AUGUST 2014

Military & Aerospace Electronics®

ENABLING TECHNOLOGIES FOR NATIONAL DEFENSE

The future of HPEC

High-performance embedded computing is taking over in compute-intensive applications. **PAGE 18**

Rugged laptop computers

Aerospace and defense organizations rely heavily on rugged laptop computers. **PAGE 24**

militaryaerospace.com

Integrating electronic warfare

EW to join spectrum of military operations

PAGE 8

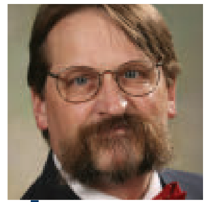
PennWell®

AUGUST 2014
VOL. 25, NO. 8

Military & Aerospace Electronics

MILITARY & AEROSPACE ELECTRONICS ©2014 (ISSN-1046-9079) is published monthly by PennWell Corp.,1421 S. Sheridan, Tulsa, OK 74112. Periodicals postage paid at Tulsa, OK 74101 and additional mailing offices. Editorial offices are located at 98 Spit Brook Road, Nashua, NH 03062-5737. Subscription Prices: Free to qualified subscribers in North America. Other subscribers in U.S.A: $175.00 one year; $309.00 two years; $440.00 three years. Other subscribers in Canada: $270.00 one year; $465.00 two years; $600.00 three years. All other international: $325.00 one year; $620.00 two years; $810.00 three years. Digital edition $70.00 yr. Call (847) 763-9540 for subscription information. We make portions of our subscriber list available to carefully screened companies that offer products and services that may be important for your work. If you do not want to receive those offers and/or information, please let us know by contacting us at List Services, Military & Aerospace Electronics, 98 Spit Brook Road, Nashua, NH 03062. **POSTMASTER:** Send change of address form to *MILITARY & AEROSPACE ELECTRONICS Subscription Services*, PO Box 3425, Northbrook, IL 60065. All rights reserved. No material may be reprinted without permission from the publisher. Back issues of Military & Aerospace electronics may be purchased at a cost of $16.00 each in the U.S., $22.00 Canada, and $27.00 elsewhere. **RETURN UNDELIVERABLE CANADIAN ADDRESSES TO:** P.O. Box 122, Niagara Falls, ON L2E 6S4. **Printed in the USA / GST NO. 126813153 / Publications Mail Agreement No. 875376**

BY **JOHN KELLER**, EDITOR IN CHIEF



A potential technological over-reaction to the shoot-down of Malaysia 17

The tragedy surrounding downed Malaysia Airlines Flight 17 keeps getting stranger and stranger, with accusations flying freely yet no real information on who is at fault.

Last month, the Malaysia Boeing 777 jumbo jet cruising at 33,000 feet en-route from Amsterdam to Kuala Lumpur was shot down over contested territory in Eastern Ukraine by a version of a Russian-designed SA-17 surface-to-air missile fired from a Buk launcher. All 295 aboard the stricken jet were killed.

Still no word about who was responsible. The Ukrainian government blames Russian-backed separatists engaged in civil in Eastern Ukraine for the shoot-down, the separatists are blaming the Ukrainian government, and everyone seems to be casting a wary look in the direction of Russia to place at least some of the responsibility for the aviation disaster.

With the incident nearly a month old now, we're deep in the throes of international reaction to the disaster. There's controversy over who has the aircraft black boxes that might shed light on the disaster. Pundits are all over the story, and everyone is having his or her say. One aspect of the disaster's aftermath that worries me, however, are calls to require sophisticated missile-defense systems for civil jetliners of the type found on military aircraft. I'm all for keeping civilian airline passengers safe from threats that be directed their way from the ground, but such a requirement for missile defenses aboard civilian jetliners would be an over-reaction that could place a heavy financial and technological burden on air carriers and airline passengers.

Airline travel today is expensive. Air carriers are hard pressed to keep their aircraft in safe working order as it is while keeping ticket prices affordable enough to keep their airplane cabins filled. Add the costs of buying, installing, testing, certifying, and maintaining missile-defense systems to the mix and who knows how high the price of an airline ticket might go. Even with missile defenses on board, there is no guarantee that a commercial jetliner could defeat a surface-to-air missile. Aircraft missile defenses often require not only quick detection and countermeasures deployment at just the right time, but also can require the pilot to take sometimes-violent evasive action to ensure the missile doesn't hit its mark.

Are civil airlines and their pilots really up to this kind financial and technological challenge? Seriously, wouldn't it be safer and far less expensive simply to fly over safe areas where the threat of ground-to-air missiles is practically non existent? I question the wisdom of the crew for flying over a known war zone.

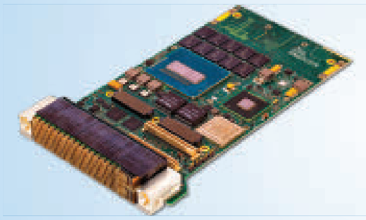
Then there's the question of technology. There essentially are two kinds of anti-aircraft missiles, those with radar guidance, and those with heat-seeking infrared guidance. If airlines are to go down the road of installing missile-defense systems on their airliners, then these systems would have to be able to defend against both. That means installing systems that are expensive and large enough to take away passenger and cargo space. That cuts directly into profits, not to mention the expenses of certifying and maintaining missile-defense systems, as well as training air crews to use them properly.

Radar-guided missiles like the Buk-launched SA-17 that allegedly downed Malaysia 17 represent a different threat altogether. Defending against these missiles can involve deploying chaff—essentially pieces of aluminum foil—to confuse the missile's radar. It also can involve sophisticated electronic warfare capability to jam the missile's radar transmitter.

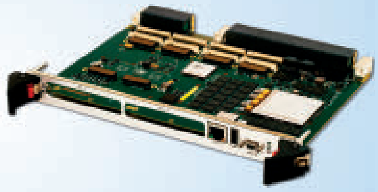
It's all complicated and expensive, and I don't know if it's a job for the world's commercial airlines. My recommendation is to avoid over-reacting in a way that would overburden commercial air carriers.

Module and System-Level Solutions from X-ES

Intel® and Freescale™ Single Board Computers

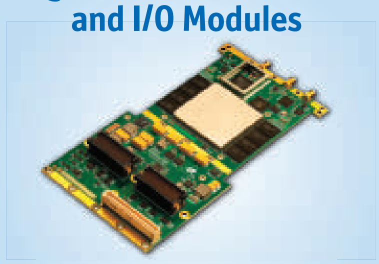


XPedite7570
4th Gen Intel® Core™ i7-based 3U VPX SBC with XMC/PMC



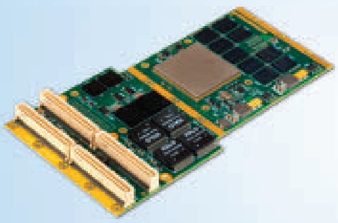
XCalibur1840
Freescale QorIQ T4240-based 6U VPX SBC with dual XMC/PMC

High-Performance FPGA and I/O Modules

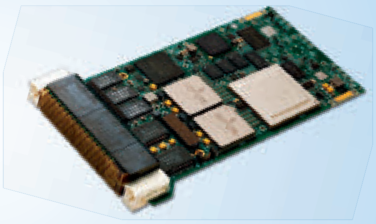


XPedite2400
Xilinx Virtex-7 FPGA-based XMC with high-throughput DAC

Secure Ethernet Switches and IP Routers



XPedite5205
Secure Gigabit Ethernet router XMC utilizing **Cisco™ IOS®**



XChange3018
3U VPX 10 Gigabit Ethernet managed switch and router

High-Capacity Power Supplies

XPm2220
3U VPX 300W power supply with EMI filtering for MIL-STD-704 & 1275

Rugged, SWaP-Optimized, COTS-Based Systems

XPand4200
Sub-½ ATR, 6x 3U VPX slot system with removable SSDs

XPand6200
SFF 2x 3U VPX system with removable SSD and integrated power supply

XPand6000
SFF Intel® Core™ i7 or Freescale QorIQ-based system with XMC/PMC

X-ES

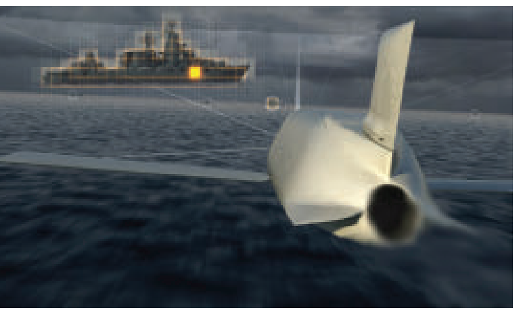
Extreme Engineering Solutions
608.833.1155 www.xes-inc.com

MADE IN USA Designed, manufactured, and supported in the USA

Lockheed to prepare new anti-ship missile for 2017 acquisition

BY JOHN KELLER

ARLINGTON, Va.—Researchers are asking Lockheed Martin to prepare an experimental anti-ship missile for the U.S. Navy F/A-18E/F Super Hornet fighter bomber and U.S. Air Force B-1B Lancer supersonic bomber.



The Lockheed Martin project to design an advanced anti-ship missile is set to enter production in 2017 after the Navy takes over the program from DARPA.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., are awarding a potential $200 million contract to Lockheed Martin Missiles and Fire Control in Orlando, Fla., for the Long Range Anti-Ship Missile (LRASM) Accelerated Acquisition program. The program calls for LRASM munitions that can be launched from the carrier-based Super Hornet jet and land-based Lancer bomber. DARPA is releasing $33 million immediately for Lockheed Martin to prepare LRASM for acquisition in 2017. The program is scheduled to switch from DARPA to the Navy by 2016.

