and efficient signal processing hardware provide the foundation for the real-time control of the EMS, which would have been impossible just a few years ago. Current technology is mature enough to develop and field an electromagnetic planning and battle management tool. This tool must scale into the future; DOD must replace its historical one-on-one analysis of spectrum dependent systems with a many-on-many approach enabled through machine-to-machine interactions. This approach must support effective, rapid, and distributed execution of EMBM both by warfighters and by our

SDSs. It must be broadly adopted so that the EMS activities of the Services in Joint operations are well integrated. Speed of maneuver will be a differentiator in the EMS contest and it hinges on the speed of decision making and execution. Maneuver in the EMS occurs orders of magnitude faster than in the other domains.

NEXT STEPS

As described through the vision statements, EMBM really represents a paradigm change in how we gain advantage through the EMS. It envisions the EMS as a medium of maneuver as opposed to a collection of resources that must be managed; thus, it signifies an essential expansion of the competitive space. EMBM provides the opportunity to meet our strategic objectives, gain operational advantages during a conflict and integrate our tactical systems. The software tools to enable EMBM offer competition opportunities for industry. Doctrine and requirements are leading the way in identifying the next steps; implementation of all the necessary elements will require dedicated effort and leadership. Implementation guides for the Combatant Commands have been issued. As is evident throughout this article, EMBM is not just one discrete thing to one small community; instead, EMBM represents a substantial change in how the DOD accesses, maneuvers and fights in, and for, the EMS.

Current technology is mature enough to develop and field an electromagnetic planning and battle management tool.

EMBM serves as a critical foundation for enabling the United States to fight together with its allied partners. As we develop electromagnetic planning and battle management tools, processes and organizations in the future, EMBM represents the integration of diverse capabilities to achieve Unity of Command.

ABOUT THE AUTHORS:

Dr. Bill Conley is the Director of Electronic Warfare in the Office of the Under Secretary of Defense for Acquisition and Sustainment. He is an Executive Secretary of the Electronic Warfare Executive Committee established in 2015.

Dr. John Stine is the Department Head for Operations Research at MITRE. A retired Army officer, his research focuses on dynamic spectrum access, management, and operations.

Adam Miller is an Electronic Warfare Program Officer at the Office of Naval Research focused on advanced RF electronic warfare technology and complex effects.

Brig Gen Lance Landrum, USAF is the Deputy Director for Requirements and Capability Development in the Joint Staff. He is an Executive Secretary of the Electronic Warfare Executive Committee and is the Deputy Director of the Electromagnetic Spectrum Operations Cross Functional Team established in 2019.

New EA Techniques Part 8

Impact of EP on Jamming Geometry and Techniques

By Dave Adamy

For the past 10 years, we have been talking about Electronic Protection (EP) in radars piecewise. This month, we will start by listing the EP features of modern hostile radars and relating them to the specific jamming geometries and modulations that we have been discussing over the last few months.

Table 1 is the list of EP techniques first presented in the EW101 column from the May 2010 JED.

Table 1: Electronic Protection Techniques

TECHNIQUE	PROTECT AGAINST
Ultra-low Side Lobes	Radar detection & side-lobe jamming
Side Lobe Cancellation	Side-lobe noise jamming
Side Lobe Blanking	Side-lobe pulse jamming
Anti-Cross Polarization	Cross-polarization jamming
Pulse Compression	Decoys & non-coherent jamming
Monopulse Radar	Many deceptive jamming techniques
Pulse Doppler Radar	Chaff & non-coherent jamming
Leading-Edge Tracking	Range gate pull-off
Dicke-Fix	AGC jamming
Burn-Through Modes	All types of jamming
Frequency Agility	All types of jamming
PRF Jitter	Range-gate pull-in and cover pulses
Home-on-Jam Modes	All types of jamming

IMPACT OF EP ON SELF-PROTECTION JAMMING

The techniques from Table 1 that impact self-protection jamming are:

- Anti-Cross-Polarization
- Pulse Compression
- Monopulse
- Pulse Doppler
- Leading-Edge Tracking
- Dicke-Fix
- Burn-Through Modes
- Frequency Agility
- PRF Jitter
- Home-on-Jam

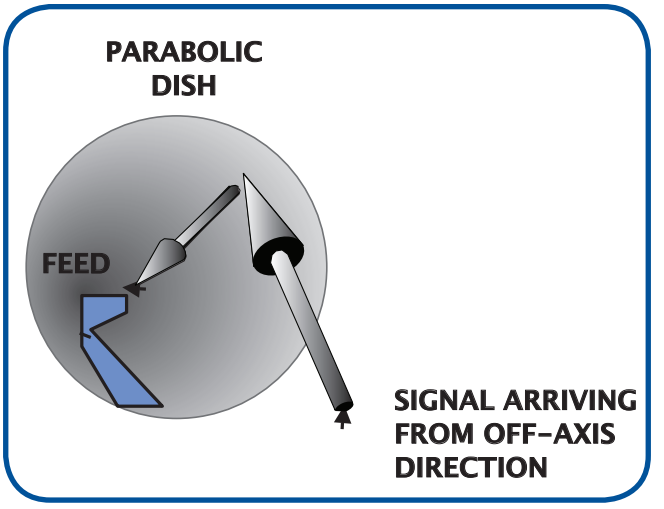


Figure 1. The forward geometry at the edges of a parabolic dish reflector causes off-axis signals to some areas of the dish to change polarization by 90° when reflected into the antenna feed.

CROSS-POLARIZATION JAMMING

Cross-Polarization (Cross-Pol) jamming is a self-protection technique that involves the generation of a cross-polarized jamming signal, which causes a monopulse radar to lose angle track on its intended target. As described in the April 2010 EW101 column, any radar that has forward geometry in its antenna (for example the shape of a parabolic dish reflector) has cross polarized lobes oriented away from the radar's boresight, as shown in **Figure 1**. In this drawing, consider a vertically polarized signal arriving at 45 degrees right of the top near the outside edge of the antenna. The 45-degree orientation of the shape of the dish would cause a reflection with a horizontal polarization. These false lobes, called "Condon Lobes," are also present in flat-plate phased array antennas in which the edge array elements have their amplitude or phase characteristics modified to "sharpen" the beam or reduce its sidelobes. **Figure 2** shows the Condon lobes response to the radar's return signals and also the response to cross-polarized jamming signals. Condon lobes typically have very low gain, so the cross-polarized jamming signal needs to be very strong to be effective (typically 20 to 40 dB stronger than the main beam signal received at the target).

