DECEMBER 2016

Military & Aerospace Electronics®

ENABLING TECHNOLOGIES
FOR NATIONAL DEFENSE

New missile technologies

Army reaching out to industry for enabling technologies in long-range battlefield missiles. **PAGE 4**

Data storage technologies

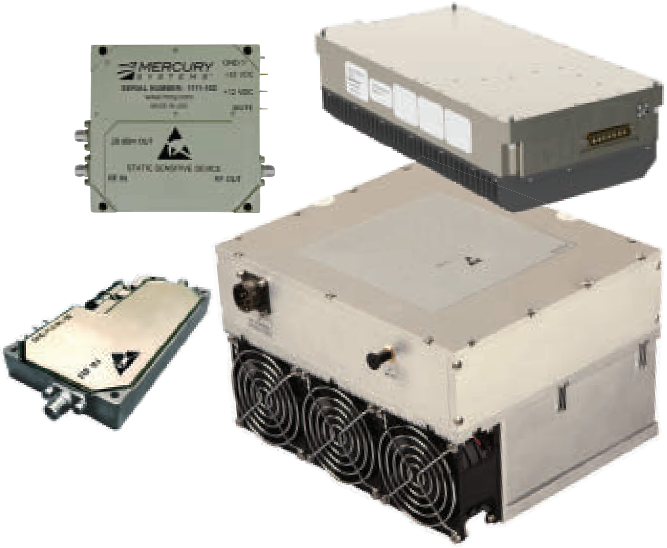
Today's systems need multi-level data encryption, quick erase, and anti-tamper features. **PAGE 16**

militaryaerospace.com

SHADOWY WORLD OF *cyber warfare*

Experts race to create the most foolproof cybersecurity. **PAGE 8**

PennWell®

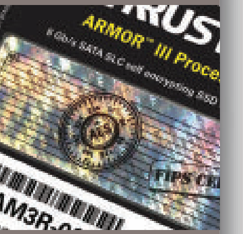

MERCURY SYSTEMS
STATIC SENSITIVE DEVICE
RF IN
RF OUT

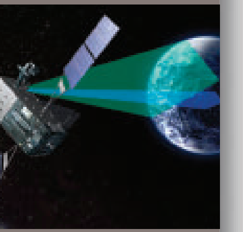
MERCURY SYSTEMS
Gallium Nitride (GaN) Power Amplifier Products

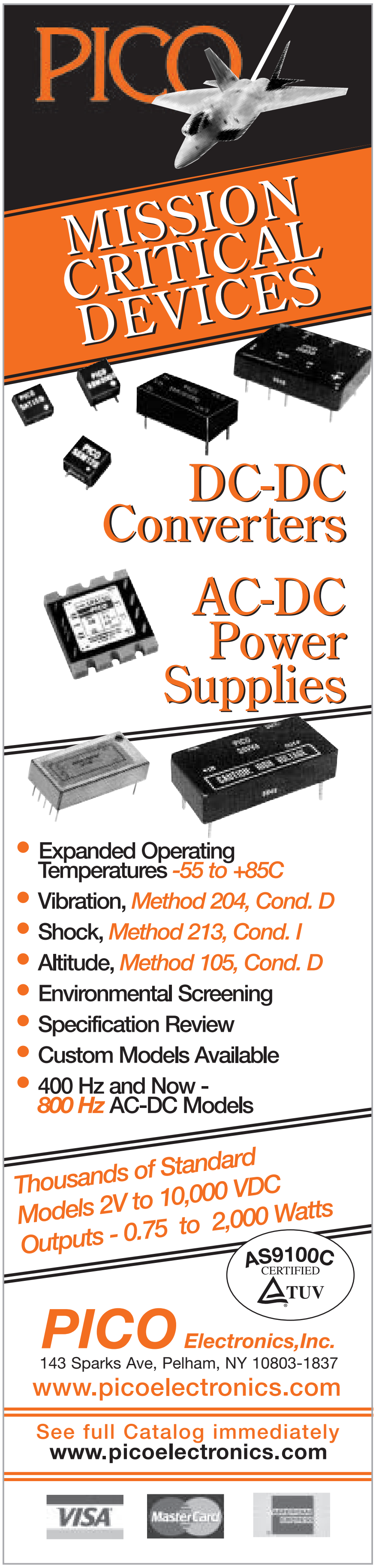
DECEMBER 2016
VOL. 27, NO. 12

Military & Aerospace Electronics

COVER STORY







Military & Aerospace Electronics® (ISSN 1046-9079), Volume 27, No. 12. Military & Aerospace Electronics is published 12 times a year, monthly by PennWell® Corporation, 1421 S. Sheridan, Tulsa, OK 74112. Periodicals postage paid at Tulsa, OK 74112 and at additional mailing offices. SUBSCRIPTION PRICES: USA $175 1yr., $309 2 yr., $440 3 yr.; Canada $270 1 yr., $465 2 yr., $600 3 yr.; International $325 1 yr., $620 2 yr., $810 3 yr. POSTMASTER: Send address corrections to Military & Aerospace Electronics, P.O. Box 3425, Northbrook, IL 60065-3425. Military & Aerospace Electronics is a registered trademark. © PennWell Corporation 2016. All rights reserved. Reproduction in whole or in part without permission is prohibited. Permission, however, is granted for employees of corporations licensed under the Annual Authorization Service offered by the Copyright Clearance Center Inc. (CCC), 222 Rosewood Drive, Danvers, Mass. 01923, or by calling CCC's Customer Relations Department at 978-750-8400 prior to copying. 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 via direct mail, please let us know by contacting us at List Services Military & Aerospace Electronics, 61 Spit Brook Rd Suite 410, Nashua, NH 03060. Printed in the USA. GST No. 126813153. Publications Mail Agreement no. 875376.

BY **JOHN KELLER**, EDITOR IN CHIEF

Defense electronics industry readies for business with Trump Administration

It's only been a month since the U.S. elected Donald Trump as its next president, and the mood of the U.S. defense industry is more upbeat than I've seen it in years.

With just another month until Trump takes office, we've seen stocks of defense companies like BAE Systems and Lockheed Martin increase sharply, new names floated for Trump's secretary of defense, and hints that Trump aims to rebuild U.S. military forces following peace-through-strength policies similar to his predecessor, Ronald Reagan.

You can't blame defense experts for feeling giddy over Trump's election; it's the first political rhetoric we've seen in quite some time concerning a big boost in support for military spending and supporting military priorities.

This is an industry that for the past eight-plus years has lived under a cloud of defense budget reductions, arms-control policies, several threats of across-the-board budget cuts known as sequestration, and a brutal attrition that effectively has hollowed-out the Pentagon's top officer corps. This is an industry that's ready for good news, and Trump's election is more than most ever dreamed. President-elect Trump has voiced military priorities that include modernizing the nation's aging nuclear weapons arsenal; securing critical infrastructure from cyber attacks; and using U.S. military power only to advance American national interests.

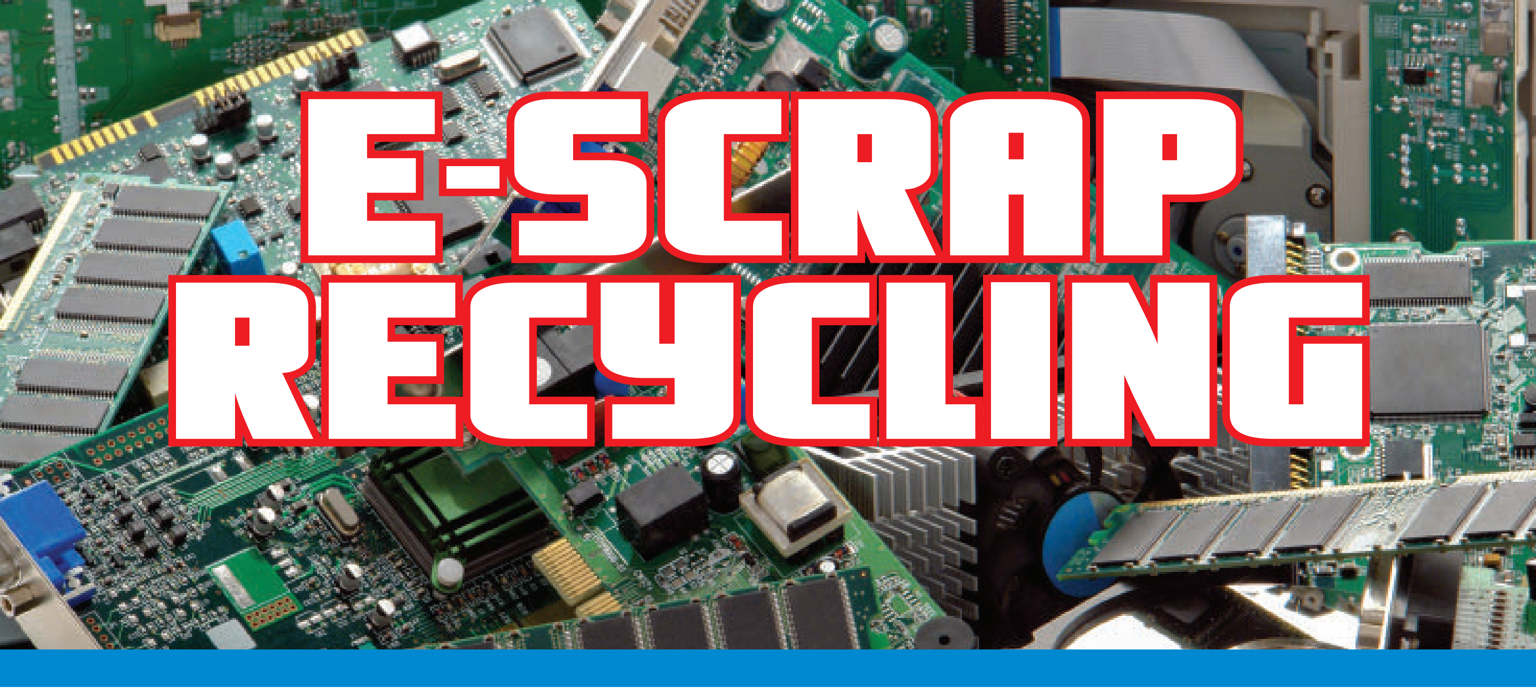
As an aside, however, I would recommend that Americans take a breath before we move forward. Those on the right are ready to let the good times roll, while those on the left are anticipating grotesque violations of human rights. I doubt we'll see either one as expected.

President Trump is bound to frustrate and infuriate those on the right and left in equal measure. He'll be called everything from traitor to the cause to a closet liberal. I think we all can agree that we need a higher employment rate, increases in paychecks, and peace abroad. Let's hope that's the direction we'll go.

On the national security front, it's worth quoting Trump's defense and national security priorities as posted on the president-elect's transition team website at www.greatagain.gov. "America's stature in the world is determined by its values, prosperity and might," the site reads. "Donald Trump understands how a strong, prosperous economy underwrites military might, and how a strong, robust military secures our way of life and the fruits of our economy. Mr. Trump recognizes that we cannot tackle challenges, especially threats to our security, unless we define the problem in a way that American resources and instruments of power can be applied against them.

"To this end, Mr. Trump recognizes the long-term threat posed to our nation and our allies by radical ideologies that direct and inspire terrorism," the site continues. "A Trump Administration will be committed to both immediate and sustainable actions to counter the threats posed by these radical ideologies. A Trump Administration also recognizes the uniquely catastrophic threats posed by nuclear weapons and cyber attacks. Mr. Trump will ensure our strategic nuclear triad is modernized to ensure it continues to be an effective deterrent, and his Administration will review and minimize our nation's infrastructure vulnerabilities to cyber threats. Mr. Trump will be a strong Commander-in-Chief befitting our American men and women in uniform, and ensure their sacrifices will only be made in operations that safeguard the interests of the American people and our allies, and that their service will be honored as they enter the ranks of veterans."