The LRASM will use on-board targeting systems to acquire the target independently without the presence of prior, precision intelligence, or supporting services like Global Positioning Satellite navigation and data-links. The missile will be designed with advanced counter-countermeasures to evade hostile active defense systems.

DARPA is asking Lockheed Martin to mature LRASM systems and technology in preparation for completing the LRASM demonstration phase and move the weapon system into production. Lockheed Martin will continue developing the LRASM long-range targeting sensor, as well as the long-range sensor algorithms and software for advanced LRASM capability against specific high-priority targets in densely spaced groups of surface ships.

Company missile experts will work on the LRASM missile-control unit to optimize processor throughput margin and address hardware obsolescence. Lockheed Martin also will refine the LRASM electro-optical terminal target sensor hardware software to demonstrate the missile's ability in poor visibility. After that, Lockheed Martin engineers will work on missile autonomy, an

Lockheed Martin is in charge of overall development, and the BAE Systems Electronic Systems segment in Nashua, N.H., is developing the LRASM onboard sensor systems.

IN BRIEF

World needs 36,770 new passenger jets over next two decades

Global demand for commercial passenger aircraft will be 36,770 new airplanes over the next 20 years' worth $5.2 trillion, say analysts at Boeing in Seattle. In the single-aisle market, which includes the Boeing 737 and Airbus A320, a total of 25,680 new airplanes will be needed, making up 70 percent of the total units in the forecast. In the twin-aisle widebody jet aircraft market, Boeing forecasts 8,600 new airplanes will be needed, led by small widebody airplanes in the 200- to 300-seat range such as the Boeing 787-8 and 787-9 Dreamliner.

NETCENTS-2 Application contractors to share $960 million in IT

U.S. Air Force information technology (IT) experts are choosing 10 companies to compete for a decade's worth of IT services contracts as part of the Network-Centric Solutions-2 (NETCENTS-2) Application Services program. The 10 companies will compete for $960 million over the next 10 years to provide IT services such as sustainment, migration, integration, training, help desk support, testing and operational support.

DARPA HERMES to defeat RF jamming with low-power wideband signals

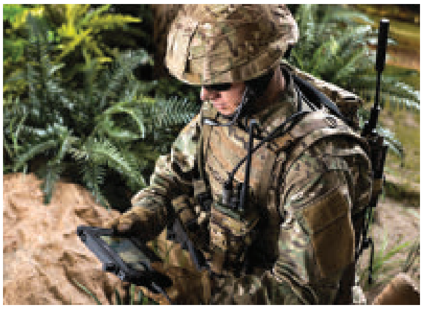
BY JOHN KELLER

ARLINGTON, Va.—U.S. military researchers are trying to find ways to use wideband low-power RF and microwave signals to mitigate the effects of RF jamming and interference that threaten to disrupt important military operations.

U.S. Defense Advanced Research Projects Agency (DARPA) officials in Arlington, Va., are launching the Hyper-wideband Enabled RF Messaging (HERMES) program to ensure reliable radio communications. The HERMES program seeks develop advanced microsystems and techniques for jam-resistant radio frequency (RF) communications that enable wide instantaneous-bandwidth waveforms, large coding gains, and adaptive filtering to operate through jamming and interference. To do this, researchers seek to keep the transmitted power spectral density of the RF signal to a minimum as a way to mitigate signal fratricide while assuring communications in congested RF environments.

Assured access to the RF portion of the electromagnetic spectrum is critical to communications, radar sensing, command and control, time transfer, and geo-location, DARPA officials say. Radio frequencies have the unique combination of all-weather penetration and low atmospheric absorption for long-distance links. Nevertheless, access to radio frequencies can be easily denied, and the root of this problem lies in economics, officials say. The last 20 years have seen growth in demand for voice and data access for cell phones, tablet computers, and other mobile devices. As a result, more frequency bands have been reallocated to commercial use, which reduces and fragments the RF spectrum available to the military.

Only 1.4 percent of the RF spectrum from 0 to 300 GHz is available exclusively to the U.S. government, and forcing the military and other government agencies to use such a small slice of the spectrum can result in signal fratricide—or government radio transmissions interfer-



DARPA is considering wideband low-power RF signals to defeat enemy attempts to jam and disrupt military wireless data communications.

ing with one another.

Malicious jamming is a growing problem. It's relatively easy for adversaries to target such a small part of the RF spectrum allocated exclusively to the government. What this means is that researchers need to develop RF data technologies to reclaim this lost bandwidth without unintentionally jamming others. DARPA officials intend to do this by exploring extremely wideband RF links in the HERMES program.

By using wideband signals in the presence of narrow-band jamming and interference, the idea is that wideband transmissions will enable an acceptable amount of signal to get through for voice and data communications. Interference can be mitigated through coding gain using techniques such as direct sequence spread spectrum, DARPA officials say. Wideband operation can provide a significant coding gain while also providing useful data-rates.

The physics of high-power amplifiers tends to stifle attempts at delivering high-power jamming signals with large fractional bandwidth. The receiver can reject in-band spectrum as wide as 1 GHz while receiving 90 percent of the signal. This enables good data-rates while maintaining ultra-low power spectral densities to mitigate interference with conventional narrow-band systems.

The goal of the HERMES program is to develop a spread-spectrum link with 10 GHz of instantaneous bandwidth with coding gain greater than 40 decibels and the ability to reject large blocks of spectrum at the receiver with minimal impact to signal integrity. Between these two effects, the objective is to achieve greater than 70 dB of jammer suppression. ←

EMAIL QUESTIONS TO
DARPA-BAA-14-34@darpa.mil.

Electronic warfare to be part of all military operations

New threats and technologies are giving rise to terms like spectrum warfare that seek to blend electronic warfare, cyber warfare, and other technological approaches to controlling the RF spectrum.

BY **J.R. Wilson**

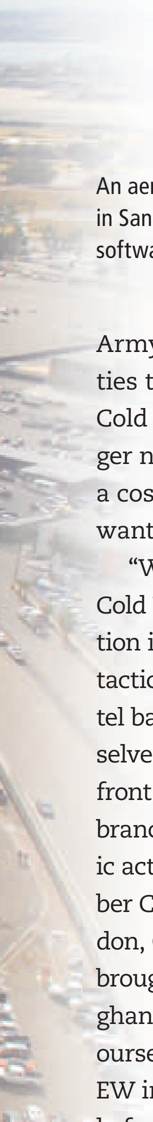
Electronic Warfare (EW) became an integral support component to more traditional warfare—offensive and defensive—in the late 20th Century. In 1973, having watched Israel jam Syrian guided missiles during the Yom Kippur War, a Soviet admiral summed it up succinctly: "The next war will be won by the side that best exploits the electromagnetic spectrum."

EW took on new dimensions and importance in post-9/11 Southwest Asia, where the enemy used electronic means to detonate their weapon of choice—improvised explosive devices (IEDs). The U.S. and its allies sought to combat those low-tech, but deadly, attacks with the components and capabilities arising from a technology boom that changed all aspects of warfare.

With the drawdown in Southwest Asia and the planned Pacific Pivot, EW now is entering yet another new stage of development, requirements and importance. Andrew Dunn, vice president of business development for Integrated and electronic warfare for Exelis Electronic Systems Division, calls it a "whole new mindset" for the U.S. military as the U.S. Department of Defense (DOD) shifts its focus to an area where uncontested access to the electromagnetic spectrum and physical battlespace may no longer exist. Instead, U.S. and allied forces must be ready to deal with near-peer anti-access/area denial (A2/AD) environments and a greater emphasis on the air-sea battle.

The fight against IEDs

In Southwest Asia, the Army and Marine Corps bore the brunt of low-tech attacks on the fringe of EW. That was especially true with the



An aerial view of the Space and Naval Warfare Systems Command (SPAWAR) headquarters in San Diego. SPAWAR is the Navy's technical lead for C4ISR, providing the hardware and software to connect sailors at sea, on land and in the air. (U.S. Navy photo)

Army, as the internal EW capabilities they had developed during the Cold War were determined no longer necessary. It would prove to be a costly mistake the Army does not want to repeat—but fears it may.

"When the USSR fell and the Cold War ended, all the organization in the U.S. Army dedicated to tactical jamming in combat EW intel battalions went away, leaving ourselves pretty vulnerable on the EW front," says Col. Rob Murray, outgoing branch chief for cyber electromagnetic activities (CEMA) at the Army Cyber Center of Excellence at Fort Gordon, Ga. "With the new challenges brought on by 9/11, going into Afghanistan and then Iraq, we found ourselves with no one responsible for EW in the Army. The enemy quickly found that seam and ways to exploit it. IEDs at first were pretty easy to spot, then they started burying the explosives and lines to them—command-detonated by hidden observers. Every time we developed a counter to what they were doing, they kept moving to new approaches."

CEMA Deputy Branch chief Matt Cullen said the insurgents' move to radio-controlled IEDs escalated the U.S. and allied death toll: "Our challenge was to 'reinvigorate' EW as the means to counter, combat and defeat RC IEDs." The Army turned for help to the U.S. Navy, which had become DOD's lead agent for EW, but it was far from a perfect solution because the EW requirements of a ground force differ from those of the Air Force and Navy.

"The Navy has a lot of its EW capability on airplanes flying off carriers and they don't turn that capability on until they are a couple of hundred miles away, so the possibility of those systems causing problems on the ship are minimal. Ships have their own EW defenses against missiles, of course, but when a missile is coming, they don't care what disruptions there may be," Cullen explains.

