NOVEMBER 2018

Military & Aerospace Electronics

RELEVANT. TRUSTED.
ENABLING TECHNOLOGIES.

New armored vehicle

Researchers ask industry for demonstrators of a future Marine Corps reconnaissance armored vehicle. PAGE 6

Flight-line test

Today's flight-line test systems are small enough to fit in a technician's toolbox, and offer new features like Ethernet and USB. PAGE 24

militaryaerospace.com

Counter-drone technology

Defending against enemy UAVs involves electronic jamming, nets, bullets, and birds of prey. PAGE 14

PennWell

FAILURE IS NOT AN OPTION.

- ☑ FIPS 140-2
- ☑ NIAP
- ☑ Rugged
- ☑ NIST
- ☑ U.S. Supply Chain

RUGGED *AND* SECURE.

Crystal Group **PASS – Platform Agnostic Security Solutions** – includes the world's first rugged FIPS 140-2 compliant data-at-rest storage devices, ruggedized Ruckus ICX switches with NIAP certified IP-security modules for network encryption, and exclusively conformal-coated Seagate 2.5-inch, dual-port SAS drives compatible with any Crystal Group server, workstation, and JBOD or RAID storage system. Crystal Group manufactures its products in vertically integrated, NIST compliant, AS9100D certified, U.S.-based facilities. To prevent security vulnerabilities, components are traced from raw materials through production processes to the delivery of the final warrantied product. To request more information or receive a quote, visit **crystalrugged.com**.

CRYSTAL

A clear advantage.

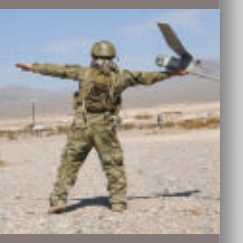
SERVERS | DISPLAYS | STORAGE | NETWORKING | EMBEDDED | CARBON FIBER

sales@crystalrugged.com | 800.378.1636 | crystalrugged.com

NOVEMBER 2018
VOL. 29, NO. 11

Military & Aerospace Electronics

COVER STORY



Military & Aerospace Electronics® (ISSN 1046-9079), Volume 29, No. 11. 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 $185 1yr., $327 2 yr., $466 3 yr.; Canada $280 1 yr., $479 2 yr., $618 3 yr.; International $335 1 yr., $638 2 yr., $834 3 yr. POSTMASTER: Send address corrections to Military & Aerospace Electronics, P.O. Box 47570, Plymouth, MN 55447. Military & Aerospace Electronics is a registered trademark.

BY **JOHN KELLER**, EDITOR IN CHIEF

Is Buy American the solution to cyber attacks like the Chinese spy chips?

There's a serious cyber warfare problem that may be drawing-in deployed U.S. military and aerospace mission-critical embedded computing systems, and few peple really want to talk about it.

It has to do with a computer chip no bigger than a grain of rice that's suspected of being surreptitiously installed by Chinese intelligence agencies on embedded servers made by San Jose, Calif-based Super Micro Computer Inc. These tiny chips may be enabling China and other U.S. adversaries to monitor the inner workings of military computers and the data they are processing.

Super Micro embedded computer servers are now, or in the past have been in use by some of the world's largest corporations, including Amazon and Apple. They also may now, or in the past have been in use by several companies that specialize in real-time mission-critical computing for military and aerospace applications.

Are these Chinese spy chips actually out there today in deployed U.S. military systems? Nobody's talking. It could represent one of the biggest national security breaches in U.S. history. We need to find out how big the problem is, and how to fix it.

How could this have happened? Super Micro designs these embedded servers in Silicon Valley and Taiwan, yet has them manufactured in China, where assembly lines were infiltrated and spy chips installed on some of Super Micro's high-performance computer boards. The chips are small, and hard to detect.

How many boards made it into the supply chain with the Chinese spyware? It's not clear. Exactly where were these boards installed? Also not clear, and the companies using Super Micro embedded server boards are silent on the topic.

Some maintain that all boards and components that go into U.S. military systems be made in America, and everything going into these systems be traceable to authorized U.S. suppliers.

Hasn't this been happening all along, what with regulations in place like the International Traffic in Arms Regulations (ITAR)? Apparently not. What regulations actually are in place may have allowed one of the biggest foreign intelligence coups against U.S. national security interests ever.

"We believe the DOD [the U.S. Department of Defense] should buy only American-designed, -manufactured and -owned servers from ITAR-approved American suppliers," said Ben Sharfi, chief executive officer of General Micro Systems in Rancho Cucamonga, Calif., in a commentary he wrote titled "Alleged China spy chips are another wake-up call to buy only American-manufactured servers."

Christopher Cummins, chief operating officer of Abaco Systems in Huntsville, Ala., says he agrees that buy-American is perhaps the best place to start working these problems out. Cummins penned an article titled "Cyber attack compromises trusted computing, and raises questions about industry's secure supply chain."

"As an industry, our need for diligence in this area is paramount," Cummins wrote. "Abaco Systems doesn't buy in commercial products and then make them rugged after the fact; we design and build rugged into our products from the ground-up. We manufacture everything ourselves: we don't subcontract offshore."

Do Abaco Systems and General Micro Systems have their own business interests to support here? Sure ... but they also have a point. It's a lot harder for Chinese intelligence to gain access to U.S.-based assembly lines than it is for them to access contract manufacturing lines inside China.

Would there be such a risk to crucial U.S. military technology if the Pentagon had been serious about buying all computer components only from security-certified U.S. manufacturing lines?

It's imperative for the Pentagon to get to the bottom of this, determine if Chinese spyware is inside any deployed U.S. military computer systems, and rectify the problem, fast. As for the future? It seems obvious that the Pentagon needs to do a better job of relying exclusively on U.S.-manufactured computer systems. ←

Air Force asks Boeing to provide 18 additional KC-46 tanker aircraft

U.S. Air Force aerial refueling experts are asking the Boeing Co. to build 18 KC-46 Pegasus twin-engine widebody tanker aircraft under terms of a $2.9 billion order. Officials of the Air Force Life Cycle Management Center at Wright-Patterson Air Force Base, Ohio, are asking the Boeing Defense, Space & Security segment in Seattle for lot 4 KC-46 aircraft production, initial spare parts, and support equipment. The KC-46 is a military aerial refueling and strategic military transport aircraft based on the Boeing 767-200 widebody jet airliner. The multirole tanker can refuel all U.S., allied, and coalition military aircraft compatible with international aerial refueling procedures. In addition to refueling other aircraft in midair, the KC-46 also can carry passengers, cargo, and medical patients. Boeing received its first two production lots, for seven and 12 aircraft in August 2016. The third lot for 15 aircraft was awarded in January 2017. The KC-46 aircraft can detect, avoid, defeat and survive threats using several layers of protection that enable it to operate safely in medium-threat environments. For more information contact **Boeing Defense, Space & Security** online at www.boeing.com/defense, or the **Air Force Life Cycle Management Center** at www.wpafb.af.mil/aflcmc.

Lockheed Martin to provide electro-optical targeting systems for U.S. Marine Corps attack helicopters

Electro-optics experts at Lockheed Martin Corp. are building five multi-sensor electro-optical and infrared (EO/IR) fire-control systems for U.S. Marine Corps AH-1Z Viper attack helicopters. Officials of the Naval Surface Warfare Center in Crane, Ind.,

Boeing to build 17 new and rebuilt AH-64E attack helicopters for UAE

BY **John Keller**

REDSTONE ARSENAL, Ala. — Military helicopter experts at the Boeing Co. will build 17 new and remanufactured AH-64E Apache Guardian attack helicopters for the government of the United Arab Emirates (UAE) under terms of a $242.1 million foreign military sales order.