Attentions are now turned to those who might head-up Trump Administration cabinet and other senior-level positions for defense and national security, such as secretary of defense, secretary of state, secretary of homeland security, and director of national intelligence.



Army eyes enabling technologies for MLRS long-range tactical missiles

BY JOHN KELLER

REDSTONE ARSENAL, Ala. — U.S. Army fire-support experts are reaching out to industry for help in developing enabling technologies for a long-range tactical missile able to hit stationary and moving targets about 200 or more miles away.

Officials of the Army Contracting Command at Redstone Arsenal, Ala., issued a broad agency announcement (W31P4Q-17-R-0028) for the potential $148 million New and Innovative Technologies for Long Range Fires Technology Development and Demonstration project.

It seeks to develop component and systems-level technologies for a new generation of tactical missiles that can be fired from the Army's Multiple Launch Rocket System (MLRS). The longest-range missile that MLRS can fire today is the Lockheed Martin MGM-140 Army Tactical Missile System (ATACMS), with a maximum range limited to 300 kilometers, or about 189 miles.

The project seeks to enhance the range, precision, and lethality of Army long-range fires against stationary and mobile land and sea targets, at ranges beyond 300 kilometers. The Army Contracting Command is issuing the solicitation on behalf of the Weapons Development & Integration Directorate of the Army Aviation & Missile Research, Development & Engineering Center (AMRDEC).

The new long-range tactical missile should be able to function in all operating environments, and be compatible with MLRS launchers "to the greatest extent possible."

At this stage, Army researchers are trying to advance the state of the art in tactical missile inertial navigation; multi-mode seekers; high-temperature seeker dome materials; signature reduction; warheads; digital data links; propulsion; and attitude control. Army experts are asking industry for proposals on new and innovative technologies that focus on one or more of these technical areas.

The Army is asking industry for enabling technologies for a new generation of long-range tactical missiles like the ATACMS, shown above.

Inertial navigation involves highly accurate, low-cost inertial sensors that enable precision long-range navigation in environments where reception of global positioning system (GPS) satellite navigation signals are degraded or denied.

Multi-mode seekers involve active and passive seekers that enable

IN BRIEF

Raytheon eyes revolutionary new testing for SM-3 missile circuit cards

Missile experts at Raytheon Co. will carry out revolutionary new test and measurement procedures for circuit cards of the U.S. Navy Raytheon Standard Missile 3 (SM-3) under terms of an $18.2 million contract modification. The Missile Defense Agency (MDA) is asking Raytheon Missile Systems to develop testing for circuit card assemblies and circuit card stacks using the Presidio Gen 2 Block IV/V automated test architecture for the SM-3 Block IIA missile. The Presidio Gen 2 Block IV/V automated test architecture represents a breakthrough in testing automation for production of Raytheon's SM-3 missile. It replaces 17 test positions and 27 environmental conditioning systems with one automated installation. SM-3 missiles are part of the armament for Navy Arleigh Burke-class destroyers and Ticonderoga-class cruisers. These missiles can acquire, track, and destroy incoming ballistic missiles.

target detection, acquisition, tracking, discrimination, and aim-point selection in GPS-degraded or -denied environments.

High-temperature seeker-friendly dome materials should be able to withstand the temperature extremes of extended-range, high-velocity flight profiles, while making the most of radar, infrared sensors, or other kinds of seekers.

Signature-reduction technology involves making these new munitions stealthy and difficult to detect by radar, infrared sensors, or other kinds of target-detection systems.

Warhead technology involves kinetic and non-kinetic ways to enhance lethality with relatively small size, weight, and power consumption (SWaP). Propulsion technology, meanwhile, involves enhanced performance in hybrid, gel, liquid, or air-breathing solid rocket motors for long-range missions.

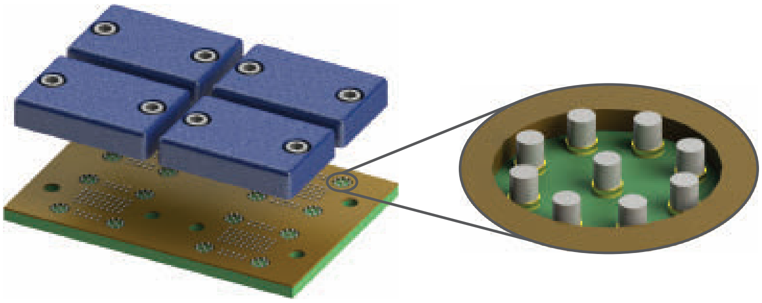
Digital datalink technology involves communications for integrating smart munitions in a secure battlefield network for synchronizing weapon aim points and arrival times. Attitude-control technology, finally, involves advanced divert thrusters, canards, fins, and jet vanes for improved weapon maneuverability and reduced SWaP.

After these enabling technologies are developed, Army researchers would like to test them together in a sub-scale or full-scale flight test. All technologies developed in this program will be subject to International Traffic in Arms Regulations (ITAR) regulations, and the project is not open to foreign participation at any level.

Army researchers first want concept papers from interested companies, and those submitting the most promising papers will be invited to submit full proposals. Several companies could be chosen to participate in this program with four-year contracts worth between $1 million and $135 million apiece.

Companies interested should e-mail concept papers no later than 24 Oct. 2017 to the Army's Candace Tucker at candace.s.tucker.civ@mail.mil, with a copy to Janet Childers at janet.childers@us.army.mil. ←

MORE INFORMATION IS online at *http://bit.ly/2gQQCz2*.



Sierra Nevada demonstrates helicopter synthetic vision for degraded visibility environments

BY JOHN KELLER

YUMA PROVING GROUND, Ariz. — U.S. Army helicopter aviation experts are moving forward with a program to use synthetic vision technologies to enable rotorcraft pilots to take off and land in degraded visibility environments (DVE) from blowing dust, snow, or other conditions that make it difficult to see.

Officials of the Aviation and Missile Research, Development and Engineering Center (AMRDEC) at Redstone Arsenal, Ala., are working with avionics designers at Sierra Nevada Corp. in Sparks, Nev., to develop and demonstrate degraded visual environment (DVE) technologies to mitigate the effects of brownout or whiteout conditions on helicopter pilots.

Sierra Nevada Corp. engineers are using their company's synthetic vision technology to help helicopter pilots land in zero-visibility conditions.

Landing a helicopter in choking dust or blinding snow can be particularly difficult because pilots can become disoriented easily near the ground as they lose view of the horizon and other visual cues.

Sierra Nevada engineers displayed advancements in the company's synthetic vision technology during demonstrations at the DVE Mitigation (DVE-M) program's NATO Yuma Flight Trials in Yuma, Ariz., company officials say.

The DVE-M program is a multi-year U.S. Army research effort to ground and flight test sensor, flight control, and cueing technology combinations to provide helicopter pilots with visual awareness in DVE environments, such as brownout conditions.

Brownout from dust and whiteout from snow are particularly dangerous for helicopter pilots because without help pilots can lose track of the horizon during critical moments in takeoff and landing. This can cause pilots to roll the aircraft while close the ground, which risks hitting the rotors on the ground or other nearby objects.

For the DVE-M program, Sierra Nevada engineers are focusing on real-time fusion of multi-sensor data from millimeter-wave radar, light detection and ranging (LIDAR) sensors, infrared cameras, and various a-priori digital terrain data, company officials say.

During recent tests at Yuma Proving Ground, Sierra Nevada's DVE technology enabled pilots to conduct more than 86 safe approaches to hover and landing in dust and heavy brownout conditions.

Next February, Sierra Nevada will demonstrate company DVE technology again at the European NATO DVE Flight Trials, focusing on additional degraded visual conditions involving fog, rain, sand, and snow.

Applicable to helicopters and fixed-wing aircraft, Sierra Nevada's DVE solutions provide increased flight safety and operational capability for all modes of flight in natural and aircraft-induced DVE by restoring pilot situational awareness through real-time, multi-sensor fused imagery, company officials say.

In mid-2013, the Aviation Applied Technology Directorate of the Army Research, Development, and Engineering Command at Fort Eustis, Va., awarded a contract to Sierra Nevada to integrate and test the company's Helicopter Autonomous Landing System (HALS) aboard an Army UH-60A/L helicopter as part of the AMRDEC DVE-M program.

The Sierra Nevada HALS helicopter avionics use a 3D image-rendering 94 GHz pulsed radar, global positioning system (GPS), inertial sensors, and cockpit displays to help helicopter pilots view geographic features outside the aircraft during brownouts and whiteouts from dust, snow, or other visual impairments.

The HALS system uses radar data translated to color graphic representations on cockpit displays to help helicopter pilots control the aircraft's roll, pitch, and yaw based on radar-generated graphic representations of the ground and nearby geographic features in zero-visibility conditions.

The HALS avionics enables helicopter pilots to take off, land, and fly in all degraded visual conditions, provides visual situational awareness to enable pilots to see and avoid wires, cables, and terrain, as well as follow landmarks in poor visibility.

The system also includes Brownout Symbology Software (BOSS), precise guidance to landing in zero visibility, and safe transition from visual to instrument flying conditions.

FOR MORE INFORMATION visit **Sierra Nevada Corp.** online at *www.sncorp.com*, and the **Army AMRDEC** at *www.army.mil/info/organization/unitsandcommands/commandstructure/amrdec*.

THE SHADOWY WORLD OF CYBER WARFARE

Private industry and government agencies push technology in the race to create the most foolproof cybersecurity. BY **J.R. Wilson**

Cyber warfare still is a relatively new concept, for the military and civilians. To some it is an offshoot of electronic warfare (EW) or information warfare or even signals intelligence (SIGINT). A common definition calls it "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." It has rapidly evolved and expanded in the 21st Century, so that definition is far too limited.

More recent definitions have expanded to include non-state actors: terrorist groups, corporate espionage, political and ideological extremist groups, individual or small group hackers (aka, hacktivists), and transnational criminal organizations, such as the drug cartels and various "mafias." That diversity, however, also raises the difficult separation of cyber warfare from cybercrime, which share many of the same techniques and technologies and often lead to common results.

The major public emphasis has remained centered on national militaries, especially the U.S., China, Israel, Russia, the United Kingdom, Germany, France, and Iran. All have their own equivalents of the U.S. Cyber Command (CYBERCOM), stood up in mid-2009 as a sub-unified command subordinate to U.S. Strategic Command, but operated by the National Security Agency (NSA). CYBERCOM's charter was to pull all existing military cyber resources together, creating synergies, and synchronizing combat effects in defense of the information environment.

ABOVE: An Air Force network administrator prepares a server for a command cyber readiness inspection.

The U.S. Army Cyber Center of Excellence brings cyber experts together from the military services to define best practices for cybersecurity.

Officially, it “plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified military information networks and prepare to and, when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace, and deny the same to our adversaries.” While it began with a predominantly defensive posture, it increasingly has looked to offensive strategies and technologies, as well.

Efforts to develop military cyber capabilities — offensive, but especially defensive — are now as common among nations of all sizes and strengths as the possession, use, and production of unmanned aerial vehicles (UAVs). Even more than UAVs, however, cyber already is a critical and ubiquitous component of society, from grade-school students’ tablets to international financial records and transactions, from individual cell phones to top-secret military satellites, from personal computers to national power grids.

Defining cyber warfare

This has made the term “cyber warfare” universally all-encompassing and confusing. That also is true for its place in the military — as a capability, offense, and defense, or as a new and separate “fifth operational domain,” equal to land, sea, air, and space. Some even predict all five soon will be superseded by a sixth domain — a combination of information operations (IO) and brain-computer interface (BCI) to control the human mind by manipulating emotional and cognitive responses or by exploiting man-machine technology.

The U.S. Army Cyber Command is one of many organizations in the U.S. Department of Defense seeking innovative cyber defenses.