"But the Army has jammers in the middle of convoys in the middle of bad-guy territory—and when those jammers are turned on, they also disrupt our communications on the ground," Cullen continues. "Early in the war, the Army was buying jammers from the Air Force and Navy and support from those service's EW officers, but what they didn't understand was the jammers also disrupted our soldiers' communications."

CEMA's three pillars of EW are:

1. electronic attack;
2. electronic support—what frequencies and technologies do friendly forces use to defeat the enemy; and
3. electronic protection—keeping U.S. and friendly forces safe from fratricide and enemy EW

"The artillery guys—such as Col. Murray—take that very seriously regarding mortars. They figure out problems during planning. The same has to be done with jammers," Cullen explains. Military forces have important RF frequencies that are restricted from U.S. and allied electronic countermeasures called the Joint Restricted Frequency List (JFRL). Despite the best intention, the JFRL does not protect against accidental disruptions—especially if using a frequency that is not on the JFRL. "In a modern Army, where we have portable computing and internet capabilities that can move information around the battlefield, we should be using radio frequency engineering during the planning process, to predict the effect of jammers on our own radios."

It was not until 2008 to 2010 that the Army was able to begin restoring an organic EW capability, says Lt. Col. Keith Cantrell, CEMA's incoming branch chief. That included standing up the Cyber Center of Excellence (COE), incorporating the work of the Signals COE it replaced, and slowly incorporating EW.

The U.S. National Security Agency (NSA) is a lead agency in signals intelligence and electronic warfare. This photo shows the NSA's National Security Operations Center floor in 2012 (NSA photo)

Shipboard and airborne EW

Despite the Navy's role as DOD's executive agency for EW, its leaders are being forced to redesign the Navy's own capabilities—air- and ship-borne. That includes the Surface Electronic Warfare Improvement Program (SEWIP) to upgrade existing shipboard signals technologies used to identify, assess and analyze EM signals and EW threats. A major problem, especially with aircraft carriers, is the massive number of radars, antennas, and other electronic systems operating simultaneously in a highly complex shipboard electromagnetic spectrum.

With the prospect of near-peer EW threats in the future, carriers and other combat and support vessels will need even greater capabilities to conduct offensive and defensive EW. That includes the NGJ, designed to give the EA-18G Growler advanced technologies for offensive EW missions when the jammer goes operational by 2020.

"The vision for the future is to take what our collection, exploitation, and early warning capabilities [find] and turn them into offensive ways to use electronic attack," says Christine Fox, who recently retired from the Pentagon after serving as acting deputy secretary of defense. "If we can go after the C2 or ISR pieces of a threat instead of putting a missile against a missile, I can potentially disrupt that missile's ability to find its target."

In addition, the Office of Naval Research (ONR) in Arlington, Va., is developing a prototype technology called Integrated Topside (InTop) to extend the range and flexibility of shipboard EW. For example, InTop would integrate the current forest of antennas on a ship's deck into a shared multi-function, multi-beam aperture array that could collect signals across a wide range of frequencies, then use a central resource allocation manager to share that information with several EW processes.

Perhaps equally important is the 21st Century version of "quiet running." The Chief of Naval Operations is pushing for greater education of officers and enlisted personnel on electronic spectrum awareness and understanding all aspects of a ship's electromagnetic signature.

"We have to be more mindful of how we operate in the electromagnetic domain and in cyberspace and how those capabilities come together," wrote Margaret Palmieri, director of the Navy's Integrated Fires Division, in the July 2014 issue of U.S. Naval Institute Proceedings. "We are working on better understanding how networks and signals and networks and information come together. What do we really look like to the enemy?

"Integrated-fires capabilities are a central part of the asymmetric advantage our Navy, joint and coalition forces bring to a fight. They include capabilities that disrupt adversary C4ISR systems, deliver electronic payloads that limit an enemy's freedom of maneuver and action and enhance the ability of our own forces to place ordnance on target," Palmieri wrote. "It integrates lethal and non-lethal fires, underpinned by superior battlespace awareness and assured C2, to provide commanders an expanded set of warfighting tools especially important in A2/AD environments, like Air-Sea Battle."

In that same issue, Vice Adm. Ted N. Branch, deputy chief of naval operations (CNO) for information dominance, discussed the Navy's need to dominate all segments of future battlespaces—on, above, and below the sea, as well as outer space—to sustain America's "global primacy'. "However, commanding, controlling and fighting our forces in these areas requires dominance in the information domain, to include the electromagnetic spectrum and cyberspace," he wrote. "The name we've given to this concept—information dominance—is still new and unfamiliar to some, but it's indispensable to Fleet operations, so much so that we've adopted it as a distinct warfare discipline.

"Formerly perceived by many as a collection of support activities performed by specialized restricted line officers, information dominance is increasingly recognized by Fleet operators as a critical force multiplier. It's no longer just an adjunct to warfighting. It is warfighting," Branch wrote.

Navy information dominance focuses on three goals: robust and agile C2 in all operating environments; superior knowledge of the battlespace, the physical environment as well as threat capability, disposition and intent; and projecting power through the integration of kinetic and non-kinetic effects. "We refer to these three elements, or pillars, as assured C2, battlespace awareness and integrated fires. Through them, information dominance creates decision superiority, provides asymmetric advantage and enhances the lethality of our deployed forces with non-kinetic options," Branch added. Those pillars, in turn, are designed to correspond to the CNO's three tenets: warfighting first; operate forward; and be ready.

"The critical element of the information dominance definition is integration, Branch wrote. "Blending the attributes of ISR, oceanography, meteorology, networks, cyber, and EW allows for better planning, smarter decisions and earlier results. Aligning the related restricted-line communities of naval oceanography, information warfare, information professional, intelligence and the space cadre into the information dominance corps has likewise advanced our concept and capability development and improved data and system interoperability."

U.S. Marine Corps

While the Army and Marine Corps both are viewed as ground forces, the Marine Corps' EW requirements differ significantly from those of the Army, especially in meeting future anticipated threats. In recognition of that, the Corps has created a Marine Air/Ground Task Force (MAGTF) EW concept to develop an integrated system of distributed, platform-agnostic EW systems, including the progressive inclusion of technologies and capabilities from other services and commercial vendors.

MAGTF EW elements have several programs in development. Among them are Intrepid Tiger II (IT-2): An EW pod for communications-based targets, expandable to radar-based targets, currently deployed to CENTCOM and with Marine expeditionary units in three different versions for fixed-wing aircraft, unmanned aerial vehicles (UAVs), and helicopters.

Another program is the Electronic Warfare Service Architecture (EWSA)—an extended data exchange and hardware protocol to connect EW/SIGINT airborne nodes, via an adaptive multi-waveform network, to ground operators, Cyber/EW Coordination Cells (C/EWCCs) and other air EW nodes. The Corps also has stood up several new or redefined units, including the Cyber and Electronic Warfare Integration Division (CEWID), the Capabilities Development Directorate's integration and execution authority for all Marine Corps warfighting development activities associated with Cyberspace and EW.

Navy sailors on the watch-floor of the Navy Cyber Defense Operations Command monitor, analyze, detect and respond defensively to unauthorized activity within U.S. Navy information systems and computer networks. (U.S. Navy photo)

CEWID coordinates with operating forces, supporting establishment and mission partners in order to identify, prioritize and integrate capability solutions across DOD's Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) protocols. CEWID, in turn, comprises three branches: computer network attack, computer network defense, and MAGTF EW.

The General Atomics Aeronautical Systems Predator B/MQ-9 Reaper's new electronic attack capability, using the Northrop Grumman Pandora EW system, is a major part of the Marine Corps future EW effort. The system could advance the Reaper from its existing role as a counter-insurgency ISR/hunter-killer aircraft to a broader spectrum of EW missions, says GA-ASI President Frank W. Pace.

Pandora is a pod-based, multifunction, wideband system providing electronic attack, such as jamming, support and protection. Demonstrations at Yuma Marine Corps Air Station, Ariz., were designed to evaluate the ability of Pandora-equipped aircraft to conduct coordinated EW missions in a multi-node approach against a more capable integrated air defense system.

"Pandora brings optimal size, weight and power to current and future high-endurance platforms, opening up a new world of electronic attack capabilities," says Janine Nyre, vice president of radio frequency combat information systems at Northrop Grumman.

"We demonstrated operational concepts using a layered approach to electronic warfare with Reaper, EA-6B Prowlers, and other Group 3 UAVs," adds Brig. Gen. Matthew G. Glavy, assistant deputy commandant for Marine aviation. "By conducting multiple events, we were able to evaluate the viability of UAVs to conduct EW missions against enemy air defenses in support of tactical strike aircraft."

The 2013 Marine Corps Operating Concept for Information Operations termed information operations (IO) as a complex box of tools the Corps must incorporate and exploit within the context of its overall maneuver warfare philosophy and expeditionary culture to operate "effectively against a myriad of potential adversaries and perform multiple, diverse and simultaneous tasks across the ROMO [range of military operations]".

"In the Marine Corps, IO is not a warfighting function in its own right; it is an integrating function which facilitates the six warfighting functions of C2, fires, maneuver, logistics, intelligence and force protection. This distinction between warfighting and integrating function is key to the Marine Corps' belief IO does not—and will not—replace any of the time-tested warfighting functions. It will enable each of them," says the OCIC.

"IO is not a discrete, stand-alone capability, but is the integrated, coordinated and synchronized operational application of all information-related capabilities (IRCs), organic and non-organic, to affect decision-making by adversaries and potential adversaries, thereby creating an operational advantage. Integration is accomplished under the purview of the operations section, based upon commander's guidance, and supports achievement of the commander's end state. "IO is not synonymous with individual discrete capabilities or activities, much like fire support is not synonymous with artillery or aviation. More art than science, IO is focused on the human mind and seeks to influence behaviors to produce operational advantages."