Officials of the Army Contracting Command at Redstone Arsenal, Ala., are asking the Boeing Defense, Space & Security segment in Mesa, Ariz., to provide nine new and eight rebuilt AH-64E helicopters.

The AH-64 Apache is a multirole combat helicopter with integrated avionics and weapons, as well as advanced digital communications to enable real-time, secure transfer of battlefield information to air and ground forces.

The AH-64E Apache Guardian features enhanced performance, joint digital operability, improved survivability and cognitive decision aiding, and reduced operating and support costs, Boeing officials say. The AH-64E Apache, is being delivered to the U.S. Army and has been selected by several international defense forces.

The AH-64E Longbow remanufacture effort upgrades existing AH-64 Apaches to the AH-64E Apache Longbow Block IIIA configuration. It involves the Northrop Grumman AN/APG-78-millimeter wave fire-control radar, radar frequency interferometer, fire-and-forget radar-guided Hellfire missile capability, and cockpit management and digitization enhancements.

The AH-64E Apache Guardian attack helicopter is a sophisticated sensors and weapons platform that can fire a variety of munitions.

The combination of the fire-control radar, radar frequency interferometer,

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

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

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

866.727.8376
Pasternack.com

an INFINITE company

PASTERNACK®
THE ENGINEER'S RF SOURCE

announced an $11.8 million order to the Lockheed Martin Missiles and Fire Control segment in Orlando, Fla., for five AN/AAQ-30 target sight systems (TSS). The TSS equipment for Marine Corps Viper helicopter gunships is part of the Marine Corps H-1 upgrades program for the remanufacture of legacy aircraft with state-of-the-art designs to convert the Marine Corps' existing fleet of AH-1W SuperCobra attack helicopters to the AH-1Z Viper, Navy officials say. The Lockheed Martin AN/AAQ-30 TSS provides target identification and tracking, passive targeting for integrated weapons — including Hellfire missiles — and a laser designation for laser-guided weapons. TSS can identify and laser-designate targets at the maximum ranges of Viper helicopter weapons. The AN/AAQ-30 targeting system is a large-aperture midwave forward-looking infrared (FLIR) sensor, color TV, laser designator and rangefinder (with eye-safe mode), and on-gimbal inertial measurement unit integrated into a stabilized turret on the nose of the helicopter.

L-3 and Harris agree to merge, creating $33.5 billion military technology giant

L-3 Technologies and Harris Corp. have agreed to merge in an all-stock deal, the two companies announced in October, creating a $33.5 billion military technology company. The combined company will be called L-3 Harris Technologies and will be based in Melbourne, Fla., the home of Harris Corp. The deal is expected to close next year, pending a review by the U.S. Department of Defense. Harris handles complex military communications networks for battlefield management and military aircraft. It is also known for a brand of Stingray cell phone trackers used by U.S. law enforcement. New York-based L-3 Technologies provides the 360-degree scanners that travelers encounter when they go through airport security, part of a $170 million line of

and the advanced navigation and avionics suite provides increased situational awareness, lethality, and survivability, Army officials say.

This program also installs the Lockheed Martin Apache Arrowhead Modernized Target Acquisition Designation Sight (M-TADS) and Pilot Night Vision Sensors (PNVS) systems aboard remanufactured AH-64E helicopters.

Formerly known as AH-64D Block III, the AH-64E Guardian has improved digital connectivity, the joint tactical radio system (JTRS), more powerful T700-GE-701D engines with upgraded transmission to accommodate more power, capability to control unmanned aerial vehicles (UAVs), new composite rotor blades, instrument flight rules (IFR) capability, and improved landing gear.

The AH-64E is designed for armed reconnaissance, close combat, mobile strike, and vertical maneuver missions in day, night, obscured-battlefield, and adverse-weather conditions. The helicopter has self-diagnostic abilities, Link-16 data linking, and updated Longbow radar with oversea capacity that could enable naval strikes.

Versions of the AH-64 Apache attack helicopter have been in service with the U.S. Army since 1986. It is a four-blade, twin-engine attack helicopter with a tandem cockpit for a two-man crew.

It has a nose-mounted sensor suite for target acquisition and night vision systems. It is armed with a 30-millimeter M230 Chain Gun carried between the main landing gear, under the aircraft's forward fuselage.

The attack helicopter has four hardpoints mounted on stub-wing pylons, typically carrying a mixture of AGM-114 Hellfire missiles and rockets. The helicopter was designed to replace the Bell AH-1 Cobra as the Army's primary attack helicopter. The U.S. Marine Corps still operates late-model versions of the AH-1 Cobra.

Boeing began deliveries of the AH-64E model in October 2011. Seven customers outside the U.S. have ordered this variant. Including this latest version, the U.S. and 15 other countries have used the Apache during the past three decades. On this order Boeing will do the work in Mesa, Ariz., and should be finished by February 2023. ←

For more information contact ***Boeing Defense, Space & Security*** *online at* www.boeing.com, *or the* ***Army Contracting Command at Redstone Arsenal*** *at* http://acc.army.mil/contractingcenters/acc-rsa.

Marine Corps goes to industry for armored vehicle and open-architecture vetronics

BY **John Keller**

ARLINGTON, Va. — U.S. Navy and Marine Corps researchers are asking industry to build full-scale technology demonstrators of a future reconnaissance armored vehicle to enable Marine battlefield reconnaissance units to fight through the enemy to gather and disseminate crucial intelligence information from the battle front.

Officials of the Office of Naval Research (ONR) in Arlington, Va., released a broad agency announcement last month (N00014-19-S-B002) for the Armored Reconnaissance Vehicle (ARV) Technology Demonstrator

Design, Fabrication, Test & Demonstration program.

The future ARV will be able to fight for information on a complex and contested battlefield using an automatic rapid-fire medium-caliber cannon, remotely operated medium-caliber machine gun, and open-architecture vetronics to include sensors, communications, and battlefield networking.

The project seeks to build two ARV variants — a base model and an at-the-edge model to evaluate technologies, performance, and battlefield concepts. Contractors will build two demonstrators of each variant.

The ARV demonstrators must be able to collect mobility data, determine reconnaissance and sensing capabilities, determine unmanned systems integration and operation, evaluate platform lethality, determine platform survivability, and evaluate overall performance.

Technology demonstrators will have modular open systems architectures, with an eye to future integration of third-party hardware and software and will enable third-party repair.

The base variant and its vetronics will have an average manufacturing unit cost of $6 million per platform for 500 units, with initial operating capability (IOC) in 2027.

The ARV is a possible replacement for the U.S. Marine Corps legacy Light Armored Vehicle (LAV). It would support light armored reconnaissance battalions within the Marine divisions.

The vehicle will have new ways to sense and communicate, will be able to destroy heavily armored threats close-in and at range, and will be transportable with the naval expeditionary force by military and commercial trailers, railway, C-17 fixed-wing aircraft, naval amphibious warfare ships and surface connectors, and Military Sealift Command and commercial ships.

The ARV will have persistent surveillance capability using manned and unmanned vehicles; modern command, control, communications, and computers (C4I) vetronics; cross-country and on-road land mobility with shore-to-shore water mobility; passive & active force protection; direct and indirect weapons; be similar size and weight to the legacy LAV; drive-by-wire capability; and a modular interoperable open-systems architecture.

The ARV will identify weapons and targets through obscurants, beyond

business with the Department of Homeland Security. It also makes night-vision equipment and sensor systems used in military aircraft. The company has established new business units around next-generation military technologies such as undersea drones.

Can China's satellite lidar detect and track deep-diving submarines?