The growth and development of cyber security attack and cyber warfare strategies and technologies also has led to the creation of Cyber Centers of Excellence (CoE). These range from private corporate entities like the Lockheed Martin Cyber Center of Excellence (CoE), opened in late 2015, to national entities like Germany’s

Nationale Cyber-Abwehrzentrum (National Cyberdefence Centre); to international entities like NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Tallin, Estonia, and the European Cyber Security Organisation in Belgium.

"When we stood up our CoE late last year, it really focused on where we thought the future of cyber was going in the new warfighting domain," says Doug Booth, director of cyber and EW business development at Lockheed Martin. "The CoE is a combination of all our programs and engineers and consultants, coming together as one to help protect our customers, deliver capabilities, and look at the future to see what challenges we can help our customers overcome.

"It is more than a think tank; it's where all our internal business and external customers go when they have a challenge and where we bring in individuals who are interested in learning about what capabilities we have. We resolve problems, tabletop exercise problems, taking a multi-task approach."

Lockheed Martin's CoE has four pillars:

- networks and infrastructure, which build capability to secure, attack, and defend;
- weapons systems, which cyber warfare and EW to target and exploit adversary weapons systems;
- U.S. Department of Defense (DOD) platforms, which build resiliency into those platforms to ensure they are cyber-protected and can operate when under cyber attack in all warfighting domains; and
- international, which take any export-controlled capabilities and push them into relevant cyber programs internationally.

"Where we can get export approval, we're more than willing to take our capabilities, mostly defensive at that point, into those regions," Booth adds.

Cyber centers of excellence

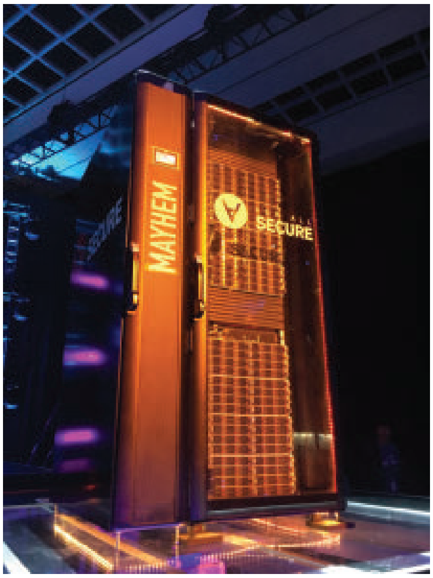
NATO's Cooperative Cyber Defence Centre of Excellence was established in 2008 following significant cyber attacks in Estonia in 2007. Henry Rõigas, researcher, CCDCOE Law and Policy Branch, emphasizes that while the Centre tries to provide

the organization with a 360-degree perspective on cyber defense, it is not tasked by NATO nor part of the alliance's command or operational structures.

"The attacks served as a kind of wake-up call to NATO that cyber defense security is an issue NATO cannot ignore. However, Estonia already had planned to establish the Centre before that, so it was not created directly because of the cyber attacks," Rõigas says. "Basically, we function as a think tank, providing support to NATO and its members, but funded by voluntary contributions, currently from 16 NATO member nations and some non-NATO contributing members, such as Austria and Finland.

"Our role is to provide knowledge, functioning as a research center, education and knowledge hub, provide training exercises and presentations on cybersecurity from different perspectives. I am part of the Law and Policy Branch, which focuses on international law and policy," Rõigas says. "We also have a technology branch, who are penetration testers and monitors; a strategy branch that focuses mainly on military and strategic questions; and an education branch that supports NATO's exercises and organizes our exercises and training."

According to the "Tallinn Manual on International Law Applicable to Cyber Warfare," a study commissioned by CCDCOE that is not considered a legally binding document, cyber weapons are cyber means of warfare designed, used, or intended to cause either injury or death of people or damage to or destruction of objects. The scope and limitations of that definition are critical to the potential implementation of NATO Article 5, which says an attack on any NATO member is considered an attack on all and NATO will respond accordingly.



The DARPA Cyber Grand Challenge winner was the ForAllSecure Mayhem, an autonomous software program able to find weaknesses in a target system and repair them in minutes, even seconds.

"In 2014, in the Summit declaration, NATO signaled that if a cyber attack reaches a certain threshold, the NATO decision-making body may decide Article 5 may be invoked. That will happen on a case-by-case basis and to date no cyber attack has reached that threshold under international law. The consensus among lawyers, politicians, and nations is the decision to invoke Article 5 in a cyber attack means the results must equal the results of a kinetic attack: deaths, injury, etc.," Rõigas explains.

"That does put out a definite deterrent effect. The main strategic question for us is how to deter the most common attacks that do not yet reach that very high threshold, such as espionage. So far, states with cyber capabilities have shown restraint with respect to very large-scale cyber ops that would reach that trigger threshold. It's clear the opportunities and capabilities are there, but so far those states have not gone that far," Rõigas says.

Cyberterrorist weapons

Rõigas says the Centre does not believe such an attack is likely, at least not in isolation — that should an Article 5-level cyber attack take place, it would be in concert with more traditional kinetic attacks. At the same time, he acknowledges "it still is a new area and things are not entirely clear. Nations are trying to determine how to live with everything that is developing, through international law and policy, etc., but cyber is so huge and has so many perspectives, it is difficult to focus."

He also is far less concerned than many others about non-state actors using cyber weapons, despite the increasingly easy and cheap availability of sophisticated systems on the open commercial market, much less the traditional underground weapons market, now residing largely in the so-called "dark web" — a majority of all Internet websites, but not seen by search engines such as Google and Yahoo.

"The private sector development of new technology is a race for innovation, with a market failure programmed in where manufacturers don't focus on security so much as new technologies that will sell," Rõigas says. "That will enable smaller players to pull off one-time effects. You can go onto the dark web and buy off-the-shelf hardware and software so you really don't need technical knowledge to conduct operations on that level. This is why rogue actors, tier 2 nations, have more opportunities in the future.

"At the moment, the consensus is terrorist organizations don't have the capability, know-how, or motivation to conduct high-level ops through cyberspace. They can more effectively use older methods, such as suicide bombs, which are cheaper and require less knowledge, to achieve their goals. A terrorist's main goal is to create fear, typically through bloodshed; while a cyber attack can be very effective, from a terrorist perspective, it makes more sense to use traditional means of attack."

In recent years, the Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., has used a series of challenges to encourage industry and private groups to push cutting-edge technology beyond its current boundaries and provide proof-of-concept demonstrations. In August 2016, DARPA's latest such effort, the Cyber Grand Challenge, concluded with a start-up company called ForAllSecure as the victor with a software program called Mayhem, a fully autonomous system capable of finding weaknesses in a target system and repairing them in minutes, even seconds.

Unlike the real-world threat, however, DARPA restricted the challenge to memory safety vulnerabilities and information leaks.

Cyber Grand Challenge

"Our goal is to be able to check everything, check the world's software for exploitable bugs, from mobile phones to battleships," says David Brumley, ForAllSecure's CEO and co-founder. "In the challenge, there was exploit — find and prove vulnerabilities — and auto patching software to defend against vulnerabilities. It went beyond strategy to include winning technology.

"Part of our strategy was creating a suite of patches, so every time we got a new program as part of the challenge, our automated cyber reasoning system looked at our suite of patches and picked the one that worked best, that didn't slow the software down or interfere with its functionality," Brumley says. "We were given programs we'd never seen before, so our system had to auto-identify possible vulnerabilities, but it also looked for common security measures. For example, hardening, which is like adding airbags to protect against a lot of problems and not specific to anything."

Brumley, who also is director of the Carnegie Mellon CyLab Security and Privacy Institute, is one of many in the cybersecurity and warfare arena who believe offense and defense are opposite sides of the same coin.

"In my view, offense and defense are tied as mission areas. In both, you want to identify vulnerabilities and prove they really are vulnerabilities. I think what we developed can be applied to offense and defense," he says.

"When you look at national security, automating these tools has given us the capability to look at a much larger variety of software than ever before. Offense often focuses on specific programs or hardware and is limited to experts on those. We enable them to look at all programs without targeting anything ahead of time," Brumley says.

> "Cyber warfare is a great alternative to conventional weapons… it is cheaper for and far more accessible to these small nation-states. It allows these countries to pull off attacks without as much risk of getting caught and without the repercussions when they are." — Amy Chang, research associate, Center for a New American Security

Lockheed Martin's seven-step "cyber kill-chain" to defend against an advanced attack would appear to support that premise as company experts look to a future of smarter adversaries and greater difficulty identifying the source of an attack.

"Following the seven steps helps understand what is happening, where you have potential vulnerabilities, and track an attack," Booth says. "On the offense side, we build exploit and attack capabilities, some under IRAD [independent research and development]. One of those is a specific technology built to do a D5-type disruption [deception, denial of service, disruption, degradation, destruction] focused on cellular systems — LTE disruption. That is ready for marketing and has been flown on UAVs, field-tested and demonstrated in the past 18 months."

The seven kill-chain steps are:

1 — reconnaissance
2 — weaponization
3 — delivery
4 — exploitation
5 — installation
6 — command and control
7 — action-on-objectives

"These are the steps an attacker would take in trying to penetrate your network. By identifying these and the particular tools and payloads they would build for each step, then building countermeasures for each of those, you can create a seven-layer protection for your entire network," Booth continues. "It can identify new activity, regardless of adversary, new techniques versus old techniques, looking inside and outside your network. We also keep a large repository of available technologies and can look to that to help identify an attacker.

"When you think about how wars will be fought in the future, I think they may begin with non-kinetic cyber warfare and EW. With software-defined radios and miniaturization, you now have the ability to take systems that once were built separately — some for EW, some cyber warfare, some SIGINT — and pull them into one multifunctional system that can determine the best approach for going after a target," Booth says. "You now can conduct your mission, whichever of those it may be, from one platform; the customer will be able to decide whether to use an EW technique or a cyber technique or even use both simultaneously. Basically, EW technology is more temporary, cyber warfare more permanent."

The growing vulnerability of every segment of global society has many fathers: the shift of advanced technology development from the military to the commercial sector; the ubiquity of increasingly connected electronics, the Internet of Things (IoT); mass-market commercial manufacturers placing customer-attracting new technologies ahead of built-in security measures; a general lack of knowledge or understanding of cyber vulnerabilities among consumers and as-yet-unresolved cyber disparities within the military.

"The cyber threat reaches beyond traditional information technology networks and computers to systems that affect nearly every aspect of the Navy's mission; this increased attack surface makes defending Navy data, systems and networks more challenging." — Troy Johnson, director, Navy Cyber Security Division

That is further complicated by a continuing U.S. belief in secrecy that has limited the number of qualified people able to work on classified government projects, while International Traffic in Arms Regulations (ITAR) restricts international cooperation and co-development. Distrust among European and other nations, with respect to the most advanced cybersecurity developments, also remains high.

Cyber personnel

"Current technology in every country relies on people, which takes considerable skill and time — and industry can pay them a lot more than any government," Brumley says. "National attitude also is important. Countries like Israel tend to have a significant interest in automated tools and are a lot more explicit in asking for them.

"The U.S. still thinks hackers are bad guys and finding vulnerabilities should be locked inside a black room. Developers of that capability are a lot more socially acceptable in other countries, from Israel to China, who are not as concerned about these kinds of capabilities being out there in the public."

Rõigas agrees, saying balancing a fundamental need for secrecy in developing cyber/counter-cyber technologies and capabilities with an adequate level of cooperation among the NATO allies is one of the most important issues surrounding cybersecurity in general.

"That is especially so where allies view these capabilities as something very strategic and are reluctant to share this kind of information, which can be a frustration to cooperation. That also influences researchers, who often make assumptions based on very limited information in trying to understand what various states are doing, especially in terms of offensive operations," Rõigas says. "But I think the states are becoming more open and understand we need more cooperation.

"The U.S. is the biggest and most advanced cyber power, but you also have Germany, France, and the U.K. Politicians often say there is a low level of entry into cyber and small states can push beyond their weight, but when you consider strategic military offensive capabilities to conduct sophisticated operations on a large scale, you have to look at those countries with other major military capabilities. Which is why cyber really has not changed the balance of power," Rõigas says.