EW in the air

While emphasizing they "do not generally comment on EW requirements, specific technologies or capabilities of our or others' systems", the Acquisition, Science, Technology and Engineering Directorate within the office of the Secretary of the Air Force (SAF/AQRM) did provide the following statement: "The Air Force recognizes that increased budgetary constraints, coupled with widespread availability of modern electronics, requires new technology and acquisition approaches for EW. The Air Force is tackling the problem along five fronts: 1) enabling fundamental components, 2) new techniques, 3) new adaptive modular approaches, 4) early prototyping and rapid reaction developments and 5) early in-the-loop testing.

"Today's EW, Communications, Navigation, Sensing and Cyber

technologies require a more integrated use of the electromagnetic spectrum than ever before. The Air Force Research Laboratory (AFRL) is working on full spectrum science and technology, which includes: radio frequency EW; avionics protection; position, navigation and timing [PNT] in contested/denied environments; electro-optical/infrared threat warning and countermeasures; protected communications and robust cyber."

In its "Strategy for Spectrum Warfare", SAF/AQRM noted it is pursuing those goals through a comprehensive Advanced Components for EW (ACE) program and developing cognitive and distributed techniques, adaptive modular approaches and rapid prototyping.

AFRL issued a broad agency announcement (BAA) last fall for the Advanced Novel Spectrum Warfare Environment Research (ANSWER) program to develop adaptive spectrum warfare technologies to maintain warfighting capabilities in contested and denied environments consistent with A2/AD scenarios. AFRL encouraged industry to employ unconventional thinking on the use of advanced computing power, signals processing, modeling and simulation, anti-tamper and software protection technologies, GPS alternatives with comparable accuracies for warfighters in A2/AD environments, vision and laser-based navigation and electro-optics countermeasures.

"With an ever-changing environment between red and blue forces, the ability to control the electromagnetic spectrum is a key requirement to achieving success in warfighter operations. This is a daunting task under benign conditions and becomes even more of a challenge as adversaries are able to employ various denial capabilities," the BAA noted. "If one can conduct electromagnetic spectrum operations under A2/AD conditions, then successful operations in other less challenging environments should be achievable as well. To accomplish this, the warfighter needs to be able to control adversary use of electromagnetic spectrum, ensure friendly access to/use of electromagnetic spectrum, protect sensor/avionics end nodes, establish/maintain secure communications/data links in dense electromagnetic spectrum environments and assure the availability of accurate PNT information. The ANSWER program is designed to address these challenges."

The Navy Boeing E/A-18G Growler combat jet is the nation's primary airborne electronic warfare platform, and should see land- and carrier-based use well into the 21st century.

The Post-OEF/OIF EW Environment

"When it comes to EW, it doesn't have to be a near-peer or even a known rival. Electronics that can be made to be a problem are ubiquitous throughout the world," says the Army Cyber Center's Murray. "You can find a thousand types of cell phones in Afghanistan, which I certainly wouldn't call the modern world. So a lot of technology is out there, worldwide, that, in the wrong hands, can be a very severe problem, no matter what kind of advanced weapons or armor we have.

"Technology changes so fast that what is considered SOTA today may not be in another year," Murray says. "And that's one of the challenges on things we would like to have now and in the future. But the processes we must go through to acquire the equipment we would like to have and need to have are not as agile as we need them to be. They're OK now, but if we get into a new fight, you can't wait for what you need."

The possibility of near-peer conflict is growing as the U.S. puts a greater focus on the Asia/Pacific region and Eastern Europe once again feels threatened by Russia, even as the Middle East continues increasingly tech-based rounds of ancient conflicts. In addition, the vast distances involved and the lack of U.S. land bases in the Asia/Pacific—outside of South Korea and Okinawa in the north—will mean a greater focus on the Navy and Marine Corps, especially with respect to EW.

There was a sharp reduction in the Pentagon's EW research and development budget from 2013 to 2015—a cut from $3.5 billion to $2.1 billion—more than half from the Navy and Marine Corps. Of course, an unknown—but suspected substantial—part of EW research falls under classified "black" budgets.

"Although EW is declining through 2015, we expect to start seeing a resumption of spending from 2016 on," says John Hernandez, a senior aerospace and defense industry analyst at market researcher Frost and Sullivan. "That is an area that is being underdeveloped right now, but with the potential new adversaries in the coming years, it will need to be reinvigorated. Some analysts are predicting an increase in small, even hand-held jammers, but our analysts expect to see more modularity, especially for ship-board systems.

"There was a move for a while to make the F-35 the new EW platform, but I don't think the expense was worth it, given the fine job the Growler is doing. But in the future, I can see unmanned systems doing more EW, whether that is a single platform or a flock of UAVs doing jamming or AD missions. Personally, I suspect protecting our own systems is and will continue to be a priority over offensive technologies."

Defense industry adapts

The new environment and focus on naval assets also has been reflected in industry. In February 2014, for example, Raytheon Space and Airborne Systems combined several EW efforts into a new mission area called Electronic Warfare Systems, based at the company's El Segundo, CA, campus. The new unit will focus on the Navy's Next-Generation Jammer (NGJ);; EW self-protection systems; EW communications systems; advanced EW programs; and airborne information operations.

At the Northrop Grumman Integrated Systems sector, meanwhile, airborne early warning and electronic warfare systems have seen a similar growth in importance, including the June 2014 award of a joint service (Army/Navy) contract for 18 APR-39D(V)2 radar warning receiver (RWR)/EW management system (EWMS) pre-production units.

"Our APR-39D(V)2 merges the baseline capability of previous systems with the Northrop Grumman digital receiver technology to provide advanced capability for today's and tomorrow's threat environment," says Northrop Grumman's Nyre. "This lightweight system maintains interfaces with legacy systems and includes flexibility for future growth enhancements."

The company is to deliver the systems in late 2014 preparatory to hardware-software and platform integration testing in 2015.

Also next year, Northrop Grumman is scheduled to complete equipping the Navy's MQ-8C Fire Scout rotary UAV with a new external Multi-Capability Pod, providing it with "multiple EW sensors for employment in the littorals", says a DOD announcement in May 2014.

BAE Systems is leveraging advances in signals processing and machine learning under a DARPA-funded program called Adaptive Radar Countermeasures (ARC). The goal is a next-generation EW algorithm suite as a software upgrade existing EW hardware to can use to operate against emerging radar threats and help achieve and maintain U.S. air dominance in future battlespaces. Special emphasis will be on countering never-before-seen threats with unknown waveform characteristics and behaviors.

"This technology will provide a revolutionary capability to EW systems on U.S. military airborne platforms to counter adaptive radar threats and significantly improve survivability," says Joshua Niedzwiecki, BAE's director of strategic development. ARC is projected to be ready for live demonstration flight tests by 2018.

Mercury Systems in Chelmsford, Mass., has been predominantly involved with air-to-air/surface-to-air systems, but Chief Technology Officer Chris Lewis says the current SOTA for them "has been the transition from classic denial—jamming—to more deceiving your adversary".

"The world today is less bifurcated between EW and Cyber, which I consider part of the same continuum," he says. "The kinds of things we're seeing starting to come on line are systems that are much tighter in their response. Where conventional systems saw a new waveform that then was captured and technology to deal with it developed in the lab, today's system is tighter, with techniques being developed in days rather than months. And the goal is be instantaneous.

"Enabling technologies for future EW include continuing improvement in the performance of FPGAs and microprocessors, the continued drive in communications and great improvement in solid state amplifiers due to gallium nitride. Further down the line is photonics for very wide bandwidth and high dynamic range. Another, not a technology so much as capability, is the adaptive learning system. Some of the SOTA things being done today are just scratching that surface and I see more of that coming online in the next few years."

Lewis sees the largest EW market for the foreseeable future being retrofits for legacy platforms DOD cannot afford to replace: "As the U.S. goes forward, there will be more and more demand to do things with less and less. And the leverage of doing that in terms of retrofits will have a lot of benefits for the country as a whole."

Spectrum warfare

Rapid advances in technology have complicated the definition of EW. The Air Force uses spectrum warfare to bring together all elements of

Unmanned aerial vehicles (UAVs) of various sizes, including the lightweight ScanEagle shown above, are taking on increasing roles in offensive and defense electronic warfare.

EW with cyber warfare, information operations and essential capabilities to enable a full range of electromagnetic operations—offensive and defensive—in A2/AD environments against all levels of adversaries.

The Army prefers cyber electromagnetic activities. According to recently revised Army Doctrine for Unified Land Operations, CEMA involves "activities leveraged to seize, retain and exploit an advantage over adversaries and enemies in cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system". Implementation is achieved through synchronization and integration of cyberspace operations, EW and electromagnetic spectrum operations (electromagnetic spectrum).

Terminology aside, nearly every aspect of command, control,

communications, computers, intelligence, surveillance and reconnaissance (C4ISR) has (or is) a component of or dependent on 21^{st} century EW.

Frequency-hopping radios and radar soon may be replaced by "cognitive" systems that don't rely on a set list of frequencies, but look for available "holes" throughout the full spectrum, jumping from one to the next on the fly. A primitive version of that is a smartphone that uses the best available way to connect, from nearby WiFi to 4G.

But control and unchallenged access to battlespace spectrum also is critical for navigation—from precision-guided munitions to logistics—semi-autonomous combat robots, field and battlespace medicine and more. And as spectrum becomes ever-more crucial to military and commercial communications and data transfer, two long-standing "laws" of technology continue to converge.

The more widely known Moore's Law, named for Intel co-founder Gordon Moore, states that CPU speeds double every two years (although purists note it is more accurate to say the number of transistors on an affordable CPU is what doubles).