Since long-range, new-generation radars typically have significantly increased maximum engagement elevations, radar signals must pass through much of the atmosphere. This means that the signals will be subject to significant rotation

Priority

Source High-Reliability RF Cables

Available for Same-Day Shipping!

Complete Line of High-Reliability RF Cable Assemblies Shipped Same Day!

Our new portfolio of commercial-off-the-shelf (COTS), high-reliability RF cable assemblies are designed and processed to stand the test of time. These new cables are assembled using J-STD soldering processes and WHMA-A-620 workmanship. Inspection data, test data and material traceability are all included as part of the package. The combination of materials, processing and supporting data work together to create a dependable, fieldable cable assembly for applications where performance over time is critical and the cost of failure is high. Call or visit us at pasternack.com to learn more.

866.727.8376
pasternack.com

PASTERNACK
an INFINITE brand

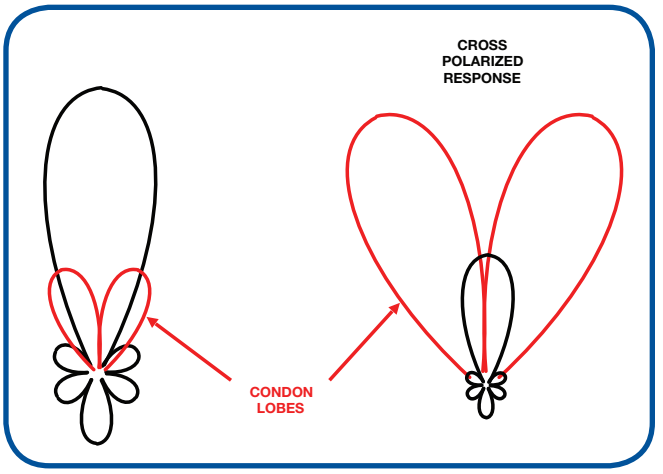


Figure 2. Some radar antennas have cross-polarized lobes oriented away from the co-polarized bore sight.

of the signal's polarization. This is called Faraday rotation. A polarization mismatch between the skin return and the receiving antenna can reduce the received signal by many dB. Therefore, modern long-range radars typically use circular polarization – which is not subject to this loss.

Cross-pol jamming is effective against either linear or circular polarization. For linear polarization, a strong cross-polarized jamming signal (i.e., with polarization 90 degrees away from the radar's transmitted signal) is generated as shown in **Figure 3.** This same jammer configuration will also produce a jamming signal with the sense (right or left circular) reversed. In either case, the jammed radar will steer itself so the target is centered in the Condon lobe. This, of course, causes a significant tracking error.

Another jamming technique, shown in **Figure 4,** time shares the two antennas between the receive and (cross polarized) transmit functions using nanosecond switches. Note that the time-shared receive and transmit waveform would have transitions so fast that the jammed radar could not detect them.

ANTI-CROSS-POL ELECTRONIC PROTECTION

A radar with anti-cross-pol EP has the ability to reduce or eliminate Condon Lobes. This can be accomplished by incorporation of a polarization filter across the whole antenna to eliminate cross-polarized responses. It can also involve design features of the radar's antenna. For example, a flat plate phased array with no beam sharpening features also avoids Condon Lobes.

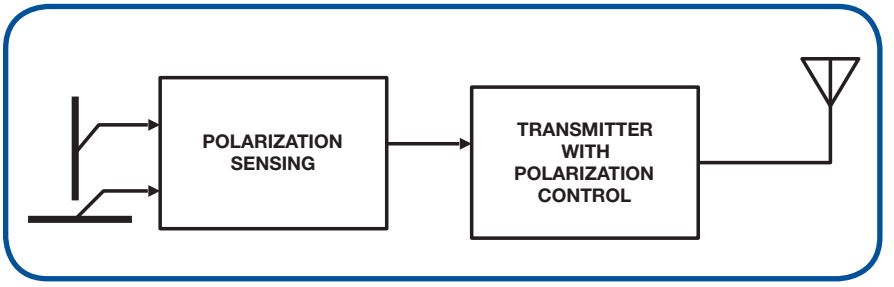


Figure 4. One technique for creating a cross-polarized jamming signal involves sensing the polarization and then generating a return signal with the proper polarization. This requires sharing the antennas between receive and transmit – using nanosecond switches.

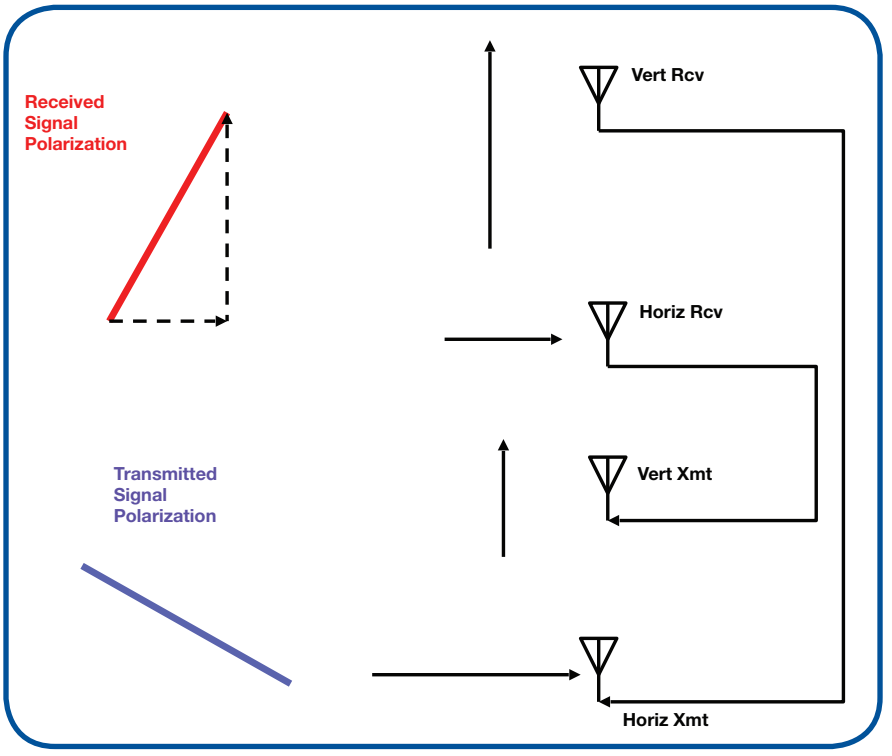


Figure 3. Cross-polarized jamming generates a strong cross-polarized return signal, which causes the radar to track the target in one of its Condon Lobes.