NATO's own cyber defense policy highlights each nation's responsibility to defend its own networks. Which, without significant sharing of cyber warfare capabilities, means those with fewer resources and national military capabilities probably are the most vulnerable.

Shrouded in secrecy

Secrecy is even more prevalent among potential adversaries — China, Russia, Iran — with the first two widely regarded as already having conducted cyber ops, from largely espionage-based penetrations by China to Russia's cyber takedown of the electric grid in western Ukraine. But the general consensus is the Stuxnet attack on Iran's nuclear research facility, for which no nation has taken credit, was created and launched by the U.S. and Israel. None of those, according to Rõigas, met the threshold for Article 5.

"The truth is, we just don't know every nation's real capabilities because there are vulnerabilities in critical infrastructure and other systems where a lot of things can happen," Rõigas says. "So it's a game of assumptions."

U.S. Cyber Command seeks to pull all existing military cyber resources together to find the best approaches to offensive and defensive cyber warfare operations.

Military cybersecurity requirements range from the individual warfighter, now heavily equipped with networked electronics, to ships, aircraft, and satellites.

"Platform protection is applying cyber protection to big platforms to ensure our adversaries do not disrupt their capabilities through anti-tamper, secure processing, and electronics design, ensuring these systems are built following risk-management framework guidelines," Booth says.

"It begins with an awareness of the possible vulnerabilities, then building resiliency into those platforms [on the production line]. That would include ground vehicles, communications systems, sensors, etc., starting with the large platforms and working down, but the focus is on larger platforms, not individual warfighter gear."

Cyber arms race

Although cybersecurity and cyber warfare organizations have proliferated to virtually every military, government, academic, industrial, and commercial organization worldwide, the future of cyber/counter-cyber remains murky, at best — a new domain of warfare no one fully understands nor knows for certain what others, friend and foe, understand.

"We're in a race. I don't think anyone is ahead in any big way among our competitors. The U.S. doesn't want an even fight; we want overwhelming superior technology. DOD's Third Offset Strategy means we don't want to match the enemy tank-for-tank, but offset any larger numbers they may have with superior technology," Brumley concludes.

"First was nukes, second precision, and the third will be autonomy — not just physical, but cyber autonomy. China has 22 percent of the world's population and so may have 22 percent of the world's cyber experts, compared to 6 percent in the U.S. So we have to make sure our 6 percent are better than their 22 percent — that is modern warfare with the U.S. in a nutshell." ←

Security and solid-state media driving data storage

It's not enough to have rugged data storage with massive capacities and solid-state storage technology; today they also must offer multi-level data encryption, quick erase, and anti-tamper features.

BY **John Keller**

The rugged data storage business today is just as much about information security as it is about the actual storage media.

It's a given that mission-critical aerospace and defense applications must store data on rugged and reliable disks and drives, yet today's attention to cyber security also demands that data be reliably secure once it's stored.

This confronts aerospace and defense electronics systems designers with a doubly difficult challenge for the future, because the military's appetite for data never stops. Today we're talking about rugged data storage systems able to hold terabytes of information, and a growing amount of it has to be secured.

In the recent past, systems designers used to talk about the need for megabytes and gigabytes of data storage capacity. Today we talk about terabytes, and soon petabytes, exabytes, and even zettabytes may enter the conversation. The continuing explosion of sensors, intelligence-gathering platforms, and real-time tactical networking all will keep the pressure on military data storage technologies.

Data storage media

Where years past saw a relatively even distribution in solid-state data storage and rotating magnetic media, the past two to five years have seen trends toward solid state. Today almost all aerospace and defense data storage for deployed applications have moved to solid-state memory.

"For us, we are focused on deployed applications, so it is really solid-state drives for us now," says Paul Davis, director of product management at the Curtiss-Wright Corp. Defense Solutions Division in Ashburn, Va.

The one-terabyte TRRUST-StorR SATA SLC self-encrypting solid-state drive (SSD) from Mercury Systems offers data protection and data management, protection from silent data corruption, and operational stability during power interruptions.

"With solid-state costs coming down so much, we can get multi-level cell technology that supports wide temperature ranges," Davis says. "There hasn't been applications where we can't use them."

Although rotating magnetic storage media may have its niches, it's largely disappearing in deployed military applications. "Most of our applications involve removable storage to take back to a ground station," Davis says. "You need to remove and carry those drives, and even the transport of rotating drives could get high levels of shock. Solid-state drives are more reliable."

It's the same across many data storage applications for rugged deployed systems. "Everything we are involved in is solid state," says Ian Mackie, vice president and general manager of the Mercury Systems Microelectronics Secure Solutions business unit in Phoenix (formerly White Electronic Designs Corp.). "Out in harsh environments where special security is a concern, I'm not aware of any rotating media anymore."

Rugged and reliable storage

Not only have the costs of solid-state data storage come down drastically over the past five years, but its reliability also has improved. "The technology is getting better and better," says Rodger Hosking, vice president at Pentek Inc. in Upper Saddle River, N.J. "A major benefit of the last five years has been solid-state drives are much faster and are suitable for high-vibration environments. They are smaller, lower weight, and the pricing is driven by commercial devices."

One knock against solid-state data storage in previous years was its endurance. Drives wore out in data-intensive applications if data transferred to data cells too many times. A lot of that has changed, Hosking points out. "There are more and more endurance cycles, and this is changing every few months."

Pentek and other companies that build and design-in solid-state storage are using a technology called wear leveling. This involves a data controller that keeps track of the number of times data writes to a solid-state drive's data cells. Then the controller distributes writes evenly to the drive's data cells so as not to use one memory cell too many times and wear it out.

Amos Deacon III is president of longtime military data storage specialist Phoenix International in Orange, Calif. While Phoenix worked for years to ruggedize rotating magnetic disks for military and aerospace applications, much of the era of rotating media is coming to a close, Deacon acknowledges.

“Certainly it’s heading in that direction; there’s no doubt,” Deacon says. “We have seen a significant increase in volume in our solid-state drives in the embedded space — particularly in the OpenVPX form factor, but also in our RAID disk array systems.”

Although the cost of magnetic data storage still is far less than solid state, the price of solid-state storage has come down sufficiently to make it the more attractive option for aerospace and defense applications, Deacon says.

Phoenix International’s RPC24 high-performance Fibre/SAS/iSCSI Host Channel, 6-gigabit SAS/SATA III solid-state/hard disk drive RAID subsystem offers self-encrypting drive (SED) technology, and support FIPS 140-2 certified AES 256 encryption as well as instant secure erase.

The Pentek RTR 2623 6GHz RF Sentinel intelligent signal scanning portable, rugged recorder has an integrated 6GHz RF down converter for real-time signal monitoring and detection that is user configurable.

“I believe that the price point for SSDs has come to the point where it makes more sense for the users — for its performance and its environmental characteristics,” Deacon explains. “For airborne applications, almost everything we see these days is solid-state disk. The hard drive’s big drawback is it needs an atmosphere to operate. Up above 10,000 feet, there is not enough air for the heads inside the hard drives not to crash against the disk of the storage media.”

The big transition from rotating media to solid-state storage in aerospace and defense applications started about two years ago, and continues at an accelerating rate. “About two years ago, we started seeing a number of tech refreshes where we swapped-out rotating for solid-state disks,” Deacon says. “What started people going in that direction was the overall reliability in those deployed environments.”

In rugged conditions, there’s just no beating solid-state storage these days, Deacon says. “In temperature extremes, altitude, and shock and vibration, it’s much easier to create a system where you don’t have to worry about cooling and shock isolation to the extent you did with a rotating hard drive,” he says. “You still pay more for SSD, but you benefit on the back end because systems don’t have to be so complex.”

Data storage and data recording

Although a prime consideration in data storage is the sheer capacity of data-storage systems, a close second consideration is the speed at which a data-storage device can write and read data. Those systems designed reliably to read and write data in real time typically are called data recorder systems, rather than data storage.

“The difference between data storage and data recording is whether it is real time, or not,” explains Pentek’s Hosking. “With data recording you need to be doing it in real time. The whole key for what we do in recording is to guarantee we absolutely record data in real time, and never drop one bit of data that is being acquired. Eventually we will run out of total size, but that is a secondary concern to the rate at which we store data.”

Data recorders typically are for intelligence-gathering systems that may have only one chance to capture crucial information on an adversary’s radar system, new weapon, or military communications system.

Three things are key to a data recorder’s speed. The first is how quickly analog information can be converted to digital data via analog-to-digital (A/D) converters. The second is the speed of a redundant array of independent disks (RAID) controller, and third is the speed of the data-storage medium itself.

As far as the storage medium is concerned, solid-state is the choice for data recorders because it offers so much faster read and write speeds.

“SSD is much faster than the magnetic rotating drives we used 10 years ago,” Hosking says. “We are constantly looking for the fastest data converters, the fastest RAID controllers, and the fastest storage media like solid-state drives.”

A/D converters switch analog signals like radio waves into digital information. RAID controllers move digital data from A/D converters to the storage media. The storage media is where the data ends up. A delay in any of those three segments can spell the difference between real-time data recording, and non-real-time data storage.

“The price of solid-state storage has come down sufficiently to make it the more attractive option for aerospace and defense.”

Another technology advancement contributing to the speeds of data recorders are bridge chips that tightly couple PCI Express switches to multi-core microprocessors, Hosking says.

“That chipset provides an extremely high-speed path between PCI Express peripherals like data-acquisition boards and the RAID controller we are using for writing to the disks and to system memory,” Hosking says. “We manage the interfaces on our boards from high-speed data converters through to PCI Express so we can write to system memory in real time.”

With today’s data conversion and RAID controller technologies, data recorders can store data in real time at a bandwidth of about

1,500 MHz, says Pentek's Hosking. "We can do a lot of what's out there with what we have today," Hosking says. "Soon we will be able to double that with new products we are working on right now to get to 2.5 to 3 GHz signal bandwidth."

There may come a time when technology advancements will blur the line between data recording and data storage. Phoenix's Deacon points to a new technology called Non-Volatile Memory Express (NVM Express). This eliminates the SATA or SAS interface and connects data storage directly to the PCI Express bus.

"In effect you're bypassing a network interface card, and the data storage connects directly to the CPU; it's extremely fast," Deacon says. "With NVM Express you're talking about 2,000 to 3,000 megabytes per second. It's a quantum leap in performance."

Security in data storage

With all the issues surrounding data storage for aerospace and defense applications, volume and speed of storage don't make up the whole picture. Data storage needs big volumes and fast speeds, but it needs security, too.

"Security is as important as anything else, and perhaps more important with regard to the nature of the data we are storing," says Mercury's Mackie. He's not the only such proponent. "In just about any new program we work with now requires some level of data encryption," echoes Phoenix's Deacon. "If you're not able to support that, you're not a player."

The trend today is for ever-growing amounts of security in data storage. "I really see the trend heading toward more security," says Bob Lazaravich, director of research and development at the Mercury Systems Microelectronics Secure Solutions business unit in Phoenix. "Historically for cost reasons people have been using commercial drives not purpose-designed for this kind of application. That has been the trend, but in military applications we are considering military-level security, and unfortunately that's not free."

The Curtiss-Wright Data Transport System (DTS1) is a rugged network attached storage (NAS) file server for use in unmanned aerial vehicles (UAVs), unmanned underwater vehicles (UUVs), and intelligence, surveillance, and reconnaissance (ISR) aircraft.

The chief concern of information security for data storage is preventing crucial data from falling into the wrong hands, whether the data drive has been lost, stolen, or captured. There essentially are three ways of doing that: encrypting the drive, erasing the drive, or sanitizing the drive. A fourth measure involves anti-tamper, which carries out one of the first three if sensors detect unauthorized attempts to access the data.

"I could envision a day coming when all military data storage will at least require encryption," says Curtiss-Wright's Davis.

Data encryption

The first way to keep stored data out of enemy hands is encryption. This involves using an encryption key to write and read data.