The lesser known Cooper's Law, formulated by the inventor of the cell phone Martin Cooper, notes the number of conversations, whether voice or data, that theoretically can be conducted using a specific piece of useful radio spectrum has doubled every 30 months for more than a century. As a result, total spectrum allocation for personal communications alone has increased more than one trillion-fold in the last 90 years.

Increasingly competitive, congested and contested cyberspace and electromagnetic spectrum will be even more important as the U.S. faces potential conflict with a near-peer adversary for the first time since World War II—and as CEMA capabilities spread and grow down to the level of individual terrorist cells, criminal organizations and Third World nations, none of whom could ever hope to survive a traditional engagement with the U.S.

The services' differing views of the involved technologies are more than semantic, they also are operational. The Navy sees EW as modern warfighting, the Air Force considers it an essential and integrated component to the success of A2/AD and air dominance, but the Army continues to view it as a support component, not warfighting.

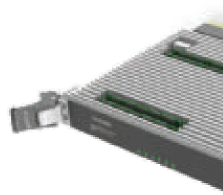
"When you talk about maneuver commanders, the objective is to seize and secure terrain. The EW mission is to support that, but EW and cyber have separate roles to play. Cyber can and is moving into a major combat role; the EW role is to control the spectrum to allow the maneuver commander to achieve his goals," says the Army Cyber Center's Cantrell.

CEMA's Cullen agrees, adding those in combat are only interested in what works: "From a maneuver commander's perspective—infantry or armor—they don't care if it is EW or cyber or whatever. There are advantages and disadvantages to both EW effects, cyber effects and kinetic effects. The requirement is to figure out which is best in a given situation."

In April 2014, the Naval Air Warfare Center Weapons Division and the Association of Old Crows held the 43^{rd} Electronic Warfare Symposium at Point Mugu, Calif., with the theme "Enabling Collaborative EW Through Innovation and Invention."

"Staying up-to-date in EW technology is essential to supporting the warfighter, said Dr. Ron Smiley, director of the EW/Combat Systems and Avionics departments at the Naval Air Systems Command at Patuxent River Naval Air Station, Md., told the conference. "Electronic warfare is changing, becoming more challenging and has continued to become a lot more esoteric, particularly with the convergence of EW and Cyber Warfare."

Rear Adm. Mark Darrah, commander of the Naval Air Warfare Center Aircraft Division, summarized the conference discussions with a view to potential enemy developments and the changing nature of U.S. technology development. "Unlike 20 years ago, our advisories are developing similar technologies that we are—and are doing it right now," he says. "The only way we will stay ahead of the threat of our enemies is to take paper ideas and give it to our people for trial-and-error until we succeed." ←



The future of high-performance embedded computing

HPEC technology is leading to never-before-envisioned applications like mobile tactical cloud computing and compact systems on chips that bring supercomputer performance to small platforms like unmanned vehicles.

BY **John Keller**

The military has a class of compute-intensive applications such as signals intelligence, radar processing, and electronic warfare (EW) that have such a voracious appetite for digital signal processing power that no kind of embedded computing—real or envisioned—ever could satisfy completely. The more embedded computing power becomes available, the more these applications use it, and call for even more power than what's available.

The embedded computing developers who seek to address this need are hard at work on what they call high-performance embedded computing, or HPEC for short. HPEC is a general term and has a variety of definitions, but one of them has to do with addressing the never-ending demands for more computing power for the most demanding applications.

Essentially these kinds of HPEC applications seek to embed supercomputer-like performance in a relatively small, rugged, and embedded form factor in applications that can compromise neither on performance no on size, weight, and power consumption (SWaP).

These kinds of applications can involve unmanned vehicles for surveillance that must process mountains of sensor data while remaining small and power-stingy. As aerospace and defense applications rely increasingly on cloud computing, HPEC also offers to create a "mobile cloud," which can provide essential information when military platforms are disconnected from the tactical Internet.

Other definitions of HPEC, involve a somewhat normal evolution of embedded computing, which follows steady improvements in commercially available microprocessor technologies. These refer to embedded computing products that use the latest and greatest microprocessor technologies from Intel, Freescale Semiconductor, Texas Instruments, and others.

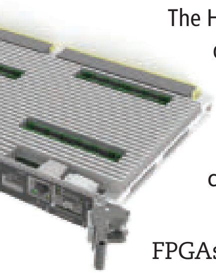
As the Intel Core i7, Haswell-EP, and Xeon Phi microprocessors become available, these microprocessors quickly become available in rugged embedded computing versions, and become important HPEC components.

What is HPEC?

Essentially there are two camps among practitioners of HPEC: a complex integrated approach, and very high-end embedded computing. The most complex and high-performance incarnations of HPEC often involve an integration of one or more embedded processing technologies such as general-purposes processors, field-programmable gate arrays (FPGAs), and general-purpose graphics processing units (GPGPUs).

Among the HPEC approaches under development at the Curtiss-Wright Corp. Defense Solutions division in Ashburn, Va., involves a heterogeneous mix of the best of microprocessors, FPGAs, and GPGPUs, says Marc Couture, senior product manager of digital signal processing at Curtiss-Wright.

Blending microprocessors, FPGAs, and GPGPUs in one architectures forms a heterogeneous computing slice "that plays to the strengths of those processing elements," Couture says. "FPGAs are all about I/O, and bringing in a lot of I/O in parallel and doing that over and over again.



The HDS6602 is the latest high-density server signal and image processing engine from Mercury Systems, harnessing two server-class Ivy Bridge 10-core Intel Xeon processors.

FPGAs can aggregate data and hand it off to a lot of Intel cores that are good a multiple nodes and at making decisions. If you want to accelerate performance, that's where the GPGPU might be very effective."

Embedded computing designers in recent years have found that high-end graphics processors that were designed to render complex computer graphics also have the ability to massively parallel processing. This capability helps bring more power into embedded computing systems, or helps to shrink embedded computing architectures to the do the same amount of work in smaller more lightweight packaging.

"Over time you see all the silicon vendors get enough compute power per one watt, and they finally have it within that physical SWaP envelope," Couture says. "If you can develop this capability and make it robust, that gives the warfighter more capability."

Some in the embedded computing industry see HPEC as the latest and greatest hardware and software in the embedded world, involving the best server-class or cloud-based computing environments bridging to the embedded world, says Chad Augustine, product marketing manager for software at Curtiss-Wright.

Some see HPEC as using open-systems software from the high-performance computing—or supercomputer—world and making embedded supercomputing that fits in a slot. Recent developments in very large scale integration are seeing HPEC-type computing that once fit in a 6U or 3U backplane chassis and integrated such that they fit on one special-purpose chip, or system on a chip.

"What used to happen in a VME card cage now is done in silicon," says Ben Sharfi, president and CEO of General Micro Systems Inc. (GMS) in Rancho Cucamonga, Calif. "Each core communicates with the others in the same exact way that embedded blades communicate with each other over a backplane."

Sharfi says HPEC "is all about

performance and horsepower, or floating point and integer work and data movement. It's all about moving data and being able to do that as fast as possible."

The GMS approach to HPEC revolves around the choice of a general-purpose arithmetic logic unit (ALU), or a dedicated ALU, Sharfi says. "The general-purpose ALU is the microprocessor, like PowerPC or Intel; it is designed to do anything and everything. Then you have an FPGA-based ALU dedicated to do a certain function at a very fast rate. The dedicated ALU will always outperform a general-purpose ALU," he says.

The ability to embed a supercomputer on a chip is enabling a broad variety of applications that simply were not possible before—especially in space-constrained applications like unmanned vehicles and wearable computing. Thermal management is one of the HPEC designer's core concerns, Sharfi points out. Some of the most advanced microprocessors used for HPEC applications consume a lot of power and run hot. "If you have 75 watts just for the processor, and then you have 130 to 140 watts for the system, it doesn't fit on a 3U board," he says.

GMS and other companies find that when pushing the SWaP envelope with HPEC designs, sometimes standard architectures like VPX cannot accommodate the necessary size, performance, and cooling limitations. "You might need 6U packaging, but then the problem is heat transfer. In cases like this a custom architecture like the GMS Tarantula HPEC system might solve the problem.

The GMS Tarantula small rugged chassis has six secure virtual machines based on the 10-core Intel Ivy

The General Micro Systems Tarantula embedded computing system, shown above, requires custom packaging to accommodate the systems processors and thermal management. Standard architectures are not sufficient to accommodate its capabilities.

Bridge-EP microprocessor, an 18 port switch, RAID data storage and auxiliary power unit in a package that measures 11.75 by 7.75 by 4.5 inches and weighs about 18 pounds, Sharfi says. Its power consumption can be as low as 180 watts.

Some see in HPEC technologies a new generation of flexible and scalable computing architectures that enable systems designers to upgrade embedded computers easily to keep pace with application demands while making broad use of commercially available high-performance computing technologies. "HPEC is about bringing software from high-performance computing into embedded computing," says Michael Stern, product manager for high-performance embedded computing at GE Intelligent Platforms in Towcester, England. "It's not about one form factor against the other; it's taking the software and putting it in a ruggedized form factor that is upgradable over time."

Among the key open-systems technologies involved in HPEC are 10-Gigabit Ethernet, Infiniband, and others that are helping designers move toward the Petaflop range in cluster computing, including central processing units (CPUs), general-purpose graphics processing units (GPGPUs), and enterprise distribution of remote memory access, Stern says.

Commercial high-performance computing can scale many thousands of graphics and central processors using essentially the same application software, "and we want to make that same technology available in a scalable, ruggedized form factor—typically in 6U OpenVPX, and sometimes in 3U OpenVPX for some of the smaller applications," Stern says.