Chinese scientists are working on a laser satellite device they hope will be able to detect from space the location of submerged submarines located as deep as 1,600 feet below the ocean surface. It is the latest addition to China's expanding deep-sea surveillance program, and aside from targeting submarines — most submerged submarines operate at a depth of less than 1,600 feet — it also could collect data on the world's oceans. Project Guanlan, meaning "watching the big waves," officially was launched in May at the Pilot National Laboratory for Marine Science and Technology in Qingdao, China, southeast of Beijing. It aims to strengthen China's surveillance activities in the world's oceans, according to the laboratory's Website.

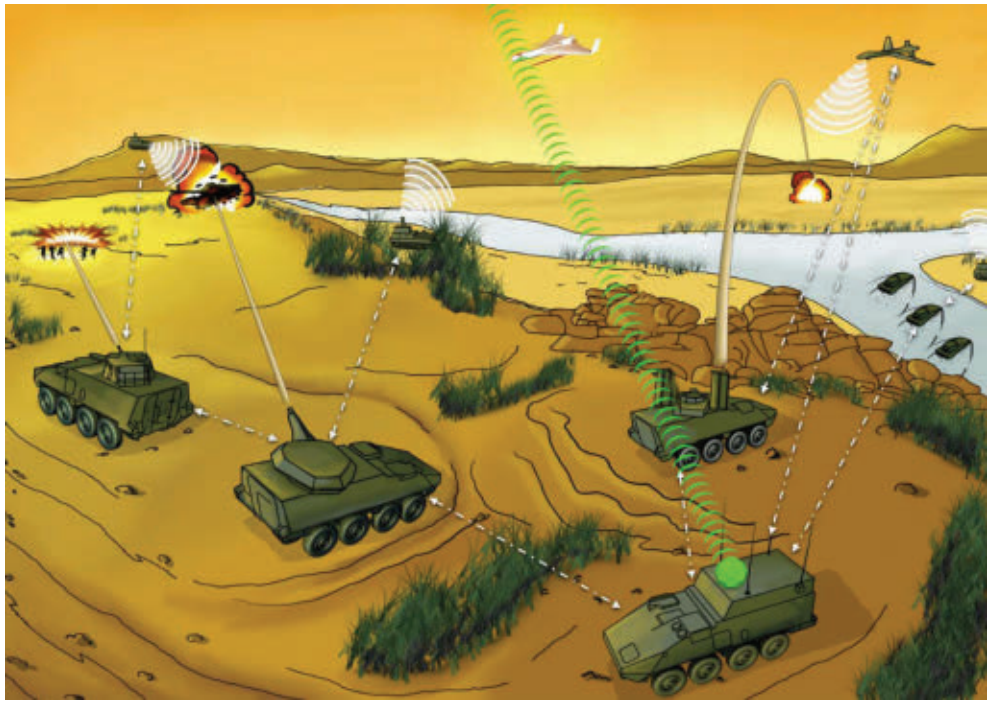
The big hack: how China used a tiny chip to infiltrate U.S. company computer servers

A cyber attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, Bloomberg reported. Amazon.com Inc. began quietly evaluating a startup called Elemental Technologies, a potential acquisition to help with a major expansion of its streaming video service, known today as Amazon Prime Video. Elemental's national security contracts weren't the main reason for the proposed acquisition, but they fit nicely with Amazon's government businesses, such as the highly secure cloud that Amazon Web *[PAGE 12]*

threat range, and beyond line of sight. It also will be able to transmit sensing and targeting information among the crew, the dismounted scout team, other ARV crews, and other Marine Corps sensors, as well as collect, process, and exploit sensor information and disseminate it to other Marine Corps units.

The ARV will be survivable against weapons as large as heavy machine guns, artillery fragmentation rounds, land mines, and improvised explosive devices (IEDs). The Marine Corps is interested in modular and upgradable armor.

The ARV will achieve standoff with active and passive protective systems to sense, orient, classify, track, and



The U.S. Marine Corps wants a new networked armored vehicle with open-systems electronics to conduct reconnaissance and surveillance on the battlefield.

The ARV also communicate voice, video, and data where sensors and communications are degraded. Its command and control system will handle weapons fire control; secure voice, video, and data exchanges; battlefield situational awareness in GPS-denied environments; and control unmanned systems beyond line of sight. Its communications network suite also will be able to operate through cyber attacks, and the vehicle will minimize its visual, infrared, RF emissions, radar cross section, and acoustic signatures.

defeat incoming rocket-propelled grenades, anti-tank guided missiles, and precision-guided munitions.

Companies interested were asked to submit proposals by 19 Nov. 2018. Contract awards will be on or about 4 March 2019. Email technical questions to the Navy's Jeff Bradel at jeff.bradel@navy.mil. Email business questions to Justin Fraser at Justin.S.Fraser@navy.mil. ←

More information is online at https://www.fbo.gov/spg/DON/ONR/ONR/N00014-19-S-B002/listing.html.

Blue Canyon Technologies to design SWaP-C-optimized military satellites

BY **John Keller**

ARLINGTON, Va. —U.S. military researchers are looking to Blue Canyon Technologies in Boulder, Colo., to help develop a constellation of small, secure, and affordable military satellites that not only are able to operate in low-Earth orbit (LEO), but also that capitalize on modern commercial satellite technologies.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., announced a $1.5 million contract to Blue Canyon last month for the Blackjack program to develop SWaP-optimized military communications and surveillance satellites designed to operate in LEO.

Blackjack seeks to develop low-cost space payloads and commoditized satellite buses with low size, weight, power, and cost (SWaP-C) with similar capabilities as today's military communications satellites that operate at geosynchronous orbit (GEO), but at a fraction of the cost.

Blue Canyon Technologies is helping develop a new generation of military communications and reconnaissance satellites optimized for low size, weight, and power consumption (SWaP).

Military satellites are critical to U.S. warfighting capabilities. Traditionally they are placed in GEO to deliver persistent overhead access to any point on the globe.

Yet in the increasingly contested space environment, these costly and monolithic systems are vulnerable targets that would take years to replace if degraded or destroyed.

Moreover, their long development schedules make it difficult or impossible to respond quickly to new threats.

Blue Canyon specializes in turnkey small satellite solutions for surveillance and other applications, including nanosatellites, microsatellites, and Evolved Expendable Launch Vehicle (EELV) Secondary Payload Adapter (ESPA) satellite payloads, including spacecraft buses and custom ground software.

The company has expertise in precision pointing platforms based on high-performance attitude determination and control components. Blue Canyon has developed low-cost high-reliability spacecraft systems and components to enable academic, commercial, and government small satellite applications. The company's spacecraft and subsystems are supporting LEO, geosynchronous orbit (GEO), lunar, and interplanetary missions.

For the first phase of the Blackjack program, Blue Canyon will define bus and payload requirements. Subsequent phases will develop bus and payloads for a two satellite on-orbit demonstration; and demonstrating a two-plane system in low-Earth orbit for six months.

A future Blackjack demonstration constellation will involve 20 spacecraft in two planes with one or more payloads on each satellite.

The DARPA Blackjack program is developing enabling technologies for a global high-speed network backbone in LEO that enables networked, resilient, and persistent military payloads that provide infinite over-the-horizon sensing, signals, and communications capabilities.

Historically, U.S. Department of Defense (DOD) satellites have been custom-designed, with lengthy and expensive design and upgrade cycles. The evolution of commercial space, however, has led to LEO broadband Internet communications satellites that could offer attractive economies of scale.

The Blackjack program emphasizes a commoditized bus and low-cost interchangeable payloads with short design cycles and frequent technology upgrades, based on 'good enough' payloads optimized for more than one type of bus.

Commoditized satellite buses based on open-architecture electrical, software, and mesh network interface control are expected to provide

a way for dozens or hundreds of different types of military satellite payloads to operate in low-Earth orbit, DARPA officials say.