There is an extensive discussion of cross-pol jamming in chapter 4 of volume 3 of *Applied Electronic Countermeasures* (now out of print) by Leroy Van Brunt. Some of them required components which were unavailable at the time the book was published in 1995 but are now within the state of the art.

Anti-cross-pol EP is typically described in terms of "some number of dB of anti-cross-pol protection." This is not clearly described in the literature, but it seems to refer to the amount of isolation between the co-polarized and cross-polarized response of the radar's antenna.

WHAT'S NEXT

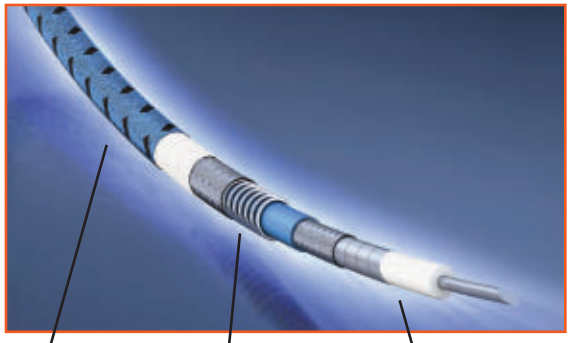
Next month, we will continue our discussion of the impact of Electronic Protection techniques for various jamming geometries and techniques. For your comments and suggestions, Dave Adamy can be reached at dave@lynxpub.com.

When Everything is Important...
the NEW *Clarity™ Series* is the *Clear Choice*

Applications:

Research & Development Labs
VNA Test Port Extension Cables
High Volume Production Test
Bench or Portable Test equipment
RF Module Testing

Industry leading performance, unparalleled value, and stock to 4-week lead times.



Phase stability <3.5º
Guaranteed up to 50,000 flexes
Super-sharp Sure-Grip™ knurl
Ergonomically designed Sure-Grip™ molding

TIMES MICROWAVE SYSTEMS
An Amphenol Company

World Headquarters: 358 Hall Avenue, Wallingford, CT 06492 • Tel: 203-949-8400, 1-800-867-2629 Fax: 203-949-8423
International Sales: 1+ 203 949 8503 • 1+ 800 867 2629
China Sales: TMC Building 4, No. 318 Yuanshan Road, Xinzhuang Industrial Park, Shanghai, China 201108 Tel: 86-21-5176-1209 Fax: 86-21-64424098

www.timesmicrowave.com

The EM Domain is an Integrated Domain

By John Knowles

In the previous installment of the EM Domain series (in the May issue of JED*), we discussed the structure of the Electromagnetic (EM) Domain and the way military forces* use *it,* manage *it and achieve some modest degree of* control *within it. This month, we will look at the way these functional elements interact within the domain.*

As we discussed previously, the major warfighting domains (Air, Land, Sea, Space, Cyberspace and the EM Domain) can be described in three functional layers: users, managers and controllers. At the same time, these are not isolated functions, regardless of the domain. Actions that occur in one functional layer often influence actions or decisions in at least one of the other two. The users and controllers in a domain are constantly maneuvering, and they must observe and/or perform some degree of domain management at the weapons platform level in order to deconflict operations in the battlespace. The management function actively manages the users and controllers to deconflict their actions while also allowing them to perform their roles.

In the Air Domain, for example, the crew of a C-130 flying from the UK to Turkey must be able to maneuver among other air space users (other aircraft) by complying with agreed "rules of the road" (flight altitude, air traffic lanes, etc.) and coordinating their flight with civilian air traffic control centers and military air operations centers (i.e., air domain managers actively monitoring, deconflicting and guiding the domain's many users). In other words, the user is performing part of the management function by complying with the management protocols.

During peacetime, the primary objective for most military aircraft is to facilitate maneuver (fly) while following flight management protocols and air traffic control guidance to mitigate the effects of congestion (other aircraft) in the domain. In a battlespace during a military conflict, however, the Air Domain users must also be able to maneuver while mitigating adversary action (avoiding enemy fighters and surface-to-air missiles, for example). Another factor during wartime is the presence of the friendly air superiority fighters and ground-based air defense systems (the controllers) that determine which aircraft can access the air space in a given area. This control element must comply with the air domain managers and perform the critical role of combat identification in order to avoid engaging friendly aircraft while still performing its mission of denying enemy use of the Air Domain. The point is that while the air operations center is obviously an important aspect of Air Domain's management function, it is not the only piece of air space management; the domain users and the domain controllers must also participate to some degree in the management function of the Air Domain.

MANEUVER IN THE EM DOMAIN

These same basic domain roles and functions hold true in the EM Domain. However, the number of EM Domain users (radios, radars, GNSS systems, EO/IR systems, IFF systems, mobile phone systems, etc.) is much larger, which makes for greater potential congestion in a battlespace. Also, these EM users are transmitting and receiving photonic energy that is traveling at the speed of light (as opposed to a ground vehicle traveling at 50 km/h or a plane flying at Mach 1). This makes the task of managing the users in the EM Domain very challenging, especially as the number of EM Domain users continues to grow. As if this were not already challenging enough, friendly EW systems (EM controllers) are sensing and attempting to deny adversary use of the same EM battlespace. Robust spectrum management is essential in order to prevent EM fratricide between friendly emitters and receivers. Some parts of the spectrum management function are performed through specific frequency allocations to specific users and controllers in a given location for a set period of time. EM maneuver becomes more complicated with the introduction of adversary EW actions, which create contested EM environments in addition to EM congestion. Increasingly, the users are employing cognitive technology to autonomously maneuver to open frequencies.

It's worth noting that EM maneuver is not a widely understood concept. At a basic level, a radar or radio can maneuver in terms of frequency, physical location and time. But this model doesn't depict the complete picture of EM maneuver, according to Jesse Bourque, who has authored several EM Domain articles for *JED*. He explained that EM maneuver is not simply a matter of movement through space. Rather, as depicted in **Figure 1,** an EM system utilizes three

FEATURED LIVE COURSES

SPACE EW

Dave Adamy

Mondays, Wednesdays, & Fridays
13:00 – 16:00 EDT | September 4 – 20, 2019
In the eight sessions of this course, we will cover the nature of EW in space and go on to work practical EW problems appropriate to the space environment.

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

Dr. Clayton Stewart

Mondays, Wednesdays, & Fridays
13:00 – 17:00 EST | February 3 – 21, 2020
This course offers a comprehensive overview of modern electronic (EW) warfare systems, technology, and techniques.