There are several encryption schemes to secure military data, ranging from those administered by the National Institute of Standards and Technology (NIST), to higher levels of classification administered by the National Security Agency (NSA).

One good commercial level of encryption is FIPS 140-2, administered by NIST, which is common for military data drives. One readily accessible encryption method administered by the NSA is called Commercial Solutions for Classified (CSfC), which is a new way of delivering industry-developed and government-certified secure solutions quickly.

CSfC is based on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications. CSfC, however, falls short of the stringent levels of NSA Type 1 encryption, which must be provided by NSA-certified companies.

With encryption, the way to safeguard stored data from prying eyes is to destroy the encryption key. Although the data is still on the disk, it's virtually guaranteed that unauthorized attempts to access it will fail.

"The easiest approach is to blow away the key, so that nothing of the key is available in any part of the system," explains Mercury's Mackie. "So long as the key and its residuals are completely gone, we are assured that the data is completely safe as long as it's encrypted."

Although encryption might be fine for most data, those involving national secrets and national security require something more.

"We in our industry are paid to be paranoid, so we also would like to erase the whole drive," Mackie says. "We can erase a 1-terabyte solid-state drive in about four seconds."

The enabling technology for fast erase is NAND Flash solid-state memory, which is a type of non-volatile storage technology that does not require power to retain data.

Using the NAND erase command can wipe out data on all solid-state memory drive plans simultaneously. Some data storage designers use a command that erases the drive even if power is cut off mid-process. This command simply resumes erasing the drive when power is restored.

There even is a procedure that goes beyond erasing the data, called sanitizing, or zeroizing, the drive. This involves not only erasing the drive, but also over-writing the erased drive several times. The industry has four or five sanitizing algorithms, such as NSA 9-12, for data destruction, says Mercury's Mackie.

Crystal Group's RSS13S17 JBOD Rugged 1U Storage System, with up to six removable SATA/SAS hard drives and able to withstand the harshest environments, is designed for operational, deployable, and high-reliability applications.

"Some drives we use have a signal — a circuit built in — that if you initiate sanitization it literally burns the circuits," says Phoenix's Deacon. "Once that starts, even if you pull power to that drive, as soon as you apply power again you can't stop it; it will continue."

There are times — particularly in forward-deployed military applications — in which security means the ability to erase or sanitize drives, and to do it quickly. This is another area where solid-state drives are superior to rotating media, because solid-state drives can sanitize in seconds, where rotating media might take hours.

The Model 9740 Complete Data Storage Solution from Kaman Precision Products' Memory Division is designed for use in severe environments, including military settings such as fighter aircraft, as well as other aerospace and industrial settings.

"We are talking about where critical data must be protected from the enemy," says Mercury's Mackie. "If it is a warfighter's job to protect that data, we can do an erase in four seconds. Others might take tens of minutes to hours, and if a warfighter has to stay with the drive until it's erased, that's life or death."

"Even though you can sanitize it, if you can't sanitize it in the time frame the customer requires, you're out of the running," echoes Phoenix's Deacon.

The future of secure data

Experts agree that keeping data secure over time remains a moving target. Adversaries continually will find ways of defeating nearly every data security measure.

"You can imagine that attackers might use quantum computers to crack encryption," says Mercury's Lazaravich.

Quantum computers are different from binary digital electronic computers based on transistors, in that it uses analog signals and uses quantum bits, which can be in an infinite number of superpositions of states.

"The encryption we have today, while very good, won't last forever," Lazaravich says. "We'll need better encryption algorithms against the early quantum computers that will develop over the next five to ten years. This could involve quantum encryption." ➔

Leonardo-Finmeccanica to supply AESA radar for unmanned helicopter

The U.S. Navy is ordering an AESA radar system for the upgraded MQ-8C Fire Scout unmanned helicopter from Leonardo-Finmeccanica in Rome, Italy. Under a contract issued by the Naval Air Systems Command at Patuxent River Naval Air Station, Md., the company is to deliver five of the AESA radar units for testing and evaluation. The contract contains an option to buy a larger quantity of the radars for use in real operations aboard the MQ-8C Fire Scout. The Osprey radar uses electronic beam technology to scan from high in the sky to detect threats beyond the range of standard ship-based sensors in all environmental conditions, when visibility is extremely poor.

MDA to develop Canada's space-based synthetic aperture radar

MacDonald, Dettwiler and Associates (MDA) in Richmond, British Columbia, won an $11.4 million contract option by Canada's Department of National Defence to develop space-based synthetic aperture radar technology for a maritime surveillance project. The space-based radar will support the Polar Epsilon 2 broad-area maritime surveillance system that will use Canada's RADARSAT satellite constellation mission. PE2 ground systems

Keysight signal generators help Navy upgrade electronic test facility at China Lake

BY **John Keller**

RIDGECREST, Calif. — U.S. Navy avionics researchers needed vector and analog signal generators to upgrade the RF and microwave hardware-in-the-loop test facility at the Naval Air Warfare Center Aircraft Division-China Lake in Ridgecrest, Calif. They found their solution at Keysight Technologies in Englewood, Colo.

Officials of the Naval Air Warfare Center Weapons Division announced a $300,673 sole-source contract to Keysight for three vector signal generators and one analog signal generator to upgrade the hardware-in-the-loop facility at China Lake Naval Air Weapons Station in Ridgecrest, Calif.

China Lake integrates weapons and avionics onto tactical aircraft that include the F/A-18 jet fighter bomber; AV-8B jump jet; AH-1W and AH-1Z attack helicopters; EP-3E signals intelligence and reconnaissance aircraft; and the F-22 jet fighter. The naval weapons station, located in the Mojave Desert northeast of Los Angeles, is home to interconnecting hardware-in-the-loop virtual test facilities, as well as large outdoor flight test ranges to help develop and test network interoperability among aircraft systems.

The electronic combat range (ECR) at China Lake is the Navy's primary open-air range for test and evaluation of airborne electronic warfare (EW) systems. The ECR provides engineering support, developmental and operational test and evaluation, analysis, and training resources for users of systems designed to counter or penetrate enemy air defenses. Combat aircraft pilots can train against air-to-air and surface-to-air missiles, as well as complete an air-to-ground strike mission.

Keysight signal generators will help upgrade a hardware-in-the-loop test facility at China Lake Naval Weapons Station in California.

For test and verification purposes, Navy officials are adding three agile RF sources to the existing scene-generation system at the hardware-in-the-loop facility at China Lake: the three vector signal generators and one high-performance analog signal generator from Keysight.

Signal generators produce repeating or non-repeating analog and digital RF signals to help engineers design, test, troubleshoot, and repair electronic devices. In addition to the signal generators, the hardware-in-the-loop facility has two anechoic chambers and work areas for testing and simulation of how missile seekers and threat targets interact. ←

FOR MORE INFORMATION visit **Keysight Technologies** online at *www.keysight.com*.

are designed to receive and process information from RCM SAR satellites that MDA is also constructing for Canada's space agency. MDA also has unveiled a U.S. Access Plan as part of the company's push to win government contracts for information technology and communications services intended to support classified space programs in the U.S.

Custom MMIC introduces GaAs switches for military RF and microwave uses

Custom MMIC in Chelmsford, Mass., is introducing the DC-18 GHz SP3T and SP5T non-reflective RF and microwave gallium arsenide (GaAs) switches for military, telecommunications, and test and measurement applications. The SP3T CMD234C4 provides high isolation of 40 dB at 10 GHz and low insertion loss of 2 dB. The CMD234C4 includes an onboard binary decoder circuit, requiring 2 complementary control voltage logic lines of 0/-5 volts. The SP5T CMD235C4, similar to the SP3T design, has a low-power integrated 3:8 TTL decoder for enhanced digital control. The CMD235C4 provides low insertion loss of 2.5 dB and a high isolation of 40 dB at 10 GHz. The CMD235C4 and CMD234C4 come in small size and lead-free, RoHs-compliant 4x4 SMT QFN packages, and have a switching speed of 66 nanoseconds. ←

Raytheon to build electronic warfare-equipped MALD-J radar-jamming drones

EGLIN AIR FORCE BASE, Fla. — U.S. Air Force airborne weapons experts are asking Raytheon Co. to build potentially hundreds of electronic warfare (EW) radar-jamming drones under terms of a four-year $76.1 million sole-source contract.

Officials of the Air Force Life Cycle Management Center at Eglin Air Force Base, Fla., are asking Raytheon Missile Systems in Tucson, Ariz., to provide lot 10 of the Miniature Air Launched Decoy Jammers (MALD-J), which are relatively simple air-launched unmanned aerial vehicles (UAVs) designed to jam enemy radar.

MALD-J is an electronic jamming version of the Raytheon Miniature Air Launched Decoy drone that navigates and operates much closer than conventional EW to the victim radar, Raytheon officials say. Last June, Raytheon won a $118.5 million order for lot 9 of MALD-J production.

The MALD-J EW drone can loiter in the target area for an extended time to help keep manned aircraft out of harm's way. The MALD-J low-cost, air-launched programmable unmanned aircraft duplicates the combat flight profiles and signatures of U.S. and allied aircraft. By duplicating the radar signatures of manned aircraft, the MALD-J can spoof enemy radar and tempt ground-to-air missiles to shoot at the wrong targets.

The expendable air-launched UAV presents a radar signature that looks like a U.S. or allied aircraft to enemy integrated air defense systems (IADS). The U.S. and its allies use MALD and its jamming companion MALD-J to confuse and deceive enemy air defenses by sending a formation of these smart drones into hostile airspace. MALD offers counter air operations to neutralize air defense systems that pose a threat to U.S. and allied pilots.

The Raytheon Miniature Air Launched Decoy Jammer (MALD-J) is designed to jam and confuse enemy air defenses.

Major suppliers to the MALD system include AML Communications in Camarillo, Calif.; AUSCO in Port Washington, N.Y.; BAE Systems in Berthoud, Colo.; CEI in Sacramento, Calif.; Celestica in Austin, Texas; Eagle Pitcher in Joplin, Mo.; EDO in Bohemia, N.Y.; Enser in Pinellas Park, Fla.; Engineered Fabrics Corp. in Rockmart, Ga.; GDOTS in Redmond, Wash.; Hamilton-Sundstrand in Rockford, Ill., and San Diego; LaBarge in Joplin, Mo.; Moog in East Aurora, N.Y.; and Tecom in Westlake Village, Calif.

On this contract, Raytheon will do the work in Tucson, Ariz., and should be finished by June 2020. ←

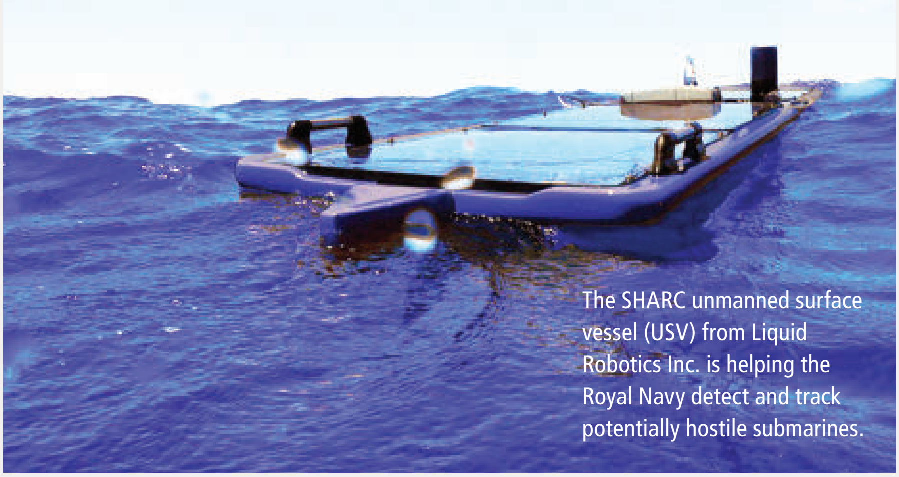
FOR MORE INFORMATION visit **Raytheon Missile Systems** online at *www.raytheon.com*.