The Blackjack program has three primary objectives:

- payload and mission-level autonomy software with on-orbit distributed decision processors that can operate autonomously with on-board data processing, and perform shared tasks on-orbit;
- advanced commercial manufacturing for military payloads and the spacecraft bus, including high-rate manufacturing using commercial off-the-shelf (COTS)-like parts, reduced screening and acceptance testing for individual spacecraft, and reduced expectations for spacecraft life; and
- satellite payloads in LEO that operate on par with current GEO systems with the spacecraft at costs of less than $6 million per satellite.

To reduce integration risk, Blackjack is developing an avionics unit called Pit Boss for each spacecraft with high-speed processor and encryption devices that will function as a common network and electrical interfaces.

Not only will Pit Boss provide a common electrical interface to each payload, but also will provide mission-level autonomy, enable on-orbit edge computing, manage communications between Blackjack satellites and ground users, provide a command and telemetry link to the bus, and encrypt payload data.

Every Blackjack satellite will consist of one commoditized bus capable of broadband-rate global communications to other nodes, one Pit Boss control unit, and one or more military payloads that can operate autonomously for more than 24 hours.

The goal is to develop a 60-to-200-satellite constellation operating at altitudes of between 310.7 miles and 807.8 miles above the Earth's surface. One operations center will cover all government satellites and payloads, and the constellation will be able to operate without the operations center for 30 days. Blackjack payload data processing will be performed on-orbit without the assistance of ground data processing. ←

For more information contact ***Blue Canyon Technologies*** *online at* http://bluecanyontech.com, *or* ***DARPA*** *at* www.darpa.mil.

[FROM PAGE 8] Services (AWS) was building for the CIA. To help with due diligence, AWS, which was overseeing the prospective acquisition, hired a third-party company to scrutinize Elemental's security. The first pass uncovered troubling issues, prompting AWS to take a closer look at Elemental's main product: the expensive servers that customers installed in their networks to handle the video compression. Nested on the servers' motherboards, the testers found a tiny microchip, not much bigger than a grain of rice, that wasn't part of the boards' original design. The chips allowed the attackers to create a stealth doorway into any network that included the altered machines.

Boeing to build Air Force trainer jets for tomorrow's combat pilots

The Boeing Co. has secured a hat-trick of Pentagon contract wins after it was awarded a deal worth as much as $9.2 billion to build new trainer jets for the U.S. Air Force. The contract to build an initial 351 T-X jets and supply training services is one of the largest Defense Department programs awarded in recent years, with the work helping sustain engineers and production equipment while the Pentagon considers the next generation of combat aircraft due to come into service in the 2030s. Analysts had favored Boeing in the long-running contest, expecting the aerospace giant to bid aggressively to secure the future of its main military jet plant in St. Louis and position itself for future aircraft competitions, such as the Air Force's Penetrating Counter Air plan. Boeing has triumphed in two recent contests to provide refueling drones for the U.S. Navy and helicopters for the Air Force, and its defense arm is on track to increase sales for the first time in four years, but the larger T-X program was viewed by analysts as a key test of its competitiveness. Boeing pitched an all-new plane built in partnership with Sweden's Saab AB. ←

TSA eyes open-systems explosives detection for rapid airport security upgrades

BY **John Keller**

ARLINGTON, Va. — U.S. government airport security experts are moving forward with a project to develop vendor-neutral software for explosives detection in baggage-screening systems at airports and other ports of entry.

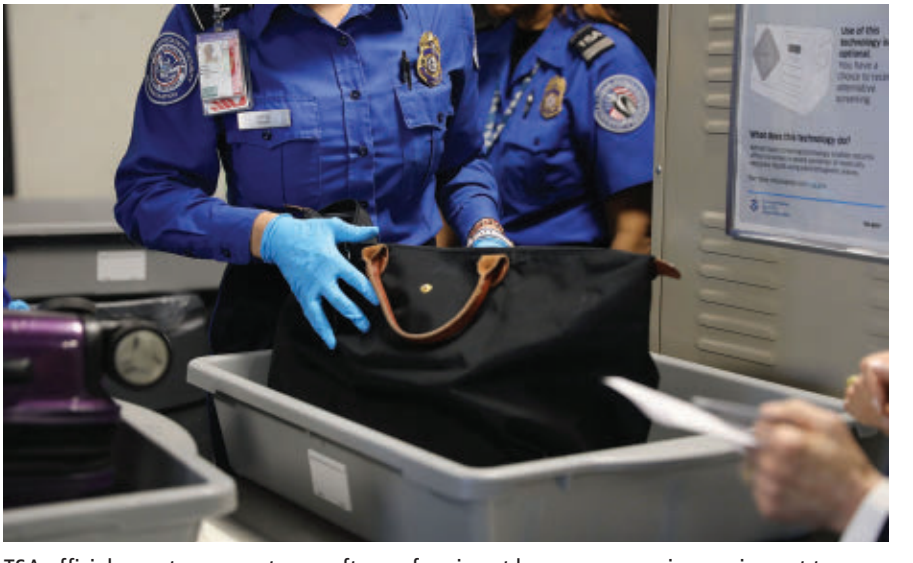
The idea is to develop open-systems explosives-detection software applications that can run on many different baggage-screening systems to enable TSA to compete airport security technology widely through industry, and ensure passenger security systems have the latest technologies.

Officials of the U.S. Department of Homeland Security's Transportation Security Administration (TSA) in Arlington, Va., have announced plans to award an estimated $3 million one-year contract to Stratovan Corp. in Davis, Calif., to develop explosives detection algorithms able to run on a variety of baggage-screening systems — especially those made by Smiths Detection, L-3 Communications, and Leidos.

This sole-source contract would continue an effort with Stratovan, and expand development of the vendor-neutral automated threat-recognition software, on which the company already has started development.

Stratovan has developed an automated threat-recognition algorithm with machine learning capability that uses computed tomography (CT) imaging technology, developed originally for medical applications, for explosives detection in a Smiths Detection CTX-9800 baggage-screening system. The idea was to determine if a third party could develop a vendor-neutral algorithm.

Stratovan has developed a software-development kit (SDK) to convert vendor-proprietary CT-formatted data into a standardized image format for Digital Imaging and Communication in Security (DICOS), and created



TSA officials want open-systems software for airport baggage screening equipment to carry out rapid technology upgrades in airport security.

vendor-neutral automated threat recognition, TSA officials say.

This contract asks Stratovan to update the company's previously developed SDK to the new DICOS 2.0A standard, and provide software tools necessary for third-party development. The company will provide a software library and conformance testing suite to help convert native security vendor data to the new DICOS 2.0A standard.

The DICOS standard, overseen by the National Electrical Manufacturers Association (NEMA) in Arlington, Va., specifies an extensible, interoperable data format that enables the integration of security screening technologies across systems from several different vendors, and facilitates wide participation in developing improved security screening technologies and algorithms.

In addition, this contract asks Stratovan engineers to enable the algorithm to detect home-made explosives and integrate it into an explosives-detection machine. If this works, TSA officials will be able to select automated threat recognition technologies independently of systems vendors.

In this way TSA can avoid being locked-in to explosives-detection technologies that are specific to baggage-screening system suppliers. In addition, TSA officials expect to upgrade explosives-detection capability of baggage-screening devices quickly by going to an industry-standard format.

This should enable TSA to address emerging threats with more resilience and capitalize on innovative solutions in the open market quickly from third party developers.

TSA officials have determined that the most effective way to enhance explosives-detection algorithms while mitigating the risk of a false alarm is through machine learning technology, which Stratovan provides.

Updating the baggage-screening SDK, compliance checker, and certifier to the most recent DICOS standard will help TSA implement the DICOS format, which ultimately will enable third party algorithm development, allow for full and open supplier competitive, TSA officials say. ←

For more information contact ***Stratovan Corp****. online at* www.stratovan.com*, the* ***Transportation Security Administration*** *at* www.tsa.gov*, or* ***NEMA DICOS*** *at* www.nema.org/Standards/Pages/Digital-Imaging-and-Communications-in-Security-Information-Object-Definitions.aspx.