The need for HPEC

"Embedded computing is about receiving data and converting it into high-value information," says Ian Dunn, vice president and general manager of embedded products at Mercury Systems in Chelmsford, Mass. "The purpose of HPEC is to render another piece of information that a machine or human can use to render a result."

HPEC is particularly beneficial to those designing sensor-processing systems because this technology is helping evolve data-processing capability at a faster rate than sensor technology itself, Dunn says. This phenomenon will help sophisticated sensor-processing technology increase in capability and decrease in size for the foreseeable future. "Sensors continue to get more complex, but not at the rate of Moore's Law," he says. "Remote sensor platforms will have more computing power available every year, so they can get smaller. We have a UAV [unmanned aerial vehicle] industry today that is thriving largely because of high-performance embedded computing, which has gotten really small."

HPEC technology is helping to enable a sensor-processing approach called processing exploitation dissemination (PED) that is having a profound influence on UAVs as sensor platforms, says Curtiss-Wright's Couture. "Some of the UAVs collect data, and may do some image processing, and stitch pixel data together. They have to store this data, which is not cheap, or steam the data down to the ground, which is like draining a bathtub with a coffee straw." PED, Couture says, "can have HPEC do things that human analysts used to do. It can run algorithms that say a target may be a tank, or a car with a wedding party. It is enabling more than just processing the sensor data; it is extracting from the sensor data."

The ability of HPEC to exploit advanced software algorithms on mobile platforms like UAVs, which only a few years ago had to be done on large land-based supercomputers, is helping unmanned vehicles perform surveillance feats that they've never been able to do before. "HPEC allows you to bring a lot more computer power with open-systems ecosystems into areas where previously you couldn't do that," says GE's Stern.

"Our customers need to harness the latest and greatest processing technology from the greater market quickly, and they need architectures that are open and flexible," Stern says. "It's true that more and more of that investment in, say, a new radar, or radar upgrade, or missile upgrade, is in software on the application side for back-end signal processing, which typically is done in software.

More and more the DOD [U.S. Department of Defense] wants common APIs so they can get developers for their applications at a high level without the need to understand machine code or driver code that is close to the hardware," Stern continues. "It's all about providing scalable and upgradable systems. You can buy a box form us or some other supplier like Mercury or Curtiss-Wright. The bottom line is DOD offices want interoperability, technology reuse, and tech refresh over time."

HPEC and the mobile cloud

High-performance yet space-constrained aerospace and defense applications increasingly depend on RF connections to the tactical Internet for access to information that resides on secure tactical cloud computing, such as image and terrain databases. Access to the cloud in tactical environments, however, cannot always be assured due to terrain masking, enemy jamming, friendly RF fratricide, or other unanticipated interference. This is where HPEC can come into its own.

"The cloud has intervened to take on some of the HPEC responsibilities," Mercury's Dunn says. "It's a credit to Intel that Moore's law has allowed them to build these very sophisticated devices, and the cost of a MIP or FLOP keeps going down. It is reducing costs to people, and people can reduce costs while wasting more computing."

Big corporations like Amazon rely on cloud computing for access to voluminous data, but unlike the military, commercial businesses don't have to rely on cloud computing for real-time processing. "In the commercial world where they don't have to make a decision quickly," Dunn says. "They can convert that computing over to cloud computing that they have in house or out of house, where they don't have a latency issue, but you can't shoot down a missile with Amazon's cloud computing network."

Mobile platforms like unmanned aerial vehicles (UAVs) cannot rely on RF Internet connections during every moment of a mission. "Mobile platforms are connectivity challenged, and they can't afford to be connectivity challenged," Dunn says. "They may have to make a decision in a non-connectivity situation. That gives us a meaty problem in the military HPEC market. We have to put the cloud on a personal platform."

Mercury Computing and other practitioners of HPEC "working on making that tactical cloud real from an embedded architecture perspective," Dunn says. "As I send different platforms out, you have this asset that has been trained in a cloud environment to do its job. It goes to the cloud because it has a database it can use to facilitate the mission, and store all the imagery. If it can't go to the cloud, then it has to bring the cloud with it."

An HPEC-enabled mobile cloud that is temporarily disconnected from the tactical Internet could make the decision for itself to access the information it has on board when its Internet connection is cut. "When it has a connection it has a connection, and when it doesn't have it, it does the best it can," Dunn says.

"The mobile cloud is tethered to backhaul to access information from a grid like the military's Global Information Grid," points out Curtiss-Wright's Couture. "If you are severed from that how can you be self-sufficient, with some sort of data set, with geography that would be useful?

"Bringing in imagery, RF emitter data, and accessing data from a database, there is some real serious computation that needs to happen, and you are doing that in real time on a platform that isn't exactly stable, like a UAV," Couture says. "There is a real need there for high-performance computing." ←

COMPANY INFO

Aitech Defense Systems
Chatsworth, Calif.
www.rugged.com

BittWare
Concord, N.H.
www.bittware.com

Creative Electronic Systems (CES)
Grand-Lancy, Switzerland
www.ces.ch/

Concurrent Technologies
Colchester, England
www.gocct.com

CSPI MultiComputer Division
Billerica, Mass.
www.cspi.com/multicomputer

Curtiss-Wright Corp. Defense Solutions
Ashburn, Va.
www.cwcdefense.com

Elma Electronic Corp.
Fremont, Calif.
www.elma.com

Extreme Engineering Solutions (X-ES)
Middleton, Wis.
www.xes-inc.com

GE Intelligent Platforms
Huntsville, Ala.
www.ge-ip.com

General Micro Systems Inc.
Rancho Cucamonga, Calif.
www.gms4sbc.com

Kontron AG
Poway, Calif.
us.kontron.com

Mercury Systems
Chelmsford, Mass.
www.mrcy.com

PCI Systems Inc.
Sunnyvale, Calif.
pcisystems.squarespace.com

Pentek Inc.
Upper Saddle River, N.J.
www.pentek.com

SIE Computing Solutions
Brockton, Mass.
sie-cs.com

Themis Computer
Fremont, Calif.
www.themis.com

PRODUCT intelligence

Aerospace and defense organizations rely on rugged laptops

BY Courtney E. Howard

Communications and connectivity are essential to aerospace and defense professionals. Daily tasks and missions today often depend on access to real-time relevant information; it can mean the difference between success and failure, or even life and death.

The premium currently placed on information access, including for deployed warfighters in the field, is contributing to increased adoption and use of ruggedized laptop computers in myriad aerospace and defense applications and environments. Military organizations the world over are opting for rugged laptops, rather than their mass-produced commercial counterparts, given the machines' ability to withstand harsh conditions, temperatures, and environments.

Militaries worldwide, once presented with a limited amount of options, now have a wide array of rugged laptop computer models and features from which to choose. Key features aerospace and defense professionals look for in rugged laptops, in addition to the ability to withstand the elements, include: security and size, weight, power, and cost (or SWaP-C).

"With the ever-increasing demands on accessing sensitive data 24/7, securing mobile platforms to the highest level is becoming increasingly significant," explains Chris McIntosh, CEO of ViaSat in Germantown, Md. ViaSat's Eclypt

COMPANY INFO

Algiz
+46 (0) 510-54 71 70
ruggedalgiz.com

Amrel
626-443-6818
amrel.com

Argon Corp.
678-608-4930
argoncorp.com

ASUSTeK Computer Inc.
510-739-3777
asus.com

Azonix Corp.
978-670-6300
azonix.com

Broadax Systems Inc.
626-964-2600
bsicomputer.com

Cyberchron Rugged Systems
845-265-3700
cyberchron.com

Dell Inc.
512-338-4400
dell.com

DRS Tactical Systems
321-727-3672
drs-ts.com

Elbit Systems of America C4I Solutions
850-350-8444
elbitsystems-us.com

GammaTech Computer Corp.
888-945-7879
Gammatech.com

Lenovo
855-253-6686
Lenovo.com

General Dynamics C4 Systems
480-441-3033
gdc4s.com

Getac Inc.
949-699-2888
getac.com

Handheld USA Inc.
541-752-0313
handheld-us.com

Hewlett-Packard Inc.
650-857-1501
hp.com

IBI Systems Inc.
954-978-9225
ibi-systems.com

Industrial Computing
781-890-3111
industcomputing.com

Intermec Inc.
425-348-2600
intermec.com

MilDef AB
+46 42 250000
login.se

MaxVision
800-533-5805
maxvision.com

Motion Computing Inc.
512-637-1100
motioncomputing.com

NEXCOM International Ltd.
510-656-2248
nexcom.com

NextComputing LLC
603-886-3874
nextcomputing.com

Panasonic Solutions Co.
201-348-7000
panasonic.com/business/toughbook

Panther Computers
850-983-2270
panthercomputers.com

Roper Mobile Technology
480-705-4200
ropermobile.com

Rugged Notebooks Inc.
714-998-1828
ruggednotebooks.com/military-and-government

Secure Communication Systems Inc.
714-547-1174
securecomm.com

Stealth Computer Inc.
905-264-9000
stealth.com

Trimble Navigation, Ltd.
408-481-8000
trimble.com/Outdoor-Rugged-Computers

Two Technologies Inc.
215-441-5305
2T.com

VT Miltope Inc.
334-284-8665
miltope.com

Xplore Technologies
512-336-7797
Xploretech.com

technology is available on the Panasonic FZ-G1 tablet to provide a "reliable, secure, and powerful portable system that can be deployed within the high threat government, military, and critical infrastructure protection environments."