First flight for new jet-powered Avenger UAV

A turbojet-powered unmanned aerial vehicle (UAV) by General Atomics Aeronautical Systems Inc. has completed its first flight. The unmanned aircraft is called the Avenger Extended Range, a variant of the company's jet-powered Predator C Avenger, which has accumulated more than 13,000 flight hours to date. The flight occurred at its Gray Butte Flight Operations Facility in Palmdale, Calif. The aircraft has a wingspan of 76 feet and carries 2,200 pounds of additional fuel. Its flight endurance is 20 hours, five more than the legacy Avenger. The remotely piloted aircraft also features a wide array of sensors and weapons payloads to perform intelligence, surveillance, and reconnaissance (ISR) and ground support missions.

Marines look for 'mega-drone' that will carry same weapons as F-35

The U.S. Marine Corps is in the hunt for a mega-drone able to take off and land vertically and deploy aboard ship, while carrying a serious amount of firepower. The MUX drone, short for Marine air-ground task force unmanned expeditionary capabilities, will reach initial operational capability by 2026, be equipped to fight from sea as well as land, and team with the F-35B Lightning II 5th-generation fighter aircraft on missions. ←



The SHARC unmanned surface vessel (USV) from Liquid Robotics Inc. is helping the Royal Navy detect and track potentially hostile submarines.

Royal Navy uses networked USVs for detecting and tracking submarines

SUNNYVALE, Calif. — The British Royal Navy has demonstrated the detection and tracking of manned and unmanned submarines using a long-endurance unmanned surface vessel (USV) called the Sensor Hosting Autonomous Remote Craft (SHARC) from Liquid Robotics Inc. in Sunnyvale, Calif.

Liquid Robotics experts used a networked set of four SHARC USVs equipped with advanced Boeing acoustic sensors. The SHARCs were deployed off the coast of Northern Scotland during the British Royal Navy's Unmanned Warrior 2016 demonstration in October.

Over the two-week demonstration, the four networked SHARCs exchanged data in real time to detect and track an advancing unmanned underwater vehicle (UUV), as well as a manned diesel submarine, Liquid Robotics officials say.

"Our work during Unmanned Warrior demonstrates without a doubt the practicality of using autonomous systems to provide real-time actionable intelligence to our warfighters," says Kory Mathews, vice president of autonomous systems at the Boeing Co. Defense, Space & Security segment in St. Louis.

In September 2014, Liquid Robotics and Boeing signed a multi-year agreement. The companies used the Liquid Robotics Wave Glider USV to develop the SHARC, which delivers continuous maritime intelligence, surveillance, and reconnaissance missions for as long as one year without fuel or manpower.

The SHARC surface vessel is about the size of a surfboard and has solar panels for power generation and antennas for line-of-sight and satellite communications. Its low profile is extremely difficult to detect from surface ships or aircraft.

The SHARC uses the Liquid Robotics Wave Glider technology for propulsion, which dangles a set of wings on a tether about 20 feet below the surface vessel, which harvests wave energy for forward propulsion. The suspended wings also keep the surface vessel stable even in hurricane-force winds and waves. One operator on shore can monitor and control large fleets of SHARC USVs.

SHARC's capabilities demonstrated during Unmanned Warrior didn't stop at anti-submarine warfare (ASW). Two SHARCs had meteorological and oceanographic sensors to gather data for prediction models.

The SHARCs operated 24/7 in harsh conditions unfavorable for manned operations — waves of roughly 22 feet and winds of more than 60 knots — to provide real-time data autonomously on weather and ocean conditions during the exercise.

"We proved that SHARCs can augment the tedious and dangerous task of continuous maritime surveillance by our warfighters and provide critical real-time intelligence to commanders," says Gary Gysin, president and chief executive officer of Liquid Robotics. ←

FOR MORE INFORMATION contact **Liquid Robotics** online at *www.liquid-robotics.com*, **Boeing Defense, Space & Security** at *www.boeing.com/defense*, and the **Royal Navy** at *www.royalnavy.mod.uk*.

Army asks Lockheed Martin to upgrade AN/TPQ-53 radar with counter-drone capability

BY **John Keller**

ABERDEEN PROVING GROUND, Md. — Radar experts at Lockheed Martin Corp. are upgrading the company's AN/TPQ-53 air-defense, fire-control radar to detect, classify, track, and pinpoint enemy unmanned drones without posing a risk to nearby U.S. and allied aircraft and military forces.

Officials of the U.S. Army Contracting Command at Aberdeen Proving Ground, Md., announced a $27.8 million contract to the Lockheed Martin Rotary and Mission Systems segment in Syracuse, N.Y., to add counter-unmanned aerial system (C-UAS) capability to the AN/TPQ-53 radar.

Lockheed Martin is upgrading the AN/TPQ-53 air-defense radar to counter enemy unmanned aircraft.

Now Army experts are asking Lockheed Martin to make software upgrades to the AN/TPQ-53 to enhance its reliability against enemy drones and other unmanned aircraft, as well as integrate an off-the-shelf identification-friend-or-foe (IFF) subsystem to the radar.

The Q-53 — designed and built by Lockheed Martin Rotary and Mission Systems — is a solid-state phased-array radar that detects, classifies, tracks, and determines the location of enemy indirect fire weapons like rockets, artillery shells, and mortars in either 360- or 90-degree modes. This system is replacing the aging U.S. Army AN/TPQ-36 and AN/TPQ-37 medium-range radars. Lockheed Martin builds the Q-53 radar in Syracuse and Owego, N.Y.; Moorestown, N.J.; and Clearwater, Fla.

To upgrade the radar to detect and track enemy drones, Lockheed Martin will modify the existing AN/TPQ-53 software to detect, track, and identify enemy drones hindering existing waveforms for detection and tracking. The goal is to integrate these upgraded counter-drone capabilities with minimal hardware modification and no increase to manpower requirements of the existing AN/TPQ-53 system.

In addition, Lockheed Martin will modify existing AN/TPQ-53 software interfaces to the Army's Advanced Field Artillery Tactical Data System (AFATDS) and Forward Area Air Defense Command and Control (FAAD C2) system to provide enemy drone information to counter-fire batteries.

Lockheed Martin will demonstrate the upgraded AN/TPQ-53 radar with counter-drone capabilities during Army field exercises in January and June 2017, and will provide the final fieldable configuration for assessment in January 2018. The final fieldable system should be ready by June 2018.

On this contract, Lockheed Martin will do the work in Syracuse, N.Y., and should be finished by 2018. ←

FOR MORE INFORMATION visit **Lockheed Martin** online at *www.lockheedmartin.com/us/rms.html*.

ISCAN eye-tracker gets platinum recognition in 2016 Technology Innovation Awards

Electro-optics experts at ISCAN Inc. in Woburn, Mass., have received a platinum award in the 2016 *Military & Aerospace Electronics* and *Intelligent Aerospace* Technology Innovation Awards for the company's OmniView eye-tracking system. The ISCAN OmniView system was part of the top tier of this year's three-tier Technology Innovation Awards. The top award level is platinum, the middle tier is gold, and the third tier is silver. *Military & Aerospace Electronics* and *Intelligent Aerospace* made awards to company entries that offer solutions to difficult aerospace and defense electronics design challenges. The ISCAN OmniView is a binocular, real-time, head-mounted, eye-tracking system for aircraft pilots or military ground vehicle drivers. It is an indicator for human factors assessment in military training to overcome limits to conventional eye trackers for military and avionics human factors and training applications. The system tracks the user's eye position and overlays a point of gaze cursor that shows precisely where the user is looking. It is designed to work under real flight or vehicle operating conditions. ←

FOR MORE INFORMATION visit **ISCAN** online at *www.iscaninc.com*, and the **Military & Aerospace Electronics and Intelligent Aerospace Technology Innovation Awards** at *www.militaryaerospace.com/innovators-awards.html.*

Raytheon is trying to develop radiation-hardened electro-optical sensors for strategic space surveillance systems.

Notional

Raytheon to build rad-hard infrared focal plane array space sensors

BY **John Keller**

KIRTLAND AIR FORCE BASE, N.M. — Electro-optical sensors designers at Raytheon Co., are pushing the state of the art in radiation-hardened infrared focal plane array space sensors for the most demanding strategic space applications.

Officials of the U.S. Air Force Research Laboratory at Kirtland Air Force Base, N.M., have announced a $7.4 million completion form contract to the Raytheon Vision Systems segment in Goleta, Calif., for the Focused Opportunity Reaching Toward Reliable Electro-Optic Strategic Sensors (FORTRESS) program.

Raytheon engineers will design, grow, and fabricate large-format mercury cadmium telluride infrared focal plane array detectors with ultra-low noise and high quantum efficiency. These devices must be able to survive bombardment by space radiation, as well as laser attacks.

The work is part of the Air Force FORTRESS effort to advance and maintain the state-of-the-art, scientific knowledge, growth, processing, and characterization capability in low-noise infrared sensor chip assemblies (SCAs) for national strategic space applications, such as electro-optical surveillance satellites.

Raytheon experts are fabricating infrared sensor chip assemblies that are at least as large as six centimeters on a side with pixel pitch of 18 microns. Supervising the program are officials of the advanced electro-optical space sensor program of the Air Force Research Lab's Space Vehicles Directorate.

These space infrared sensors must be able to resist any ill effects of 100 kilorads total-dose ionizing radiation without any single-effect upsets, and must be able to withstand charged particles of 63 MeV to a proton fluence of 7.43 x 1011 protons per square centimeter.

While these specifications represent a minimum requirement, Air Force researchers say they expect Raytheon to be able to design space sensors that will far exceed requirements. FORTRESS sensor chip assemblies are expected to operate with minimally degraded performance in a space environment where protons, electrons, heavy-ions all are present.

In addition, researchers would like these sensor chip assemblies to be immune to performance degradation when exposed to laser radiation; the read-out integrated circuit must be intrinsically hardened to prevent performance degradation when subjected to high irradiance light.

On this contract, Raytheon will do the work in Goleta, Calif., and should be finished by July 2019.

FOR MORE INFORMATION visit **Raytheon Vision Systems** online at *www.raytheon.com*, and the **Air Force Research Lab Space Vehicles Directorate** at *www.kirtland.af.mil/Units/AFRL-Space-Vehicles-Directorate.*

Quantum Imaging to provide infrared electro-optics for multispectral targeting systems

CRANE, Ind. — U.S. Navy electro-optics sensors experts needed shortwave infrared (SWIR) cameras for the Navy Raytheon Multispectral Targeting System (MTS). They found their solution at Quantum Imaging Inc. in Colorado Springs, Colo.

Officials of the Naval Surface Warfare Center Crane Division in Crane, Ind., announced an $8.2 million contract to Quantum Imaging for SWIR and visible-light camera work for the MTS.

The work will involve SWIR camera assemblies; visible and near-infrared cameras; low-light scientific complementary metal-oxide semiconductor (CMOS) camera; repairs; and spare parts for the MTS.

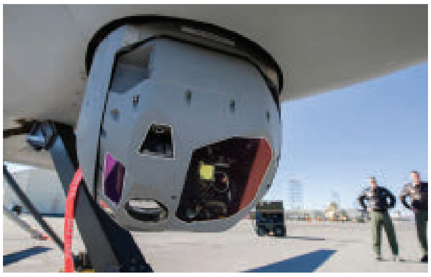
The SWIR, visible and near-infrared, and low-light CMOS cameras are for maintaining and sustaining the MTS aboard Navy, Army, and Air Force manned and unmanned aircraft.

The Raytheon MTS is an airborne, electro-optic, forward-looking infrared, turreted sensor package that provides long-range surveillance, high-altitude target acquisition, tracking, rangefinding, and laser designation, and for all tri-service and NATO laser-guided munitions.

The system is a turreted forward-looking pod combining several visible-light and infrared video cameras for long-range surveillance and high-altitude target acquisition, tracking and laser designation.