EW Against a New Generation of Threats

Dave Adamy

Mondays, Wednesdays & Fridays
13:00 – 16:00 EDT | April 13 – 29, 2020
This is a practical, hands-on course which covers Spectrum Warfare and current EW approaches, and moves on to discuss the new equipment capabilities and Tactics that are required to meet the new threat challenges.

Airborne Expendables/UAS Capabilities and Potential

Dr. Patrick Ford

Tuesdays & Thursdays
13:00 – 16:00 EDT | October 8 – 17, 2019
This course provides attendees with a strong foundation in expendables/sUAS, from basic airframe classes and capabilities, to EW potential, to the current FAA airframe and pilot certification/flight approval process.

EW Modeling and Simulation

Dave Adamy

Mondays & Wednesdays
13:00 – 16:00 EST | March 2 – 25, 2020
This is a practical course in which the basic concepts and techniques of Electronic Warfare modeling and simulation are presented and applied to practical problems.

Intermediate Electronic Warfare
EW EUROPE 2020

Dr. Clayton Stewart

Friday & Saturday | 08:00 – 17:00 BST
June 19 – 20, 2020 | Liverpool, UK
We will begin with a historical perspective and introduce use of radar, integrated air defense system, early EA functions and conclude with an overview of modern EA, ES, and EP.

= Web Course, no travel required!

AOC INTERNATIONAL SYMPOSIUM & CONVENTION

Fundamental Principles of Electronic Warfare

Dave Adamy
Saturday & Sunday
08:00 – 17:00 EDT | October 26 – 27, 2019

Advanced Principles of Electronic Warfare

Dave Adamy
Thursday & Friday
08:00 – 17:00 EDT | Oct 31 – Nov 1, 2019

Machine Learning for Electronic Warfare

Kyle Davidson
Saturday & Sunday
08:00 – 17:00 EDT | October 26 – 27, 2019

Electronic Countermeasures—Theory and Design

Kyle Davidson
Thursday & Friday
08:00 – 17:00 EDT | Oct 31 – Nov 1, 2019

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

dimensions – detail, space and power– acting over time. For example two radios that are communicating back and forth may utilize various parametric techniques – not only in terms of frequency, but also modulation, different waveforms, polarity, etc. – to communicate. They also use spatial techniques, such as geolocation, radiation patterns and directionality. And they will use power techniques, such as ERP, gain, attenuation, etc., perhaps to operate below the noise floor. These three dimensions will be used together over a temporal dimension that could involve short-duration transmissions or pulsing, for example. When you begin to aggregate this type of EM maneuver from two radios to four or eight or hundreds, and when you apply these types of approaches to radar, GNSS systems and other types of systems, you move beyond the idea of tactical EM maneuver and into the realm of strategic maneuver across the EM Domain.

Another aspect that is also worth considering, explained Bourque, is how different branches of the Armed Services (especially those in the DOD) perceive maneuver in the EM Domain. Based on their different weapons platforms, roles and missions, the Services tend to approach EM maneuver from dissimilar perspectives, as depicted in **Figure 2.** The US Army tends to deploy in large, dense formations and operate out of stationary bases. An Army force comprised of several brigades can contain tens of thousands of emitters. The Navy organizes around carrier strike groups whose ships and submarines are constantly moving. Emissions control is essential for concealing the members of the strike group. For its part, the Air Force tends to operate in widely dispersed formations flying at high speeds over relatively short periods of time on aircraft with a relatively small number of apertures. Special operations forces are small and typically rely on concealment, including their EM signatures.

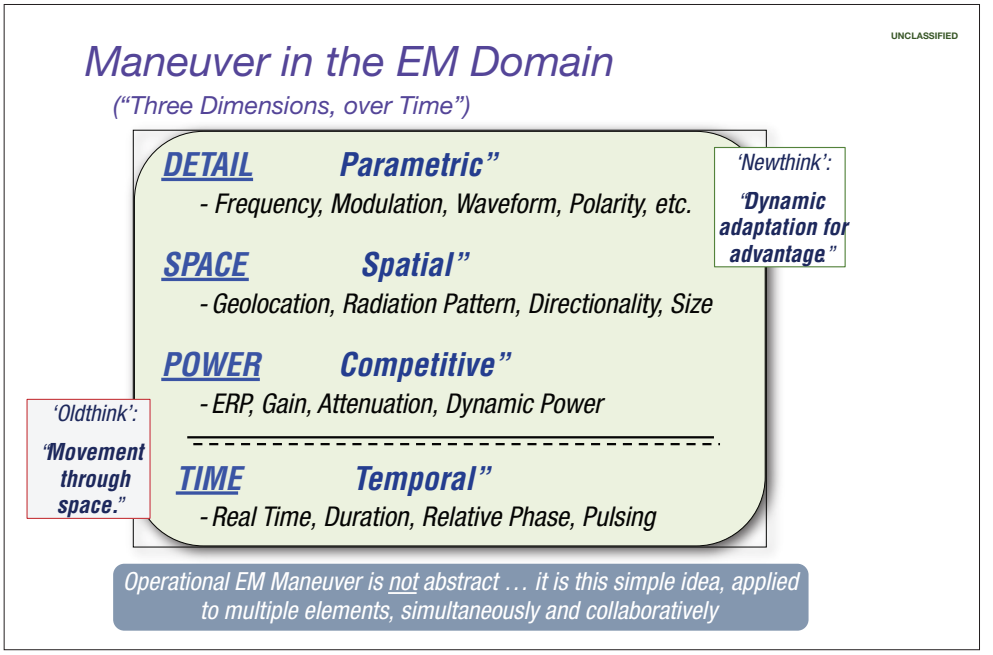


Figure 1: Operational maneuver in the EM Domain JESSE BOURQUE

These differing operational dynamics make it difficult for the Services to approach Joint EM concepts, such as EM Battle Management, with much enthusiasm. Each Service prefers to view EM operational challenges differently and solve these problems according to the perspective of their own Service. The most effective way to resolve this situation is for the OSD, the Joint Staff and the warfighter to step up and "own" responsibility for the EM Domain.

NEXT TIME

Having looked at some of the basic elements of the EM Domain over the past few columns, our next discussion will focus the way we have traditionally viewed the EM Domain and how this perspective is changing.