Aerospace and defense end users continue to opt for electronic systems, including modern rugged laptops, offering reduced SWaP-C. Manufacturers of rugged notebook computers, tapping the latest technological advances from the commercial market, continue to pack a wealth of compute power, data storage, input/output (I/O) and connectivity options, and other capabilities into ever more compact form factors.

"Militaries want rugged devices that can perform in any environment," says John Costello, vice president of marketing at Xplore Technologies in Austin, Texas. At the same time, aerospace and defense users "continue to demand smaller, thinner, lighter, more portable, and longer battery life. With that in mind, we will continue to push the boundaries building rugged devices that align with market demands and military specs."

The vendors listed provide a wealth of rugged laptop models designed to meet a wide array of aerospace and defense applications, missions, users, and environments. ←

Northrop Grumman to upgrade navigation on Fire Scout UAVs

U.S. Navy unmanned aerial vehicle (UAV) experts plan to upgrade navigation systems in the Northrop Grumman MQ-8B/C Fire Scout shipboard unmanned helicopters to improve the UAV's precision and reliability. Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced plans to award a test contract to the Northrop Grumman Corp. Aerospace Systems segment in Rancho Bernardo, Calif. The contract will call for Northrop Grumman to test and qualify the Fire Scout navigation systems made by the Kearfott Corp. Guidance & Navigation Division, a subsidiary of Astronics Corp., in Little Falls, N.J.

DHS to use Raytheon UAV radar systems

Maritime surveillance experts at the U.S. Department of Homeland Security (DHS) in Washington needed airborne radar systems for searching the surface of the ocean for a variety of security applications. They found their solution at Raytheon Co. Space and Airborne Systems in McKinney, Texas. DHS officials plan to award a sole-source contract to Raytheon for as many as 20 of the company's SeaVue maritime surveillance radar systems, as well as spare parts and subcomponents. ←

Aviation authorities to brief industry this fall on UAV sense-and-avoid technologies

BY **John Keller**

LAUREL, Md.—U.S. government aviation authorities will meet with industry this fall to discuss lightweight sense-and-avoid technologies to enable unmanned aerial vehicles (UAVs) to operate safely with manned aircraft in crowded civil airspace.

Representatives of the U.S. Department of Defense (DOD), Federal Aviation Administration (FAA), National Aeronautics and Space Administration (NASA), and the Department of Homeland Security (DHS) will meet with industry to discuss UAV sense-and-avoid technologies on 28 and 29 Oct. 2014 at the John Hopkins Applied Physics Laboratory in Laurel, Md.

Sponsoring the event is the UAS Executive Committee—a partnership of the DOD, FAA, NASA, and DHS. At this event government officials will hear presentations from industry on UAV sense-and-avoid technologies under development, and will brief attendees on government research on sense-and-avoid algorithm metrics and how to define safe separation distances between manned and unmanned aircraft. UAS stands for unmanned aerial systems.

In preparation for these meetings, officials of the UAS Executive Committee are asking for industry briefs on technologies that can reduce cost, size, weight, and power consumption of UAV sense-and-avoid systems on fixed-wing and helicopter UAVs.

Committee members particularly are interested in technologies under development in industry that can reduce the cost, size, weight, and power for onboard detection of aircraft that not communicating with air traffic control authorities, such as radar, light detection and ranging (lidar), or other sensor technologies.

Military and commercial aviation authorities will brief industry this fall on technologies for operating manned and unmanned aircraft together safely.

Authorities also are interested in design and performance standards to help UAVs participate in air traffic control systems; detection technologies that may be adapted to UAV sense and avoid; beyond-line-of-site sense-and-avoid technologies; processes to reduce certification costs of sense-and-avoid hardware and software for UAVs; and sensor-fusion technologies for several dissimilar surveillance sources.

Companies interested in submitting sense-and-avoid technology presentations should e-mail proposals to Courtney Holbrook at courtney.l.holbrook.civ@mail.mil. All presentations must be unclassified. ←

MORE INFORMATION IS online at *https://www.fbo.gov/spg/ODA/WHS/REF/UASSSA/listing.html*.

PRODUCT applications

ANTENNAS

Boeing selects SATCOM antennas from Harris

Boeing engineers needed reliable Ka-band antennas for their work on the fourth Inmarsat Global Xpress satellite, part of Inmarsat's $1.6 billion investment in the Global Xpress globally available, high-bandwidth, Ka-band network delivered by a single operator. They found their solution at Harris Corp., an international communications and information technology company, in Melbourne, Fla.

Harris won an 18-month, follow-on contract from Boeing to provide Ka-band antennas for the satellite. In orbit, the Harris antennas will direct 89 Ka-band user spot beams to the Earth creating a mobile broadband network with high-speed services for diverse applications, from deep-sea vessels to in-flight connectivity for airline passengers. Additional spot beams are available to provide dedicated service to users requiring specific coverage.

"The Harris antennas are important components in the Global Xpress satellite system, which is expected to provide global coverage by the end of 2014," says Bill Gattle, vice president and general manager, national programs, Harris Government Communications Systems. "We are committed to delivering discriminating solutions in support of the rapidly developing high-throughput satellite market."

The Global Xpress antennas are part of Harris' flight-proven gimbal dish antenna systems, which enable beams to be steered to accommodate changing or increasing user demands. Harris has more than 30 years of experience designing, building, and flying spaceborne antennas for government and commercial applications. Products include unfurlable mesh reflectors, gimbaled dish antennas, and phased array antennas.

RF AND MICROWAVE

Air Force aircraft technicians choose amplifiers from Ophir RF

U.S. Air Force aircraft maintenance technicians needed radio frequency (RF) amplifiers to support test & measurement equipment used for troubleshooting electronic faults in aircraft. They found their solution at Ophir RF in Los Angeles.

Officials of the Warner Robins Air Logistics Complex at Robins Air Force Base, Ga., awarded a $1 million contract to Ophir RF for five of the company's 5150F RF amplifiers, with options for four more pieces of RF and microwave equipment.

The Ophir 5150 solid-state broadband high-power RF amplifier covers the 0.8 to 2.5 GHz frequency range that uses Class A/AB linear power devices that provide a third order intercept point, high gain, and a wide dynamic range. The Ophir 5150 offers power output at 1dB Comp. 10 watts min.; small signal gain +42 dB min.; small signal gain flatness + 2.0 dB max.; IP3 +50 dBm typical; input voltage standing wave ratio (VSWR) of 2:1 max.; harmonics -20 dBc typical at 10 watts; spurious signals more than -60 dBc typical at 10 watts; input/output impedance 50 ohms nominal; AC input power 100 watts max.; AC input 100 to 240 volts AC, single phase; RF input +10 dBm maximum; RF input Signal Format CW/AM/FM/PM/Pulse; and class of operation A/AB.

The amplifier measures 19 by 3.5 by 18 inches, weighs 30 pounds, has type-N connectors, comes with grounding chassis, and has internal forced-air cooling. The unit operates in temperatures from zero to 50 degrees Celsius, and in humidity as high as 95 percent. It can operate at altitudes as high as 10,000 feet; can withstand the shock and vibration of truck transport; and offers circuit protection for thermal overload, over current, and over voltage.

FOR MORE INFORMATION visit **Ophir RF** online at *www.ophirrf.com*.

To submit new products for consideration, contact John Keller at jkeller@pennwell.com.

PROCESSORS

Military-grade SmartFusion2 SoC and IGLOO2 FPGAs introduced by Microsemi

Microsemi Corp. in Aliso Viejo, Calif., is introducing military-grade versions of the company's SmartFusion2 SoC and IGLOO2 field-programmable gate arrays (FPGAs) for tactical missiles, unattended ground sensors, high-altitude avionics sensors, and other aerospace and defense applications. The military-quality parts operate in temperatures from -55 to 125 degrees Celsius, and offer low power operations, as well as security, high reliability. The devices have high-speed serial I/O, embedded DSP and memory, with built-in security and anti-tamper capabilities. The parts enable defense and aerospace developers to capitalize on SmartFusion2 and IGLOO2 in data-centric communications and net-centric capabilities that are projected to drive the military communications market to reach $30 billion by 2022, analysts say. Microsemi's military-temperature tested SmartFusion2 SoC FPGAs and IGLOO2 FPGAs are sampling with full production expected this fall.

FOR MORE INFORMATION contact **Microsemi** online at *www.microsemi.com*.

POWER ELECTRONICS

AC-DC power supplies introduced by TDK Lambda

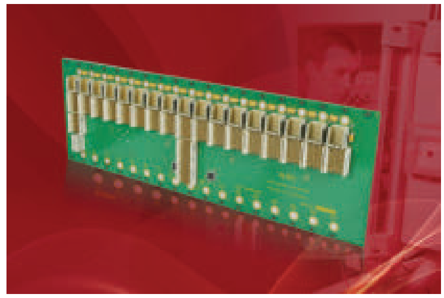
TDK-Lambda Americas Inc. in San Diego is introducing the RWS-B series of AC-DC power supplies for industrial, test and measurement, broadcast, communications, and LED signage applications. The power electronics device has a five-year warranty, and is designed to provide solid performance at an economical price, company officials say. The product line up has four power levels and compact case sizes, rated at 100, 150, 300, and 600 watts. The RWS-B operates from a universal input of 47-63 Hz, 85-265 volts AC (300 volts AC for 5 seconds), and is available with nominal outputs of 5, 12, 24, and 48 volts DC with an adjustment range of a minimum of 10 percent. The convection-cooled 100- and 150-watt models operate from -10 to 70 degrees Celsius with derating above 40 C and the fan cooled 300 and 600 watts models to 70 C with derating above 50 C. In addition over voltage and over current protection is included.