The new world of COUNTER-DRONE TECHNOLOGY

Attempts to prevent unmanned aerial vehicles (UAVs) from surveillance, terrorist, or military attacks involve methods ranging from electronic jamming, to nets, to bullets, and even to birds of prey. **By J.R. Wilson**

Only a little more than a quarter century ago, unmanned aerial vehicles (UAVs) largely were just a curiosity, with little support from the operational military. That began to change with the First Gulf War in 1991 and the successful use of the Pioneer UAV, which by today's standards, was a primitive and limited-use surveillance aircraft. The need to defend against UAVs rarely was even a consideration.

With the Second Gulf War a decade later, UAVs came into their own. Today, they are an essential part of U.S. military missions and operations and are in high demand by nearly every military and law-enforcement agency on the planet. Unlike most critical military equipment, however, UAVs also have gone commercial, equally sought by everyone from oil companies to ranchers, to news media outlets, to environmentalists, forestry services, and fish and wildlife observers.

Darker forces are at work, too. UAVs also are on the shopping lists of criminals ranging from drug cartels, to human smugglers, to corporate spies.

As UAVs have become increasingly popular across many different user communities, their prices have dropped from

The Right RF Parts.
Right Away.

We're RF On Demand, with over one million RF and microwave components in stock and ready to ship. You can count on us to stock the RF parts you need and reliably ship them when you need them. Add Fairview Microwave to your team and consider it done.

Fairviewmicrowave.com
1.800.715.4396

an INFINITE company

Fairview Microwave
RF COMPONENTS ON DEMAND. Done!

government-budget levels to less than that of a TV set. What the government developed in sensor and weapons payloads also has moved into those user groups, albeit not as sophisticated or, in the case of weapons, massively lethal. UAVs now are considered a top threat posed by terrorists, criminals, fanatics, and others who never before had such a versatile, stealthy, and cheap airborne weapon.

This has made counter-UAV technologies and systems a top — and increasingly classified — priority for the military, Department of Homeland Security, major law enforcement agencies, and the contractors producing them. Seeking to maintain a time and technology advantage over threat users, those groups essentially have stopped making public statements about C-UAV.

This new topic of C-UAV is divided into two primary areas: detection and tracking systems; and interdiction. The former includes radar, radio frequency (RF), electro-optical (EO), infrared (IR), acoustic, and combined sensors.

The Boeing laser on a heavy truck called the High Energy Laser Mobile Demonstrator.

Interdiction includes jamming RF and GNSS (Global Navigation Satellite System, which includes GPS and GLONASS), spoofing, lasers, physical nets to entangle the target, projectiles, electromagnetic pulse (EMP), water projectors, "suicide" drones, and combinations of those.

Decades ago saw a flurry of activity in developing unmanned aircraft. Today just as much effort is going into new ways to counter UAVs.

No perfect solutions

There are no perfect detection methods. Many affordable electro-optical sensors are limited to daylight operations and a direct line-of-sight to the target (also true for IR and many RF systems). RF and acoustic sensors use a library of known sounds and frequencies to detect UAVs, but the rapid development of new platforms makes it impossible for those to be fully up-to-date. Sensor sensitivity also is an issue; too sensitive generates many false positives, while reduced sensitivity leads to false negatives.

C-UAV systems, employing combined data from several sensors, also must be able to differentiate between legitimate and hostile, allied, and enemy UAVs — something no known system can do. This is where a human operator must intervene to make what often is a split-second assessment. Interdiction methods also all have potentially negative outcomes, from being blocked by electronic warfare countermeasures to falling onto civilian or friendly forces.

"Compounding the effectiveness issue is the fact that drone technology itself is not standing still," according to a February 2018 Counter-Drone Systems report from The Center for the Study of the Drone at Bard College in Annandale-on-Hudson, N.Y. "The C-UAS market will therefore have to constantly respond to new advances in unmanned aircraft technology. As the unmanned aircraft systems market expands, counter-drone systems will need to be flexible enough to detect and neutralize a growing variety of targets, ranging from large unmanned aircraft capable of carrying heavy payloads through to low-flying micro surveillance drones that might only weigh a few grams."

Sometimes UAV technologies evolve so quickly that counter-UAV systems just can't keep up. "The proliferation of C-UAS technology might even accelerate the development of technologies that will render C-UAS systems ineffective, particularly in military environments," the article continues. "Drones might be programmed to operate in patterns that make them difficult to detect, or rotors might be modified to dampen a drone's engine noise so that it can evade acoustic detection. Drones might be designed in such a way as to reduce their radar signature. Counter-laser systems could protect drones from directed-energy attacks. Finally, forces might seek to deploy drone swarms, which present a range of vexing technical challenges from a C-UAS perspective."

Ground- or air-based

C-UAV systems can be ground- or air-based or even handheld. Most systems on the market today are designed only for detection or for interdiction and the clear majority are ground-based, although a few comprise air and ground components.

One impetus for this reclassification of information about counter-UAV technologies and missions can be seen in FBI Director Christopher Wray's October comments about the "steadily escalating threat" of UAVs by terrorists and criminal organizations at a hearing of the Senate Homeland Security and Governmental Affairs Committee.

"While there has been no successful malicious use of UAS [unmanned aerial systems] by terrorists in the United States to date, terrorist groups could easily export their battlefield experiences to use weaponized UAS outside

the conflict zone," he told lawmakers in written testimony.

"The FBI assesses that, given their retail availability, lack of verified identification requirement to procure, general ease of use and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering."

The UAVs available to and used by such groups are several generations behind the most advanced U.S. military platforms. Still, their payload capacity, guidance and navigation, and range are adequate for smuggling drugs, surveilling routes for human traffickers, or even attacking critical infrastructure or mass public gatherings like sporting events or concerts.

The threat of such applications grows almost exponentially with each new development in commercial UAVs or those developed by and for foreign militaries that find their way onto the black market. It is unlikely that terrorists or criminal organizations ever will be able to match UAVs in U.S. and allied inventories, but such parity is not necessary for their applications.

One of the drones shot down by a MEHEL-equipped Stryker in April at Fort Sill during MFIX-17. Lessons learned during MFIX-17 will make the MEHEL easier for Soldiers to operate.

The counter-UAV mission relies heavily on advanced sensors; long-endurance platforms; data fusion to provide a view of the airspace being guarded; and some form of artificial intelligence (AI) to sort through and analyze incoming data. This process is far more attractive than sending raw UAV sensor data to a human operator.

C-UAV can be airborne, fixed or mobile ground-based or even sea-based. For example, a high-speed mobile battlefield C-UAV system — the eXpeditionary Mobile Aerial Defense Integrated System (X-MADIS) — is being developed by Sierra Nevada Corp. in Sparks, Nev.; Ascent Vision Technologies LLC in Belgrade, Mont.; and RADA Electronic Industries Ltd. in Netanya, Israel.

X-MADIS is capable of long-range UAV detection, identification, and defeat while traversing rough terrain at speeds to 30 miles per hour. According to Sierra Nevada, the C-UAV, radar and electro-optical/infrared (EO/IR) equipment are integrated onto a commercial off-road vehicle to detect, locate, identify, track, exploit, and defeat hostile UAVs threatening airports, critical infrastructure, or entering no-fly zones.

Leonardo DRS is developing the vehicle-mounted Mobile Low, Slow Unmanned Aerial Vehicle Integrated Defense Systems (MLIDS) to disable small drones.

Enhanced counter-UAV sensors

Sensors also have been advancing rapidly in sensitivity, range, and reduced

size and power requirements. Combined with high-speed wireless networking, onboard data fusion, and AI, they have significantly increased the capabilities of C-UAV systems.