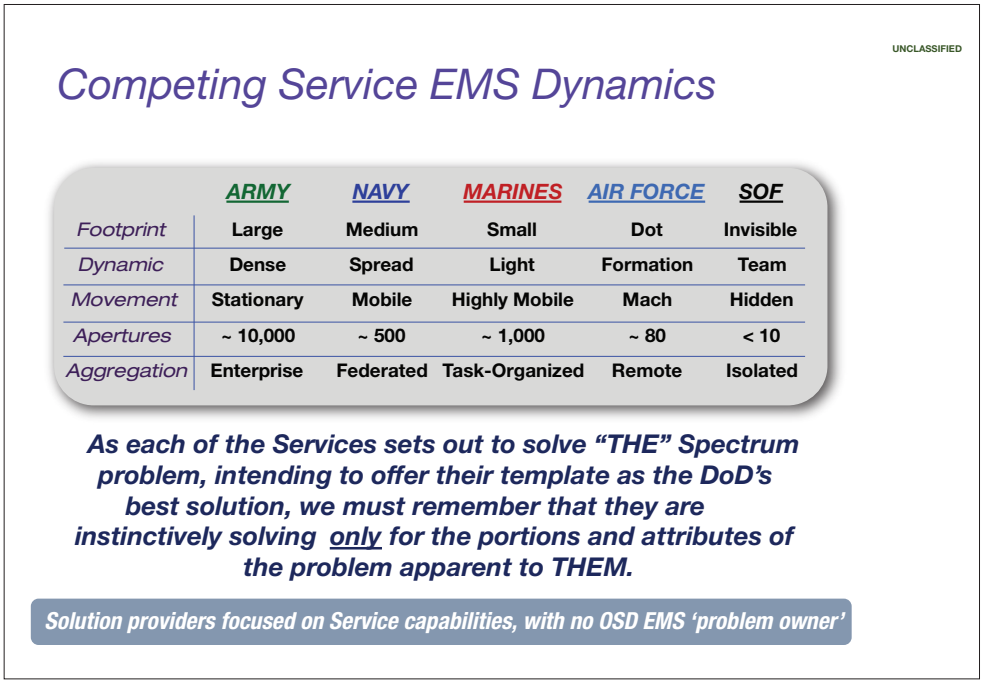


Figure 2: Based on their roles and missions, each of the Services sees the EM Domain differently. JESSE BOURQUE

ASSOCIATION OF OLD CROWS

Electronic Warfare Asia

4-5 February 2020
Marina Bay Sands, Singapore

PART OF

ADECS
ASIA DEFENCE EXPO & CONFERENCE SERIES 2020

REGISTER YOUR INTEREST AT ASIA-DECS.COM

ENABLING ELECTROMAGNETIC OPERATIONS IN THE ASIA PACIFIC REGION

The 4th AOC EW Asia event will consider the future of EW and EM Operations in the changing light of current and emerging threats.

The conference will consist of plenary sessions focusing on operations, defence capability development, and industry inventiveness. The event will bring together delegates from EW, SIGINT, C4ISR, CEMA and related communities.

Interested in speaking? Submit your conference paper on the event website.

Call for papers deadline: 18 October 2019

Silver sponsor

TERMA
ALLIES IN INNOVATION

Produced by

ASSOCIATION OF OLD CROWS

Organised by

CLARION EVENTS

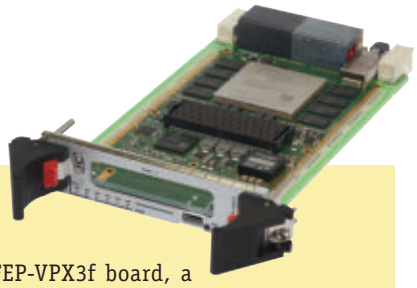
For more information please contact us:

team@asia-decs.com

www.asia-decs.com

ANTI-JAM ANTENNA

NovAtel has expanded its portfolio of GPS Anti-Jam Technology (GAJT®) to include the GAJT-410ML, a low size, weight and power (SWaP) design specifically intended for rapid integration into space-constrained military land applications. This antenna protects GPS-based navigation and precise timing receivers from interference, building on the software of previous, larger models. The GAJT-410ML also offers jammer status and direction finding capabilities when the Power Injector Data Converter (PIDC™) is installed. *NovAtel Inc.; Alberta, Canada; +1 (800) 668-2835; www.novatel.com.*

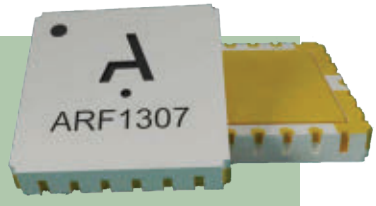


3U VPX BOARD

Interface Concept has released the IC-FEP-VPX3f board, a high-speed, VITA 66.5 compliant 3U VPX board based on the Xilinx Kintex® UltraScale™ FPGA technology. The board is designed for applications requiring intensive signal processing for high-performance embedded computing (HPEC) systems. The IC-FEP-VPX3f offers two DDR4 banks of up to 4GB each and achieves data rates up to 16.3 Gbps, optimized for digital signal processing, packet processing and board transfer performance. *Interface Concept; Quimper, France; +33 (0)2 98 573 030; www.interfaceconcept.com.*

EW TRANSCEIVERS AND TUNERS

FEI-Elcom Tech, Inc. has announced the development of a new EW product line of transceivers and tuners, the EW series VPXTR6000 next-generation microwave quad-channel synthesized transceivers, and the VPXST6000 tuners. Applications include EW, electronic countermeasures (ECM), electronic protection (EP) and SIGINT. This EW series features 2 GHz of bandwidth with a frequency range of 1-18 GHz or 6-18 GHZ, with up to 67 GHz available by special order, and delivers low phase noise and high-speed frequency switching. *FEI-Elcom, Inc.; Northvale, NJ; +1 (201) 767-8030; www.FEI-ElcomTech.com.*



GAN POWER AMPLIFIER

Altum RF has introduced the ARF1307C7 GaN distributed amplifier, intended for use in EW, radar, and test and measurement equipment systems. This amplifier operates within a 2-20 GHz frequency range, and provides 20 dB small signal gain, 10 W saturated output power and 14 dB of power gain. *Altum RF; Eindhoven, The Netherlands; +31 (0) 40 2390 888; www.altumrf.com.*

AMPLIFIER/SPLITTER MODULE

VadaTech has introduced the VPX981, an optical amplifier/splitter module intended for 6U VPX platforms that require signal distribution over fiber. Suitable for high channel count beamforming applications, he VPX981 offers 92 outputs after a signal is received, amplified and split, and matching between outputs within -1 and +1 dB. This module has applications in rugged embedded computing, radar and electronic warfare (EW) systems. *VadaTech, Inc.; Henderson, NV, USA; +1 (702) 896-3337; www.vadatech.com.*