The MTS offers a combination of sensors that include multiple-wavelength sensors; near-infrared and color daylight TV cameras; illuminators; eye-safe rangefinders; image merging; spot trackers; and similar other avionics, officials say.

Multispectral sensors capture image data at specific frequencies, and separate the wavelengths to extract information the human eye fails to capture with its receptors for red, green, and blue. It can detect things like disturbed dirt, and can be effective in finding targets hidden in camouflage. MTS sensors carry the military designations of AAS-52, AAS-53, ASQ-228, DAS-1, and DAS-2.



Quantum Imaging will provide electro-optical sensors for the Raytheon Multispectral Targeting System (MTS).

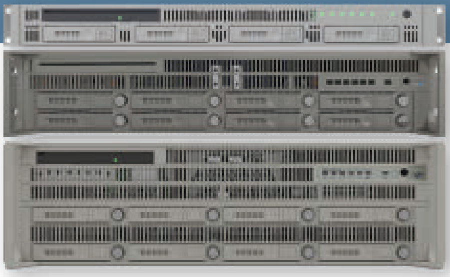
The Raytheon MTS can be fitted to the C-130 fixed-wing aircraft, the MH-60 helicopter, and the medium-altitude, long-endurance MQ-9 Reaper hunter-killer unmanned aerial vehicle (UAV).

The system works with the Hellfire missile and all tri-service and NATO laser-guided munitions, such as the Paveway laser guided bomb. The advanced targeting forward looking infrared (ATFLIR) pod also is used with Paveway, JSOW, and HARM bombs and missiles.

Quantum Imaging will do the work on this contract in Colorado Springs, Colo., and should be finished by September 2021.

FOR MORE INFORMATION visit **Quantum Imaging** at *www.quantumimaging.com.*

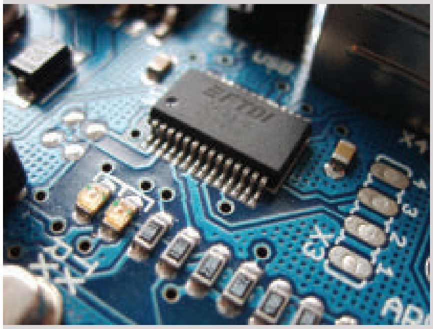
PRODUCT applications



ELECTRONICS DISTRIBUTION

Three distributors to provide components for airborne weapons work

U.S. Navy airborne weapons experts are working with three electronics distributors to provide a variety of electronic components for air-to-ground weapons development.



Officials of the Naval Air Warfare Center Weapons Division at China Lake Naval Air Weapons Station in Ridgecrest, Calif., announced contracts collectively worth as much as $9.8 million for high-reliability electronics parts to three electronics distributors: Laguna Components Inc. in Laguna Beach, Calif.; LC Engineers Inc. in Rahway, N.J.; and Pacific IC Source in Yucaipa, Calif.

The electronics distributors will compete for orders over the next five years for a variety of electronic components that include integrated circuits, resistors, capacitors, connectors, wire, diodes, flex circuits, switches, back shells, sleeving, encoders, transistors, power supplies, flash chips, potentiometers, radios, electronic subassemblies, receivers, semiconductors, plugs, Global Positioning System (GPS) components, terminal blocks, antennas, inertial measurement units, fuses, relays, transducers, switches, power cables, receptacles, oscilloscopes, and drying cabinets.

These distributors handle parts built by companies like Glenair, Mini-Circuits, Miteq, Omnetics, Teledyne Cougar, Emerson, Carolina Microwave, Microhard Systems, Frankfurt Laser Co., and Evolution Interconnect Systems.

The three distributors will do the work on this contract at their facilities in Laguna Beach, Calif.; Rahway, N.J.; and Yucaipa, Calif., and should be finished by November 2021. ←

FOR MORE INFORMATION visit **Laguna Components** online at *www.lagunacomponents.com*, **LC Engineers** at *www.lcengineers.com*, **Pacific IC** at *www.pacificic.com*, and the **Naval Air Warfare Center-China Lake** at *www.navair.navy.mil/nawcwd*.

RUGGED SERVERS

Navy orders shipboard computer servers from Themis

U.S. Navy shipboard electronics experts needed computer rugged servers for a variety of shipboard computing tasks. They found their solution at Themis Computer in Fremont, Calif.

Officials of the Naval Sea Systems Command in Washington announced a $1.6 million contract for four Themis RES-XR5 1U standard-density, rack-mounted servers; shock-mounting kits; cabling; optical transceivers; Gigabit Ethernet switches; disk-on-module data storage; and ancillary items.

The Navy awarded the contract to Strictly Technology LLC, otherwise known as StrictlyTech, in Fort Lauderdale, Fla., which is an authorized reseller of Themis items. Naval Sea Systems Command is in place to design, build, deliver, and maintain ships and shipboard systems for the U.S. Navy.

The Themis RES-XR5 standard-density, rack-mounted servers are available in 1U, 2U, and 3U RIO and FIO form factors, and have E5-2600 v3/v4 series Intel Xeon processors with as many as 20 cores per socket, as much as 1 terabyte of DDR4 ECC memory.

These cloud-ready rugged servers are designed to operate in high shock and vibration, as well as in temperature extremes. They can be mounted in standard commercial racks or mobile rugged transit cases for military, industrial, or rugged commercial applications.

FOR MORE INFORMATION visit **Themis** online at *www.themis.com*, **StrictlyTech** at *http://strictlytech.com*, and **Naval Sea Systems Command** at *www.navsea.navy.mil*.

AVIONICS

Cessna chooses Honeywell avionics for Citation Hemisphere business jet

Aircraft designers at Cessna Aircraft Co. in Wichita, Kan., needed an avionics suite for the Cessna Citation Hemisphere large long-range business jet. They found their solution at Honeywell Aerospace in Phoenix.

Cessna officials chose the Honeywell Primus Epic transoceanic flight management system for the Citation Hemisphere large-cabin business jet, which will have a range of 4,500 miles when it is ready in 2019.

The Honeywell Primus Epic cockpit will have SmartView for lower minimums, precision inertial reference sensors, and a connected aircraft solution to enable Hemisphere operators to reach destinations quickly and at affordable costs, Honeywell officials say.

Primus Epic will provide Citation Hemisphere pilots with the SmartView conformal 3D color image of runways, terrain, and obstacles even at night and in challenging weather conditions such as fog, rain, or snow to improve situational awareness.

Honeywell's connected aircraft solution includes satellite communications and connectivity airtime, as well as cockpit, cabin, and maintenance applications and services, Honeywell officials say.

The Honeywell IntuVue volumetric weather radar helps pilots see airborne weather hazards. Airport 2D and 3D moving maps show runways, taxiways, and airport markings on navigation displays, and integrate with SmartView synthetic vision for an out-the-window view of the airport.

The Honeywell avionics suite provides flight and approach capabilities with Required Navigation Performance Approval Required. LED large-format displays provide situational awareness, and touchscreen controllers help pilots manage systems and control audio.

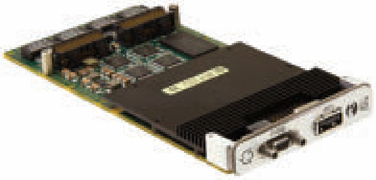
Honeywell Aspire 300 satellite communications enables simultaneous cockpit voice and data connectivity via the Iridium satellite system, and optional JetWave cabin satellite communications provide in-cabin communications and entertainment.

FOR MORE INFORMATION visit **Honeywell Aerospace** online at *http://aerospace.honeywell.com*, and **Cessna Aircraft** at *http://cessna.txtav.com*.

EMBEDDED COMPUTING

SPAWAR picks Curtiss-Wright XMC computing

U.S. Navy researchers needed small-form-factor and low-power XMC single-board computers for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) research work. They found their embedded computing solution from the Curtiss-Wright Corp. Defense Solutions Division in Ashburn, Va.



Officials of the Space and Naval Warfare Systems Center Pacific in San Diego announced their intention to order 12 Curtiss-Wright XMC-120 Switched Mezzanine Card (XMC) modules and related embedded computing equipment.

The XMC-120 is designed for space-constrained size, weight, and power (SWaP)-sensitive applications.

It has the Intel Atom Bay Trail E3845 processor, which is an integrated system on chip (SoC) based on Intel's 64-bit Silvermont processor architecture. The processor provides quad-core performance, operates at 1.91 GHz, has integrated 2-megabyte L2 cache, and provides 64-bit x86 processing while consuming less than 10 watts of power.

The upcoming contract to Curtiss-Wright has yet to be negotiated. The contract also will call for Curtiss-Wright to provide 12 RTM-120 rear transition modules (RTMs), cabling, 12 RTM3-652-0020 RTMs, and 12 RTM3-1258-1001 RTMs.

SPAWAR Systems Center Pacific provides the Navy with research, development, delivery, and support of integrated C4ISR, cyber, and space systems and capabilities. The center manages locations in the Pacific and around the world. ←

FOR MORE INFORMATION visit **Curtiss-Wright Defense Solutions** online at *www.curtisswrightds.com*.

COMPUTER BOARDS

COM Express embedded computing module for use in harsh environments introduced by Kontron

Kontron in Augsburg, Germany, is introducing the COM Express-bBD7 type 7 computer-on-module (COM) for embedded computing applications that operate in harsh environments. The module is a Xeon D-1500-based COM Express that delivers server-class performance in the COM Express basic standard form factor and is designed according to the Type 7 standard. The COM Express-bBD7 module has as many as 16 cores, support for 2x 10 Gigabit Ethernet ports, high-speed connectivity from configurable PCI Express lanes for high I/O performance, and support for as many as 32 gigabytes of ECC/non-ECC DDR4 memory. The Kontron COM Express-bBD7 also is available in industrial-grade versions, and provides operating system support that includes Linux, Windows Server, Windows 7 and 8.1, and VxWorks.

FOR MORE INFORMATION visit **Kontron** online at *www.kontron.com.*

TEST AND MEASUREMENT

Signal analyzer for test and measurement at millimeter-wave frequencies offered by Keysight

Keysight Technologies Inc. in Santa Rosa, Calif., is introducing the N9041B UXA X-series signal analyzer that provides frequency coverage to 110 GHz with a maximum analysis bandwidth to 5 GHz for spectrum and signal test and measurement at millimeter-wave frequencies. Applications of these tools include military radar, electronic warfare systems, automotive radar, 5G wireless communications, millimeter-wave backhaul, and satellite communications. Emerging applications encompass development of devices and systems capable of performing high-resolution materials measurements for manufacturing, pharmaceutical, and medical. The N9041B UXA HAS advanced front-end circuitry that achieves low loss and efficient mixing, providing a displayed average noise level (DANL) as low as –150 dBm/Hz when characterizing wideband modulated signals in the millimeter-wave band.

FOR MORE INFORMATION visit **Keysight** online at *www.keysight.com.*

TIMING AND SYNCHRONIZATION

Chip-scale atomic clock for SWaP low-power timing and synchronization introduced by Microsemi

Microsemi Corp. in Aliso Viejo, Calif., is introducing thermally improved chip-scale atomic clock (CSAC) components for SWaP-constrained, low-power atomic clock holdover timing and synchronization applications that must operate in wide temperature ranges. With an operating temperature range of -10 to 70 degrees Celsius, Microsemi's CSAC components are 17 cubic centimeters in size, 35 grams of weight, and only 120 milliwatts of power. Microsemi's thermally improved CSAC products support defense and security markets, targeting applications such as low-power holdover against GPS vulnerabilities for position, navigation, and timing security. They also are suitable for holdover in underwater (ocean bottom nodal) applications and atomic frequency reference in test and measurement applications.