"Our security mission is architected around multiple sensors to give the best picture of the airspace and lowest false alarm rate, looking for anything moving in the airspace," says Craig Marcinkowski, director of the SRC Inc. Gryphon Sensors business unit in North Syracuse, N.Y. "But a large bird and small drone could look the same on radar, so you also look for communications links, at which point you may have a camera that slews over to get a better look.

"Today, there is an operator in the loop at some level, assessing what is on the screen, what kind of payload a drone may be carrying," Marcinkowski continues. "We're working on automatic image lookup, where you can take the operator out of the loop to identify a bird from a drone. We're focused on deconflicting the low-altitude airspace and safe airspace integration, enabling beyond visual line-of-sight flying, using sensors that create an accurate 3D image of what's out there. You also can use that data for security applications around critical infrastructure."

Military challenges

The other side of counter-UAV is more complex — military programs to counter enemy UAVs, ranging from those performing intelligence, surveillance and reconnaissance (ISR) missions against U.S. or allied forces to stopping hunter-killer UAVs sent to attack such forces or cripple critical infrastructure.

While the current adversaries engaging U.S. forces are terrorist, insurgent, or would-be states (i.e., the Taliban and ISIS), whose UAVs are similar to those being confronted along U.S. borders and coastal areas. Future conflicts may see the U.S. facing something it has not seen in the air for decades — peer or near-peer technologies and capabilities.

"Enemy unmanned aircraft are among the biggest threats facing our ground troops today," Thomas Bussing, vice president of the Raytheon Co. Advanced Missile Systems segment in Tucson, Ariz., said in July while announcing a contract from the Army to use Raytheon's small, expendable Coyote UAV and KRFS radar to combat enemy UAVs in the battlespace.

Raytheon's Multispectral Targeting System (MTS) combines optical and infrared sensors to acquire and track airborne targets and direct the laser beam it fires. For C-UAV, the MTS was modified to track Class-1 drones (under 20 pounds) and Class 2 drones (between 20 and 55 pounds), the most common sizes used by terrorists and insurgents.

The Army already has tested an anti-UAV defense system (AUDS) during the 2017 Maneuver Fires Integrated Experiment at Fort Sill, Okla. AUDS comprises two 180-degree radars mounted back-to-back to provide 360-degree real-time coverage and a camera to confirm the target's identity. Once confirmed as a hostile UAV, the operators can destroy it, or jam its communications, causing the UAV to return home or crash.

Dr. Robert W. Sadowski, the U.S. Army's Chief Roboticist at the Tank Automotive Research, Development and Engineering Center (TARDEC) in Warren, Mich., says the military also is adapting and improving commercial developments to meet that threat.

"Commercial is more leveraging technologies that have been hardened for military applications," Sadowski says. "The range of temperatures they operate under is a little more relaxed, so that has to be ruggedized. The commercial world has been really pushing down the cost of sensors, which also are getting smaller, enabling more sensors to be placed on existing UAVs.

Sensor fusion

"Sensor fusion is another area where a lot of work is being done on multi-modal radars and camera imagery," Sadowski continues. "The other piece, the auto industry, brings in high computing capability for low cost and power. Where a decade ago you might have needed a supercomputer, today the gaming industry has helped bring the cost and size of high-performance computing down."

In July, the Army announced a $13 million award to Leonardo DRS to continue engineering and testing of the Mobile Low, Slow UAV Integrated Defense System (MLIDS). In October 2017, the company was awarded a $43 million production contract for an undisclosed number of MLIDS to meet the Army's need to counter small,

inexpensive UAVs — such as commercial quadcopters — operating as airborne improvised explosive devices (IEDs).

MLIDS is mounted on two mine-resistant, ambush-protected all-terrain vehicles (M-ATVs), one carrying the DRS elevated mast-mounted surveillance and battlefield reconnaissance equipment (EO/IR sensors), the other a reconfigurable integrated-weapons platform (RIwP) developed by Leonardo and Moog, capable of firing a range of kinetic weapons, and a small UAV.

"Drones are becoming an increasingly dangerous threat against our forward-deployed soldiers and we are proud to support this urgent requirement to protect them from potentially lethal small unmanned aerial vehicles," Aaron Hankins, vice president and general manager for DRS Land Systems, said at the time. "We are working hard to deliver the best capability to our soldiers as quickly as possible."

Military C-UAV systems rely on multi-layered detection technologies — EO/IR, RF scanners, radar. cameras, jammers and tracking software. They also can include a variety of kill capabilities, from guns and rockets to lasers and electronic warfare (EW).

Market analysts predict the global military market for C-UAV will grow from around $300 million today — primarily U.S. research, development, testing and evaluation (RDT&E) — to around $1 billion by the end of 2019. The commercial market has tripled in the past year, from around $30 million to close to $100 million, although that is predicted to be limited by FAA regulations on UAV flight in the

The Boeing High Energy Laser Mobile Demonstrator (HEL MD), developed originally to protect forward-deployed warfighters from rockets, mortars, and artillery shells, is yielding laser weapons technology to counter unmanned aerial vehicles.

national airspace and a lack of proven UAV attacks — including corporate espionage — on U.S. targets.

The role of artificial intelligence

AI is even more important to the future of military counter-UAV than it is to border protection.

"[The key is] how to do real-time processing of video feeds and create effective perception in a complex electromagnetic environment, synthesized so the commander can make decisions quickly," says TARDEC's Sadowski. "How do we do reasoning at the tactical level, making the mechanical platform part of the team? There is a lot of work that needs to be done on human/machine interface and cognitive load. These are things under active pursuit in the labs now, how to do real-time updates, advanced situational awareness and solving the perception and prediction problems.

"Most of what we're working on now is more deterministic systems," Sadowski continues. "AI is less deterministic. You have to train the robot to do what it needs to do. That requires lots of training runs with relevant data, but some amazing things are being done in that space. Start off with perception — is that a bird, a balloon or a UAV; then prediction, taking stuff between frames and stitching together a temporal message, which leads to planning. Prediction has not yet been done by neural nets. Some of these things can be solved working with machine learning or AI."

As with any military capability, advances by one side are quickly challenged by advances on the other side. Rapid technological advances being made on an almost daily basis by commercial and military scientists and engineers have put additional