PULSED MICROWAVE POWER MODULE (MPM)

dB Control has released the dB-3774B, a new compact, lightweight pulsed microwave power module (MPM) for EW applications, including radar jamming. Operating in the 6-18 GHz frequency range, the dB-3774B features 1kW peak power at 5% maximum duty cycle, a conduction-cooled mini traveling wave tube (TWT) for power amplification and a solid-state driver amplifier for RF gain. This MPM weighs 18 pounds and measures 7 in. by 3 in. *dB Control; Fremont, CA, USA; +1 (510) 656-2325; www.dbcontrol.com.*

AOC Patriots' Roost and MITRE Host 2019 Resilient Space Conference

With a focus on "Emergent Technologies, Faster Implementation," the Resilient Space Conference 2019 addressed enterprise challenges facing the space EW community today, including space acquisition, commercial and military leadership, and more. Sessions ranged from public releasable to TS/SCI.

The Association of Old Crows Patriots' Roost Chapter and the MITRE Corporation hosted the conference from June 11-13 in Bedford, MA. Sponsored by the Air Force Research Laboratory and Sandia National Laboratories, the conference took place in conjunction with the 11th Fault Tolerant Spaceborne Computing Using New Technologies workshop.

During his keynote address, Dr. Fred Kennedy, director of the Department of Defense's Space Development Agency (SDA), spoke to the need for faster acquisition, delivery and implementation of space capabilities. Currently, the speed at which the US acquires and delivers new space technologies is not sufficient for present or future needs, and Kennedy warned this could become an "Achilles heel" for the US.

Keynote speaker, Lt Gen John F. Thompson, commander, Space and Missile Systems Center and Air Force Program Executive Officer for Space, addressed how the commercial and defense sectors might benefit from working together to better meet the military's needs. According to Thompson, the commercial industry has already invested time and money in the development of space technologies, and the applicability of these

technologies for enhancing defense capabilities should be seriously considered to help enhance effectiveness and superiority against peer competitors.

Other keynote speakers at the conference included Mr. James A Faist, director, Defense Research and Engineering for Advanced Capabilities; Dr. William A Laplante, Mitre senior vice president; Col Eric Felt, commander, Phillips Research Site, and director, AFRL Space Vehicles Directorate, Kirtland AFB; and Col Michael McGinley, director, Defense Innovation Unit Boston.

This year's conference also included a Rohde & Schwarz Technology Tour, sponsored by the Patriots' Roost Chapter and MITRE, which comprised two unclassified seminars presented by Dave Adamy: EW Modeling and Simulation, and Radar EP and Digital RF Memories.

EW Europe 2019 Conference Highlights

The AOC Electronic Warfare Europe 2019 conference took place from May 13-15 in Stockholm, Sweden, and addressed what industry and defense leaders need to do in order to promote and ensure success in electronic warfare and signals intelligence.

In his opening address to kick off the conference, Johan Falk, head of the Communications EW Systems Department, Swedish Defence Research Agency (FOI), spoke to the need to the development of EW systems that are made to be upgraded. The EW community faces challenges in speed of acquisition and implementation, but there is also a need for more streamlined upgrades to technologies already in theater.

According to Falk, EW systems should be built, from the beginning stages of research and development, with future improvements and problem-solving in mind. In practical terms, Falk said EW systems should be as simple to upgrade as a phone or personal computer to ensure new capabilities can be readily developed and applied as defense requirements evolve.

In addition to the advancements needed in EW systems development and implementation, the conference offered an opportunity to address the need for continued and consistent EW systems training. As new systems are developed and introduced to the warfighter, and as older systems are upgraded to meet modern demands, EW training is a crucial component to ensuring readiness and superiority in the EMS.

Capt (A) Lars-Åke Siggelin, electronic warfare officer, Swedish Air Force, spoke about the Swedish Air Force's "EW Training for Pilots" (EW TFP) program. According to Siggelin, the EW TFP program includes practical live exercises to train pilots in responding to chaff and jamming by aggressors.

For the tenth year, the conference included the Plath Intelligence Workshop, a one-day conference Plath calls, "A platform that brings together users as well as providers of COMINT technology and provides the opportunity for open discussions."

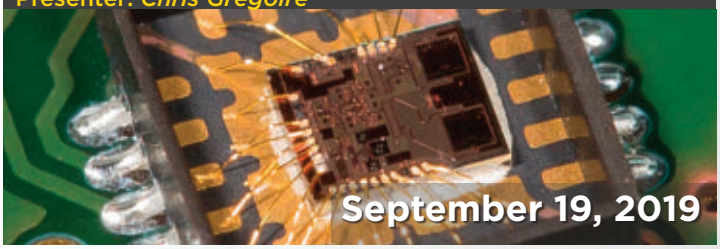
This year's conference saw the largest attendance to date, with 2,603 participants from 46 counties, including military, government, public sector, academia and industry. EW Europe 2020 will take place in Liverpool, UK in June 2020.

AOC Virtual Series Webinars

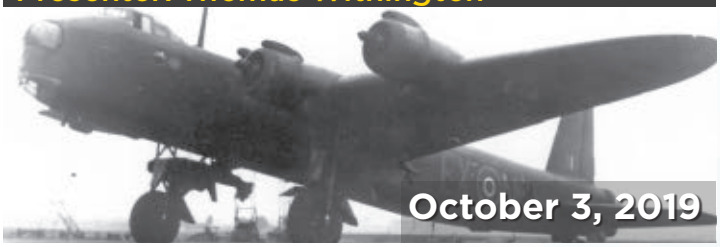
AOC Virtual Series has been a tremendous asset providing the AOC's audience with learning, advocacy, and the exchange of information. Register today to hear from subject-matter experts on all things EW!

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

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



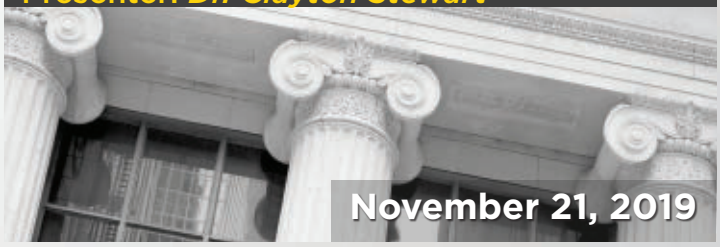
RAF 100 Group and its EW Legacy
Presenter: *Thomas Withington*



The 3 Pillars of Electronic Warfare - Electronic Attack
Presenter: *Brian Hinkley*

The 3 Pillars of Electronic Warfare - Electronic Support
Presenter: *Brian Moore*

The 3 Pillars of Electronic Warfare - Electronic Protect
Presenter: *Dr. Clayton Stewart*



Electronic Warfare Modeling and Simulation
Presenter: *Dave Adamy*

Infrared Countermeasures: A Heated Topic
Presenter: *Dr. Clayton Stewart*

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

ASSOCIATION OF OLD CROWS

AOC 2019 ELECTION RESULTS

The AOC is excited to announce the results of the 2019 Board of Directors elections! As an AOC member, you decide the future of this organization every time you participate in elections.