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

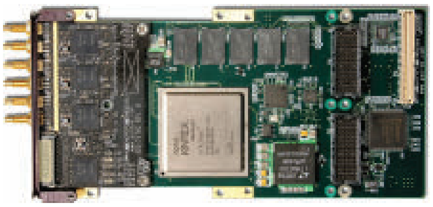
RACKMOUNT SERVERS

Rackmount secure server for cyber security and system integrity introduced by Mercury

Mercury Systems Inc. in Chelmsford, Mass., is introducing the ATX-class rackmount secure server for mission processing, sensor processing, cyber security, command and control, and battle management applications that require system integrity. These rackmount secure servers are designed and made in the U.S. in domestic

secure facilities. The servers support the U.S. Department of Defense 5200.44 directive, enabling the protection of mission-critical functions for trusted systems and networks. The servers use commercial off-the-shelf (COTS) processors, memory, and peripherals, yet have secure and rugged packaging. Chassis configurations may be commercial or ruggedized as required.

FOR MORE INFORMATION visit **Mercury Systems** online at *www.mrcy.com.*



DIGITAL SIGNAL PROCESSING

XMC module for radar signal processing introduced by Pentek

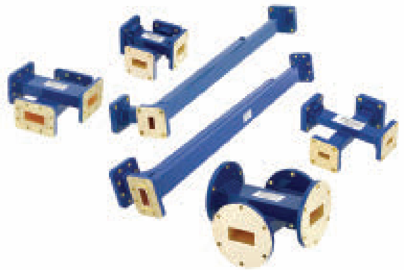
Pentek Inc. in Upper Saddle River, N.J., is introducing the Jade family of switched mezzanine card (XMC) embedded computing modules for digital signal processing (DSP) in radar, communications, and data acquisition applications. Jade is based on the Xilinx Kintex UltraScale field-programmable gate array (FPGA) for modulation and demodulation, encoding and decoding, encryption and decryption, and channelization of the signals between transmission and reception. For applications that do not need large DSP resources or logic, a lower-cost FPGA can be installed. The first product using the Jade architecture is the 71861 XMC module with four 200 MHz A/D channels and programmable multiband digital downconverters (DDCs). As with all Jade products, the model 71861 is based on the Xilinx Kintex UltraScale FPGA family with FPGA choices to match price, power, and processing performance needs. In addition to XMC, this product also is available in PCI Express, 3U and 6U VPX, AMC, and 3U and 6U CompactPCI form factors, with versions for commercial and rugged environments.

FOR MORE INFORMATION visit **Pentek** online at *www.pentek.com.*

RF AND MICROWAVE

Waveguide directional couplers to 33 GHz introduced by Pasternack

Pasternack Enterprises Inc. in Irvine, Calif., is introducing a family of waveguide directional couplers displaying performance to 33 GHz for RF and microwave applications in radar, satellite communications (SATCOM), telecommunications, and wireless transmit-and-receive systems. The waveguide directional couplers consist of 74 models spanning a frequency range of 5.85 GHz to 33 GHz across eight frequency bands. The couplers come in two physical configurations including "Crossguide" and "Broadwall" versions with either UG-style or CPR-style flanges. Pasternack's waveguide directional couplers come in waveguide sizes from WR-137 to WR-34 and 10, 20, 30, 40 and 50 dB coupling levels with full waveguide operational bandwidth. These waveguide couplers also boast low insertion loss and typical VSWR of 1.05:1. Pasternack's new couplers are constructed using rugged copper alloy.



FOR MORE INFORMATION visit **Pasternack** online at *www.pasternack.com.*

RUGGED COMPUTERS

Rugged small-form-factor embedded computer introduced by Aitech

Aitech Defense Systems Inc. in Chatsworth, Calif., is introducing the military-grade A176 Cyclone fanless, rugged, small-form-factor, high-performance embedded computer (HPEC) for applications in harsh environments. The A176 Cyclone measures 20 cubic inches and provides 1 teraFLOP of parallel processing. The embedded supercomputer delivers 60 gigaFLOPs per watt. Using the Nvidia Maxwell architecture for the GPU subsystem, the A176 integrates 256 CUDA cores with 4 gigabytes of LPDDR4 RAM. The Quad-core ARM Cortex A57 CPU provides an operating frequency to 1.9 GHz per core, with an overall maximum power consumption of 17 watts. The rugged computer is for embedded deep learning, computer vision, graphics, and GPU computing applications, especially in harsh environments. Uses include C4ISR, intelligent video analytics, image capture and processing, UAS and UGVs, as well as signal processing and persistent video surveillance. The A176 Cyclone measures 4.3 by 4.3 by 1.18 inches and weighs 2.2 pounds. It operates in temperatures from -40 to 70 degrees Celsius, with vibration and shock resistance to VITA

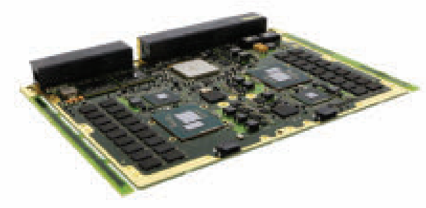
47 levels V2 and OS1, respectively. The system withstands rain, dust, salt fog, and bench handling to MIL-STD-810G and EMI/RFI levels to MIL-STD-461.

FOR MORE INFORMATION visit **Aitech Defense Systems** online at *www.rugged.com*.

BOARD PRODUCTS

Dual-processor computer for radar and SIGINT introduced by CES

Creative Electronic Systems (CES) in Grand-Lancy, Switzerland, is introducing the CIO5-2040 SWaP optimized, dual-processor, single-board computer for RF and microwave signal processing applications like radar, signals intelligence (SIGINT), and electronics intelligence (ELINT). The CIO5-2040 is built using a mirrored architecture implementing two Intel Core i7 Gen5 processors. Feeding the processors are data through four 10 gigabit Ethernet links and three PCI Express Gen3 x8 links routed in the backplane. When it comes to high-performance embedded computing (HPEC), thermal management, and heat dissipation are key factors to enabling the system to provide its full performance even when running at the highest temperature. To that intent, CES has designed a composite frame, tightly coupled with the CIO5-2040, providing the thermal dissipation of copper while weighing as little as aluminum. As a result, the performance of the board is available even at 85 degrees Celsius and the board together with the frame weigh 30 percent less than its copper-framed counterparts. A PCI Express switch with three Gen3 x8 links enables designers to connect several CIO5-2040 together to form a computing network. Mercury Systems in Chelmsford, Mass., has acquired CES. ←



FOR MORE INFORMATION visit **Creative Electronic Systems (CES)** online at *www.ces-swap.com*.

PRODUCT & LITERATURE SHOWCASE

ADVERTISERS INDEX

ADVERTISER	PAGE
Acromag	11
AIM USA Inc.	6
Emcor Group Inc.	C4
Gaia Converter US	7
Master Bond Inc.	33
Mercury Systems	C2
Pasternack Enterprises	9
Phoenix International	17
Pico Electronics Inc.	1
QML Inc.	3
R&D Interconnect Solutions	5
RGB Spectrum	32
Systel Inc.	19

Military & Aerospace Electronics

GROUP PUBLISHER Alan Bergstein
603 891-9447 / alanb@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

ART DIRECTOR Meg Fuschetti

PRODUCTION MANAGER Sheila Ward

SENIOR ILLUSTRATOR Chris Hipp

AUDIENCE DEVELOPMENT MANAGER Stephanie O'Shea
603 891-9119 / stephanieo@pennwell.com

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

MARKETING MANAGER Gillian Hinkle
603 891-9126 / gillianh@pennwell.com

PennWell®
www.pennwell.com

EDITORIAL OFFICES

PennWell Corporation,
Military & Aerospace Electronics
61 Spit Brook Road, Suite 401, Nashua, NH 03060
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 Jessica Stremmel
717 505-9701 x2205 / Jessica.stremmel@theygsgroup.com

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

For assistance with marketing strategy or ad creation, please contact PennWell Marketing Solutions
Paul Andrews, Vice President
240 595-2352 / pandrews@pennwell.com

CORPORATE OFFICERS

CHAIRMAN Robert F. Biolchini

VICE CHAIRMAN Frank T. Lauinger

PRESIDENT AND CHIEF EXECUTIVE OFFICER Mark C. Wilmoth

EXECUTIVE VICE PRESIDENT, CORPORATE DEVELOPMENT AND STRATEGY Jayne A. Gilsinger

SENIOR VICE PRESIDENT, FINANCE AND CHIEF FINANCIAL OFFICER Brian Conway

TECHNOLOGY GROUP

SENIOR VICE PRESIDENT/PUBLISHING DIRECTOR Christine Shaw

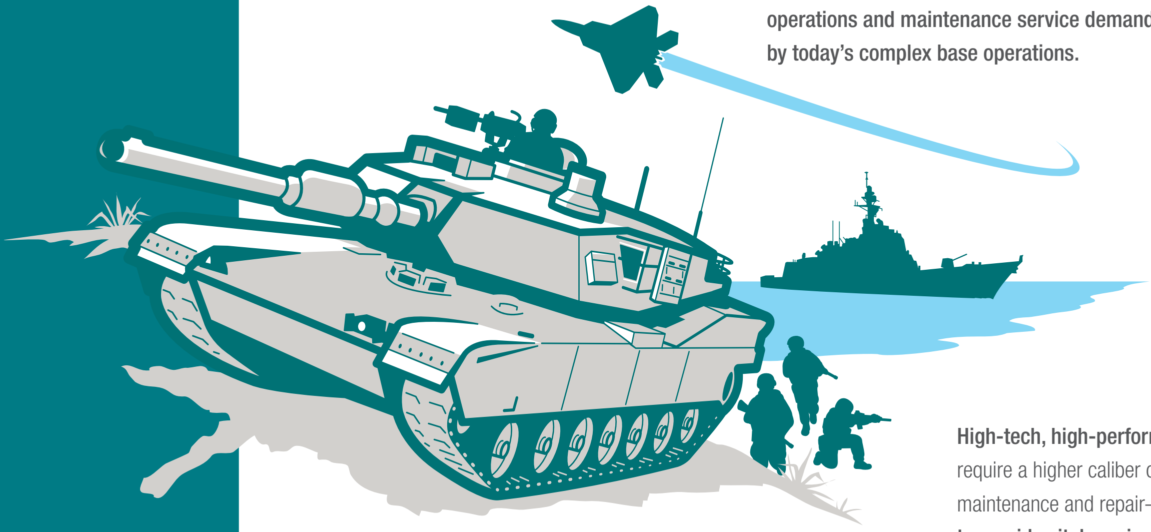
SUBSCRIPTION INQUIRIES
Phone: 847 559-7330 / Fax: 847 763-9607
E-mail: mae@omeda.com
Web: www.mae-subscribe.com

BPA WORLDWIDE™ Connectiv

What *don't* we do for the U.S. Military?

While we don't drive the armored vehicles or pilot the jet fighters, EMCOR has plenty of boots on the ground to help keep our troops and their facilities more efficient and ever ready. Below is just a sample of how we help the military accomplish its missions...

It's all about support—24/7/365 our people are on call for virtually every type of **on-site operations and maintenance service demanded by today's complex base operations.**



High-tech, high-performance facilities require a higher caliber of preventive maintenance and repair—**we are proud to provide vital services and Base Operations Support nationally.**

EMCOR Government Services takes many forms—our people support key facilities for the **U.S. Army, Navy, Air Force, Marines, Coast Guard, and more.**

Did you miss this IFMA talk?

Raising the Bar on Lowering Legionellosis Risk: ANSI/ASHRAE Standard 188

Alan Spence, EMCOR Government Services, worked with the CDC for 10 years to create a standard to help minimize the risk of Legionnaires' Disease in building water systems.

You can still download the White Paper: emcorgovservices.com.

MISSIONS ACCOMPLISHED

FEDERAL AGENCIES

U.S. MILITARY

NATIONAL SECURITY

SPACE

WASHINGTON D.C.

HEALTHCARE SUPPORT

EMCOR® Government Services

WHAT CAN WE ACCOMPLISH FOR YOU?

emcor_info@emcor.net 866.890.7794 emcorgovservices.com