COUNTER-DRONE COMPANY LIST

Aaronia AG
Strickscheid, Germany
https://www.aaronia.com

Accipiter Radar Corp.
Orchard Park, N.Y.
https://www.accipiterradar.com

Advanced Protection Systems LLC
Rutherford, N.J.
http://apsystems.tech/en/

Airspace Systems Inc.
San Leandro, Calif.
https://airspace.co

Alion Science & Technology Corp.
McLean, Va.
https://www.alionscience.com

Allen-Vanguard Corp.
Ottawa
http://www.allenvanguard.com

ApolloShield
Palo Alto, Calif.
https://www.apolloshield.com

Batelle
Columbus, Ohio
https://www.battelle.org

Blighter Surveillance Systems
Great Chesterford, England
http://www.blighter.com

Chenega Europe
Belfast, Norther Ireland
http://www.chenegaeurope.com

CINTEL LLC
Peachtree City, Ga.
http://cintelusa.com

Citadel Defense Co.
San Diego
https://www.dronecitadel.com

CTS Technology Co. Ltd.
Shenzhen, China
https://ctstechnologys.com

Dedrone Inc.
San Francisco
https://www.dedrone.com

Delft Dynamics Holding B.V.
Delft, The Netherlands
https://www.delftdynamics.nl

Department 13 International Ltd.
Columbia, Md.
https://department13.com

DeTect Inc.
Panama City, Fla.
https://detect-inc.com

DJI
Shenzhen, China
https://www.dji.com/aeroscope

Drone Defence
London
https://www.dronedefence.co.uk

Drone Major Ltd
London
https://dronemajor.net

DroneShield
Sydney, Australia
https://www.droneshield.com

Guard From Above
The Hague
http://guardfromabove.com

Hensoldt
Taufkirchen, Germany
https://www.hensoldt.net

IACIT
Sao Jose dos Campos, Brazil
http://www.iacit.com.br

KB Radar Design Bureau
Minsk, Belarus
http://www.kbradar.by/en/

L-3 Technologies
New York
https://www.l3t.com

Liteye Systems Inc.
Centennial, Colo.
http://liteye.com

Lockheed Martin Corp.
Bethesda, Md.
https://lockheedmartin.com

MBDA Deutschland
Schrobenhausen, Germany
https://mbdainc.com

Meritis
Cham, Switzerland
https://www.meritis.ch/index.html

MCTECH Technology Ltd.
Kfar Saba, Israel
http://mctech-jammers.com/index.html

Sanad Academy
Dubai, UAE
http://www.sanadacademy.ae

Securus Technologies
Dallas
https://securustechnologies.tech

Sensofusion
Vantaa, Finland
https://www.sensofusion.com

Sierra Nevada Corp.
Sparks, Nev.
https://www.sncorp.com

Snake River Shooting Projects
Emmett, Idaho
https://snakerivershootingproducts.com

SRC Gryphon Sensors
North Syracuse, N.Y.
https://www.srcinc.com

Theiss UAV Solutions
North Benton, Ohio
http://www.theissuav.com

UMS Aero Group
M^hlin, Switzerland
https://umsskeldar.aero

ZALA Aero
Izhevsk, Russia
http://zala.aero/

pressures on the development and fielding of UAVs and counter-UAV systems.

"AI is a really key area. China is making a strong push in AI, which is a serious concern. The U.S. is still in the lead, but China has made this a national priority, with large investments and a huge focus, "says Phil Finnigan, UAV analyst at the Teal Group market research firm in Fairfax, Va.

"Another revolutionary technology is low-cost HALE [high altitude, long endurance]. Some of the systems primarily being developed for the civil/commercial world, primarily by Airbus and AeroVironment, for example, offer tremendous potential for long-term surveillance or communications at low cost. That is being driven by commercial programs, but will have a lot of defense and homeland security applications."

A HALE UAV offers wider coverage for an extended time during ISR missions, giving military and homeland security users a greater chance of detecting and identifying hostile UAVs, sending back information in real-time to enable the employment of appropriate counter-UAV measures. Those range from guns and rockets to non-kinetic electronic signals to jam, spoof, destroy, or take over the target UAV's navigation and control systems. One option under investigation, for example, would cause the UAV to return to its launch point, enabling authorities to locate and take appropriate action against adversary ground-control stations and personnel.

Cyber security

In a mirroring of the long-standing armor/anti-armor development cycle, some companies have begun working on counter-C-UAV, such as Raytheon's Electronic Armor to prevent UAVs from being hacked.

UAVs have demonstrated their value during the wars in Iraq, Afghanistan and Syria. First used by the U.S., then its allies, they now are a common weapon of ISIS and other non-state groups, primarily as flying IEDs.

Today, UAVs come in all types, sizes and prices, with hundreds of manufacturers in most of the world's nations. That, in turn, has spurred an explosion in the number of C-UAV manufacturers and systems in just the past year or two and the start of yet another layer with counter-C-UAV.

Among those who have announced or demonstrated programs are: Advanced Ballistics Concepts, Aaronia AG, Accipter, Advanced Protection Systems, Airbus DS Electronics, Airspace Systems, Alion Science & Technology, Allen-Vanguard, ApolloShield, BAE Systems, Batelle, BATS, Blighter Surveillance, Boeing, CACI, Chenega Europe, Cintel, Citadel Defense, CTS Technology, Dedrone, Delft Dynamics, Department 13 Intl., DeTect, DJI, Drone Defence, DroneShield, DRS/Moog, Dubai Civil Aviation Authority, General Dynamics, Groupe Assman, Gryphon Sensors, Guard From Above, Hensoldt, IACIT, Kalashnikov/ZALA Aero Group, KB Radar Design Bureau, L3 Technologies, Liteye Systems, Lockheed Martin, Malou Tech, MBDA Deutschland, Meritis, MCTech, Northrop Grumman, OpenWorks Engineering, Prime Consulting & Technologies, Rafael, Raytheon, Saab, Sanad Academy, Securus Technologies, Sensofusion, Sierra Nevada, Skysec, Snake River Shooting Projects, SRC, Systems DroneShield, SystemsGrok, Thales, Theiss UAV Solutions, UMS Aero Group.

According to the Counter-Drone Systems report, 155 companies in more than 30 nations were working on more than 230 C-UAV products; all three numbers almost certainly have grown since then. Those do not include military labs such as DARPA, the Russian Foundation for Advanced Research Projects and China's Scientific Research Steering Committee.

SWaP-optimized instruments for flight line test and measurement

Today's flight-line test systems are small enough to fit in a technician's toolbox, and offer new features like Ethernet and USB interconnects, as well as data and cyber security

BY **John Keller**

The Abaco palm-sized BT3-USB-MON MIL-STD-1553 avionics databus monitor is for flight line databus test applications.

Perhaps nowhere else is avionics test and measurement more crucial than on the flight line. This often is the final check to ensure that aircraft weapons, navigation, communications, databuses, and other mission-critical systems are in working order. The ability to detect potential faults at the last minute can spell the difference between mission failure and mission success, and it's up to the technicians on the flight line — on the air base tarmac or on the aircraft carrier flight deck — to perform these last important checks.

These technicians need to be fast, thorough, and well trained. Their equipment also needs to be reliable, easy to use, and work in some of the most difficult and demanding conditions imaginable: extremes of heat and cold; rain, fog, and salt spray; and in the darkness of night. How many flight-line techs tell stories about rendering military aircraft mission-ready at 2:00 in the morning during a driving rain?

The good news: flight-line test and measurement equipment represents one of the most promising opportunities for systems upgrades and technology insertion. Never a top investment priority compared to aircraft, avionics, and weapons, flight-line test gear tends to be large, cumbersome, and dated. Not only can it be difficult to use right beside aircraft — especially in harsh operating conditions — but some of these instruments also are falling behind technologically as aircraft weaponry evolves rapidly from dumb bombs to smart munitions.

"The biggest thing driving our customers is moving away from sustaining legacy testing that was designed before the era of smart weapons," explains Stephen Sargeant, CEO of Marvin Test Solutions Inc. in Irvine, Calif. Marvin specializes in trouble-shooting the electronic connections between aircraft weapons racks and the weapons themselves.

Sargeant makes a distinction between what he terms the "old-old," and the "new-old," when it comes to flight line test equipment. The "old-old," he says, refers to antiquated test gear that's nearly impossible to keep working, due to obsolete parts and hard-to-find batteries. The "new-old" describes redesigned test equipment that takes care of obsolescence issues, but that still has the same technological limitations of the pre-smart-weapons era, namely, an ability to check for faults in electrical signals, but not in digital data signals.

"Customers want not just to get the old made new, but want new technology to enable the best testing of smart weapons," Sargeant says. "We can look beyond the Mk 82 and Mk 84 bombs, which are relatively dumb weapons, to JDAM [Joint Direct Attack Munition] and Small-Diameter Bomb. We can allow technicians to test functionality beyond just continuity."

Priority

Source High-Reliability RF Cables

Need(s):

- ☑ Reliability
- ☑ J-STD Soldering
- ☑ Test Reports
- ☑ Lot Traceability

Tomorrow?

Pasternack

Complete Line of High-Reliability RF Cables Shipped Same-Day!