Thank you to everyone who voted!

Total number of eligible voters – 12,323
Total members voted – 1,357
Percentage of Voters – 11.01%

PRESIDENT ELECT – 3 CANDIDATES
Glenn "Powder" Carlson – 36.48 %
2nd Place – 30.14 %
3rd Place – 26.46 %

AT-LARGE DIRECTOR – 8 CANDIDATES – Only two could be selected
Brian Hinkley – 28.81 %
Haruko Kawahigashi – 28.51 %
3rd Place – 27.70%
4th Place – 27.45%
5th Place – 21.59%

PACIFIC REGION – 2 candidates
Rick Lu – 51.49 %
Vince Battaglia

INTERNATIONAL REGION I – 1 candidate
Sue Robertson

ASSOCIATION OF OLD CROWS

10TH ANNUAL EW/CYBER CONVERGENCE CONFERENCE

The AOC Palmetto Roost Chapter hosted their 10th Annual classified Electronic Warfare/Cyber Convergence Conference June 4-6, 2019 at Naval Information Warfare Center (NIWC) Atlantic on the Naval Weapons Station, Charleston, South Carolina.

Major General Jennifer Napper, USA (ret.) former Director of Policy, Plans and Partnerships for USCYBERCOM; Colonel Craig Harm, USAF (ret.), AOC Appointed Director; and Executive Officer, Commander Jeffrey Williams, NIWC Atlantic, welcomed the more than 180 military members, government employees and contractors in attendance.

This year's theme was "New Technology and Methodologies for Mission Assurance in EW/Cyberwarfare." Master of Ceremonies Rear Admiral Gary Durante, PhD, facilitated sessions that categorized operational concepts of combining EW capabilities with cyber warfare tactics, techniques and procedures, and enabling the rapid deployment of new and improved capabilities.

Keynote speakers included Captain Ed Grohe, Commanding Officer, Information Warfare Training Group Norfolk; Captain Brian Luke, Commanding Officer, Navy Cyber Warfare Development Group; and Colonel Peter Reddy, USMC (ret.) Deputy Executive Director, NIWC Atlantic, announcing the SPAWAR name-change to Naval Information Warfare Systems Command (NAVWAR) as they align their identity with their mission.

Speakers were also present from the National Reconnaissance Office (NRO), Defense Advanced Research Projects Agency (DARPA), Air Force Cryptologic Office, U.S. Fleet Cyber Command/U.S. 10th Fleet, Office of Naval Intelligence (ONI), Central Intelligence Agency (CIA), South Carolina Army National Guard (SCARNG) and the National Security Agency (NSA).

This classified forum provides a unique opportunity for members to communicate and collaborate on a much higher level without any perceived organizational barriers. This environment, combined with a focus on operations and technology, provides a catalyst for operational forces, acquisition agencies, and engineering service-providers to discuss issues encountered and the understanding of how to resolve them. Throughout this conference series, such collaboration has yielded much-needed capabilities that would not have come to fruition without this event. The event is making significant impacts for NIWC, the EW/Cyber industry, National Security and, most importantly, for the warfighter.

The Palmetto Roost announced the establishment of the Rosemary Wenchel Memorial Scholarship at Charleston Southern University (CSU) to support a female student enrolled in the Bachelor of Science in Cybersecurity program at CSU. Mrs. Wenchel was a leader, mentor and friend to many, and the Palmetto Roost endeavors to honor her legacy.

At the event, Governor Henry McMaster of South Carolina proclaimed June 3-7, 2019 "Cyber/Electronic Warfare Convergence Week" throughout the state and encouraged all to recognize the importance of the continued collaboration between cyber and electronic warfare communities to address the changing dynamics of the digital age.

A special thanks to the conference sponsors! Title Sponsor: Scientific Research Corporation (SRC); Platinum Sponsors: Norseman Defense Technologies and SAIC; Gold Sponsor: BAE Systems; Silver Sponsors: COLSA Corporation and Motorola Solutions; and Bronze Sponsors: Sentar, D-TA Systems and Boeing.

Sixth International Conference on Electronic Warfare

17 - 20 FEBRUARY 2020

ASSOCIATION OF OLD CROWS

"EW : COLLABORATE FOR SUCCESS"

17 Feb 2020 : Pre-Conference Tutorials, 18 - 20 February 2020 : Conference and Technical Exhibition

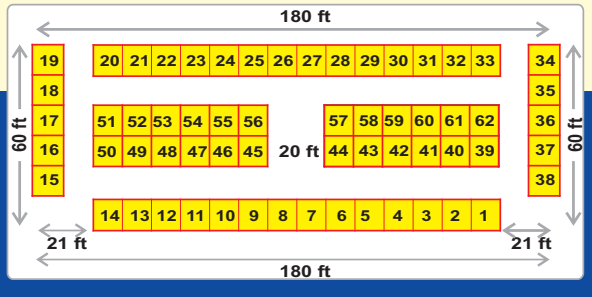
The Sixth EW International Conference India (EWCI 2020) The Sixth International Conference on Electronic Warfare (**EWCI 2020**) is the latest event in the internationally acclaimed EWCI Conference Series in India, in the field of Electronic Warfare and related areas. The Conference is being organised by the much Awarded India Chapter of Association of Old Crows (AOC), Bangalore. The Conference has the active support of Defence Research and Development Organisation (DRDO), Government of India, Ministry of Defence and the Defence Public Sector Unit (DPSU), Bharat Electronics Limited (BEL), Bangalore. The Conference is envisaged to be of great use for Modern Armed Forces, Military Planners, Developers, Procurers, Testers, Trainers and Vendors of the latest EW Technologies and Systems. Past Conferences in the Series attracted large delegations from Indian Armed Services, DRDO, Defence PSUs, National and International EW Professionals. A large scale Indoor Exhibition will accompany the Conference, displaying the latest EW Products from International EW Organisations. There will be an intense one-day Pre-Conference Tutorials preceding the Conference. The Conference is visualised to be an important platform for EW Professionals who would share the Research and Development output in the field of EW at the global level. Hence, the theme of the Conference is chosen as "**EW : COLLABORATE FOR SUCCESS**".