FOR MORE INFORMATION contact **TDK Lambda** online at *www.us.tdk-lambda.com*.

BACKPLANES

3U 17-slot PXI Express backplane introduced by Elma Bustronic

Elma Bustronic in Fremont, Calif., is introducing a 3U 17-slot PXI Express backplane for OEM embedded control and integrated test & measurement applications. The PXI Express backplane meets the PXI Express Hardware Specification Revision 1.0 (with X1 PCI Express connections), and integrates PCI Express in to the PXI architecture. Specific uses include automated test equipment, GPIB-based modular instrumentation, signal generation and analysis as well as high channel-count measurement and data acquisition and control. The PXI Express backplane has one system slot controller and one timing controller slot as well as 15 peripheral slots, each with a PCI Express Gen 1 1X lane to the controller. PXI Express, based on PCI Express, offers high-bandwidth PCI Express connections to modules, enabling to 2.5 gigabytes per second per direction to PXI Express and CompactPCI Express modules.



FOR MORE INFORMATION contact **Elma Bustronic** online at *www.elma.com/en/elma-bustronic*.

CABLING

Rugged optical cable introduced by Molex

Molex Inc. in Lisle, Ill., is introducing expanded-beam ruggedized optical cable assemblies for harsh-environment aerospace and defense applications such as tactical communications, security communications, on-board aerospace and marine networks, and I/O applications in the field. The ruggedized connectors meet MIL-DTL-83526/20 and/21 standards while delivering repeatable, error-free optical transmissions and requiring minimal cleaning.

They can withstand thousands of mating cycles, have a field-installable and repairable design to minimize maintenance downtime, and offer a stainless steel housing option, for corrosive environments. The connectors work by using lenses that expand and collimate the light emitting from optical fibers across a sealed connector interface. The expanded and collimated light beam has an active area much larger than the original optical fiber core, making it less sensitive to data transmission interruption due to dirt and debris particles, while also being more efficient to align across the two connector halves.

FOR MORE INFORMATION contact **Molex** online at *www.molex.com*.

DIGITAL SIGNAL PROCESSING

Rugged Altera FPGA boards introduced by BittWare for SIGINT

BittWare Inc. in Concord, N.H., is introducing the A10 embedded computing family based on the Altera Arria 10 field-programmable gate arrays (FPGAs) and systems on chip (SoCs). BittWare's A10 board family capitalizes on Arria 10 FPGAs's capabilities in challenging applications such as signals intelligence (SIGINT), network processing and security, compute and storage, instrumentation, test and measurement, broadcast, medical imaging, and wireless infrastructure. The A10 board family has flexible memory configurations, sophisticated clocking and timing options, QSFP28 cages that support 100 gigabits per second (including 100 Gigabit Ethernet) optical transceivers, FPGA Mezzanine Card (FMC), and support for the network-enabled Altera SDK for OpenCL. The A10 family comes in half-length PCI Express boards, Advanced Mezzanine Card (AMC), 3U VPX, and 6U VPX.

FOR MORE INFORMATION contact **BittWare** online at *www.bittware.com*.

POWER ELECTRONICS

MOSFET power devices for space-constrained applications introduced by IR

International Rectifier (IR) in El Segundo, Calif., is introducing a family of Large Can DirectFET MOSFET power electronics devices for industrial applications requiring ultra-low on-state resistance, Rds(on), including high power DC motors, DC-AC inverters, and high current switching applications such as active ORing hot swap, and eFuse. The 7-by-9-by-0.7-millimeter Large Can MOSFET devices provide Rds(on) performance leading to lower conduction losses and improved system efficiency, company officials say. Similar to Small and Medium Can DirectFET devices, the Large Can provides dual-side cooling that can make the most of thermal transfer and help increase power density.

FOR MORE INFORMATION contact **International Rectifier** online at *www.irf.com*.

ADVERTISERS INDEX

Military & Aerospace Electronics

PUBLISHER **Ernesto Burden**
603 891-9137 / ernestob@pennwell.com

EDITOR-IN-CHIEF **John Keller**
603 891-9117 / jkeller@pennwell.com

EXECUTIVE EDITOR **Courtney E. Howard**
509 413-1522 / courtney@pennwell.com

CONTRIBUTING EDITOR
WESTERN BUREAU **J. R. Wilson**
702 434-3903 / jrwilson@pennwell.com

EDITORIAL GRAPHIC DESIGNER **Cindy Chamberlin**

PRODUCTION MANAGER **Sheila Ward**

SENIOR ILLUSTRATOR **Chris Hipp**

AUDIENCE DEVELOPMENT MANAGER **Debbie Bouley**
603 891-9372 / debbieb@pennwell.com

AD SERVICES MANAGER **Glenda Van Duyne**
918 831-9473 / glendav@pennwell.com

MARKETING MANAGER **Adrienne Adler**
603 891-9420/ aadler@pennwell.com

PennWell®

Editorial offices
PennWell Corporation,
Military & Aerospace Electronics
98 Spit Brook Road LL-1, Nashua, NH 03062-5737
603 891-0123 • FAX 603 891-0514 • www.milaero.com

Sales offices
EASTERN US & EASTERN CANADA & UK
Bob Collopy, Sales Manager
603 891-9398 / Cell 603 233-7698
FAX 603 686-7580 / bobc@pennwell.com

WESTERN CANADA & WEST OF MISSISSIPPI
Jay Mendelson, Sales Manager
4957 Chiles Drive, San Jose, CA 95136
408 221-2828 / jaym@pennwell.com

REPRINTS **Jeanine Pranses**
717 505-9701 x344 / jeanine.pranses@theygsgroup.com

DIRECTOR LIST RENTAL **Kelli Berry**
918 831-9782 / kellib@pennwell.com

Corporate Officers
CHAIRMAN **Frank T. Lauinger**

PRESIDENT AND CEO **Robert F. Biolchini**

CHIEF FINANCIAL OFFICER **Mark Wilmoth**

Technology Group
SENIOR VICE PRESIDENT/PUBLISHING DIRECTOR
Christine Shaw

Subscription Inquiries
847 763-9540 • FAX 847 763-9607
e-mail: mae@halldata.com
web: https://pennwell.sub-forms.com/PNW20_MFcontact

BPA WORLDWIDE

AMERICAN BUSINESS MEDIA
The Association of Business Media Companies

Q+A

BIO:

NAME: Skot Butler

TITLE: Vice President, Sales, Marketing and Business Development

CO.: IntelSat General Corp.

ROLE: Provides satellite communications solutions to military, commercial, and government customers via 50 satellites and terrestrial network

CONTACT: *www.intelsat.com*

Skot Butler

A high-level satellite communications executive urges government and industry collaboration to strengthen the space infrastructure, as defense officials seek cost-effective access to space.

Is the satellite market changing?

The military uses "contested, congested, and competitive" to talk about the way things are changing. It used to be that only a handful of nations had the capability, interest, and money, frankly, to put things on orbit. That is changing, and there's only so much room up there.

More senior folks within the U.S. Department of Defense (DOD) are starting to believe that not only may it be acceptable for commercial [satellites] to host certain capabilities, but it may be necessary and inevitable. How do they go about doing it smartly? We have been waiting to have these conversations.

What is behind the trend?

What you are seeing is the perfect storm. A lot of people in industry, especially on the commercial side, have been saying this for a long time. Some on the more traditional defense side, that build hardware and dedicated satellites, have come on board more recently; in most cases, that's driven by budget constraints. That final point is really where the DOD is starting to pay attention.

Even though a lot of negatives come with a very constrained and uncertain budget, one of things it has done is drive a lot of very serious considerations for things that only a few years ago might not have been considered.

What types of military hosted payloads are being considered?

There were and remain some mission sets, like wideband communications, that suffer from less resistance, if you will, of entrenched interests for hosting commercially. It's not a big stretch where the DOD might just say 'we don't need our own wideband systems, we can have commercial essentially do all that for us,' host Wideband Global SATCOM (WGS) systems. Some have even said that out loud, in public.

What has been interesting more recently is the DOD, services, and agencies looking harder at commercial supporting the types of missions that might see more resistance: protected communications, infrared, and certain weather missions.

Much of this is still in the study phase, in terms of what the government is actually doing. The Hosted Payload Office in the U.S. Space and Missile Systems Center (SMC) has its Hosted Payload Solutions (HoPS) initiative, and I have heard that there's up to 14 different Analyses of Alternatives (AOAs) across the government that has some bearing on how the government buys its space capabilities.

From our perspective, all this is moving in the right direction. As an owner/operator, we would like the U.S. government, particularly DOD customers, to be customers in a more collaborative fashion, with longer-term planning cycles and a clearer understanding of what the government deems appropriate to be hosted. ←

Don't miss a word

Access the rest of this conversation by visiting *www.militaryaerospace.com/LastWord* or scanning the QR code at left.

Harness the Power of a MIL-SPEC COTS Test Platform

MTS-207 TEST SET
Tough enough for your harshest environments

ULTRA-RUGGED
Ideal for armament, avionics and data acquisition test

CONFIGURABLE
PXI architecture for ultimate customization and expansion

MILITARY AND AEROSPACE PROVEN
Globally deployed in 20 countries

See how the MTS-207 can help you deliver your solution on-time and on-budget. Read our solutions white paper, “Leveraging a MIL-SPEC COTS Test Platform,” at **marvintest.com/flightlinetestsolutions**.

VISIT MARVIN TEST SOLUTIONS AT AUTOTEST 2014, BOOTH 619.

MARVIN TEST SOLUTIONS

Formerly Geotest - Marvin Test Systems

The Marvin Group

MARVINTEST.COM