Papers with deep Research Contents invited in EW/IO and related areas including following Topics :

- Advances in EW Systems, Architectures, Techniques and Technologies
- EW Systems Modelling and Simulation
- EW & EO Threat Simulators, Testing & Evaluation
- Advances in ECM / ECCM Techniques, Expendable Repeater and IR Jammers
- Electro-Optic based EW Systems - Missile Approach Warning Systems & Laser Warning Systems
- Network Centric & Information Warfare, EW Cyber
- EW Antennas, Active Electronically Scanned Arrays (AESA) and Shared Apertures
- Radar Finger Printing, LPI Emitters Techniques for Interception and Countermeasures
- Communication DF Receivers, Digital Receivers, EW Signal Processors, Satellite Based EW Challenges
- SIGINT, RWR, ESM, Multi Sensor Warner, Directed Energy Microwave and Millimeter Wave Technology for EW
- Light Weight EW Systems for UAV, Aerostat & Other Platforms
- Emitter Location Algorithms, Program Management of Complex EW Systems
- EW Interference to TV/Radio/Mobile Transmissions and their Maintenance
- EW Ops & Spectrum Management in Joint Services Operation Scenario and Challenges
- Operation Flight Programs and Airborne EW Software and their Verification and Validation
- IED Detection, EW for Counter Terrorism Operations and Low Intensity Warfare

EWCI 2020 Sponsorship (See our Web Site for more details)

Exhibition Sponsorship	Indian (INR) + 18% GST	Foreign (USD)	Free Benefits as part of Sponsorship
Diamond	8,50,000	20,000	3 Booths, 8 Delegates
Gold	6,50,000	15,000	2 Booths, 6 Delegates
Silver	5,50,000	13,000	2 Booths, 4 Delegates
Bronze	3,00,000	8,000	1 Booth, 2 Delegates
Booth	1,50,000	4,000	1 Booth
Delegation Kit	5,00,000	12,500	4 Delegates
Dinner	3,50,000	10,000	3 Delegates
Lunch on Day 1or 2 or 3 or 4	2,50,000	7,000	2 Delegates



EWCI 2020 Schedule (See our Web Site for more details)

Date	Activity
01 July 2019	First Announcement of the Conference
01 August 2019	Start date to receive Abstracts/Summary of Technical Papers (1000 Words)
15 September 2019	Acceptance of Abstract
15 October 2019	Last date to submit Full Technical Paper
30 October 2019	Intimation of Final Acceptance of the Technical Paper
31 December 2019	End date for Submission of Final Paper, Delegates & Authors Registration
01 August 2019	Start date for booking Exhibition Booths, Sponsorship & Advertisements
30 November 2019	End date for Early Bird Registration of Delegates for Concessional Fees
31 December 2019	End date for Sponsorship/Booth Fee Payment

Registration Fee	Indian (INR) +18% GST	Foreign USD
Tutorial	Rs 5,500	$ 300
Conference	Rs 14,000	$ 500

FOR MORE DETAILS PLEASE VISIT OUR WEBSITE OR CONTACT

Conference Coordinator

414, Church #Street, New Thippasandra, HAL III Stage, Bangalore -560075

Tele Fax: +91 80 2528 7813, Mobile: +91 9742218140 Email : ewci@aoc-india.org

Web : www.aoc-india.org

AOC Industry and Institute/University Members

SUSTAINING

BAE Systems
The Boeing Company
CACI
Collins Aerospace
DRS Defense Solutions
Electronic Warfare Associates
General Atomics
General Dynamics
Keysight Technologies
L-3 Harris
Leonardo MW Ltd.
Lockheed Martin Mission Systems and Training (MST)
Mercury Systems
Raytheon Company
Rohde & Schwarz USA
Saab

MILITARY UNITS

30 Cdo IX Gp RM
51 Sqn, Royal Air Force
57 IS/DOD
Air Command Denmark
French Air Force EW Unit
Helicopter Wing 53
Japan Air Self-Defense Force
NIWTG SD
Osan AB 25 FS
Zentrum Elektronischer Kampf Fliegende Waffensysteme

INSTITUTES/UNIVERSITIES

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

GOVERNMENT GROUPS

Defence Science & Technology Agency (DSTA)
SAGE

GROUPS

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

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

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

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

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

JED Sales Offices

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

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

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

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

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

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

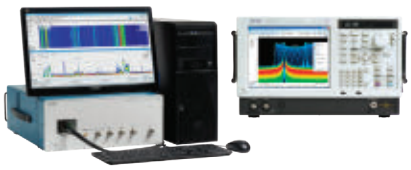
NAYLOR (Canada) Inc.
200 – 1200 Portage Ave.
Winnipeg, MB R3G 0T5 Canada
Toll Free (US): (800) 665-2456
Fax: +1 (204) 947-2047

Index of advertisers

FAILURE IS NOT AN OPTION

Tektronix co-founder Howard Vollum, along with British and American engineers, developed a revolutionary, high-resolution radar system during WWII. Since then, Tektronix has been innovating in both the time and frequency domains. We've created advanced acquisition and simulation technology with bandwidths up to 70 GHz, utilizing the industry's most advanced measurement trigger systems.

With the innovative suite of products that make up Tektronix closed-loop systems, you won't risk costly failures. Be confident your countermeasures will be effective in the most complex environments.



RSA5000/7100

Real-Time Spectrum Analysis

26 GHz with up to 800 MHz BW and two hours recording time

AWG5200/70000

High-Fidelity Arbitrary Waveform Generation

Up to 50 GS/s, fast waveform switching

MIXED-DOMAIN, MIXED-SIGNAL & DIGITAL STORAGE OSCILLOSCOPES

Next-Generation Oscilloscopes

Up to 70 GHz bandwidth

Time- and frequency-correlated measurements

For more information on these innovative solutions, visit **tek.com/mil-gov**

Tektronix®

Detection, response, and recovery where it counts

Protection against cyber and electronic warfare threats in the modern battle space is constantly evolving. BAE Systems is pioneering Resilience-in-Depth™ solutions that integrate reliable detection of cyber intrusions with timely response and recovery to increase platform survivability and to protect our warfighters.

baesystems.com/cyberresilience

BAE SYSTEMS