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

866.727.8376
Pasternack.com

an INFINITE company

PASTERNACK®
THE ENGINEER'S RF SOURCE

Flight line test today involves more than just testing aircraft cabling and connectors for their ability to carry electrical signals properly, Sargeant says. "Sure, you can test with that Ohmmeter to test whether that lamp will function properly, but now take an airplane with MIL-STD-1760 bus between the aircraft and the weapon," Sargeant says. "We can test the functionality of this 1760 bus with our hand-held test system, and actually emulate the weapon. We allow for the ability of the airman to test the functionality, select the test he wants to run, test whether it is properly communicating between the airplane and the weapon, and test the arm-and-release sequence prior to loading-up the weapons on the aircraft."

The flagship flight line test instrument from Marvin Test is the MTS-3060 SmartCan, an advanced tester for pylons, launchers, bomb racks, and pods. The hand-held device is in the shape of a beer can that provides measurement, loading, and stimuli functions for continuous squib circuit monitoring, multiple load channels, audio and video simulation, and MIL-STD-1760 support.

The SmartCan is compatible with legacy beer can testers, and offers new adapters and cables to help reduce costs, improve reliability, and provide a path forward from legacy adapters and cables.

The MTS-3060 SmartCan from Marvin Test Systems is an advanced tester for aircraft pylons, launchers, bomb racks, and pods, and offers MIL-STD-1760 support.

Size, weight, and power consumption (SWaP)

One of the chief advantages to the Marvin SmartCan is its small size, weight, and power consumption (SWaP), compared to legacy flight line test gear. "Today when you look at the F-16, F-15, A-10, F-22, and F-35 military aircraft, all have different-level test equipment supporting their armament," Sargeant says. "Now the Air Force can have the same hand-held test set across all its fighters, manned and unmanned."

The Marvin SmartCan is 8.25 inches long, 3 inches in diameter, has front and rear panels that measure 3.5 by 3.5 inches, and weighs 4.2 pounds — just right for a flight tech's toolbox. The SmartCan kit adds adapters, cables, and case, and weighs 35 pounds.

Abaco Systems in Huntsville, Ala., offers the palm-sized BT3-USB-MON MIL-STD-1553 avionics databus monitor for flight line test and measurement applications. It interfaces by USB port to laptop computers and oscilloscopes to provide flight techs with just the equipment they need, rather than provide large integrated test and measurement gear.

The 1553 databus moves data at 1 megabit per second — relatively slow for today's standards — and is designed to send digital instructions to aircraft control surfaces, weapons, and other flight- and mission-critical subsystems. It's ubiquitous, has been in service for decades, and should be part of military avionics for many years to come. "I don't see 1553 going away in any of our lifetimes; it will be out there forever," says Mike Hegarty, product line manager of databus products at Data Device Corp. (DDC) in Bohemia, N.Y.

"The BT3-USB-MON plugs into a laptop with our software called Bustools 1553, and plugs into the aircraft 1553 cabling at a coupler to record and analyze databus data," says Peter Gardiner, sales specialist for avionics at the Abaco

The Marvin Test MTS-3060 flight line test system can operate on a variety of combat aircraft, including the F-16 jet fighter and the A-10 ground-attack aircraft.

Systems Avionics Products segment in Goleta, Calif.

When it comes to analyzing analog electrical signals, the Abaco BT3-USB-MON also plugs into an oscilloscope to help technicians see rise and fall times, zero-crossing point violations, and message timing. "If the problem is in the cabling infrastructure, that can change the 1553's characteristics," Gardiner says. "This is easy to use on the flight line, and is a monitor-only device so it is very simple, and priced so we can see this in the tool kit of an avionics technician." The BT3-USB-MON is designed to be rugged to withstand drops onto concrete by flight maintenance personnel.

The Abaco device is a simple and straightforward databus monitor. "To sniff 1553 data, you don't need a high level of functionality," Gardiner says. "You just want to listen to the data, look at the data in real time, be able to record this data, and then analyze this data offline to look at and assess what's happening in the data."

DDC's Hegarty says flight line test equipment is following a trend like computing equipment "as things get smaller, lighter, faster, and in portable computing platforms as COTS building blocks."

Future trends in flight line test equipment are extending beyond 1553 to higher-speed data networks like Ethernet, experts say. "On the military side, 1553 is old technology; it's been around since the 1970s," says Abaco's Gardiner. "There are new communications protocols all the time, and it's highly likely that flight line test equipment will move to Ethernet. I see a parallel set of tools that will emerge for those kinds of applications," he says. "There is a need, because you must be able to support these products in the field at the flight-line level."

Logistics and flexibility

Today's flight line test equipment is capitalizing on modern computer technology to offer advantages above and beyond SWaP. Marvin's SmartCan test system, for example, can accommodate several different software profiles that represent different weapons and aircraft to enable one system to handle a wide variety of test scenarios.

"We have loaded multiple airplanes with their weapons into one of our test sets, and have deployed with one test set loaded with as many as four aircraft, and have tested all the weapons they carry," says Marvin's Sargeant.

COMPANY LIST

Abaco Systems
Huntsville, ala.
http://www.abaco.com

Astronics Corp.
East Aurora, N.Y.
http://www.astronics.com

Behlman Electronics
Hauppauge, N.Y.
http://www.behlman.com

Data Device Corp. (DDC)
Bohemia, N.Y.
http://www.ddc-web.com

DTS Diversified Technical Systems
Seal Beach, Calif.
http://www.dtsweb.com

Kaman Precision Products
Middletown, Conn.
http://www.kamansensors.com

Keysight Technologies
Santa Rosa, Calif.
http://www.keysight.com

Marvin Test Solutions
Irvine, Calif.
http://www.marvintest.com

Meggitt Sensing Systems
Irvine, Calif.
http://www.meggittsensingsystems.com

National Instruments
Austin, Texas
http://www.ni.com

Rohde & Schwarz
Columbia, Md.
http://www.rohde-schwarz.com

Saelig Co. Ltd.
Fairport, N.Y.
http://www.saelig.com

Tektronix
Beaverton, Ore.
http://www.tek.com

VIAVI Solutions Inc.
San Jose, Calif.
https://www.viavisolutions.com

Vishay Precision Group
Malvern, Pal
http://vpgsensors.com

VTI Instruments
Irvine, Calif
http://www.vtiinstruments.com

"We haven't maxed the can out yet. The software is how we adjust adding additional aircraft, matching the steps of the test to how the airplane talks to the weapons and back."

In addition to software, Marvin designers are using field-programmable gate arrays (FPGAs) to enhance the SmartCan's utility. FPGAs, Sargeant says, "offer a lot of flexibility, and help us miniaturize the size and logistics footprint down to handheld size, and provide very ruggedized flight-line-qualified packaging."

These advantages extend to maintaining advanced military aircraft when they are away from their home bases on extended deployments. Modern test equipment typically is small enough to move easily to new facilities where maintenance personnel might not be familiar with newly arriving aircraft, Sargeant points out. "DOD [the U.S. Department of Defense] is looking to reduce the total cost of procurement, sustainment, and ownership of test equipment," he says."

This also can help lighten the burden of training for aircraft maintenance technicians. "Part of smaller and more interoperable test equipment is ease of training," Sargeant points out. "If you are an Air Force armament maintainer on the F-16, you will have new equipment requiring more training when you move to another aircraft. But if you train on the SmartCan, you can switch airplanes and not have to be retrained. Just select a different airplane on the SmartCan, and you're ready."

Data security

Increasingly, flight line test technicians need the ability to separate classified and unclassified data as they test for the integrity of aircraft information and communications links. DDC is partnering with data security specialist Tresys Technology LLC in Columbia, Md., to enable separation of so-called red and black data, Hegarty says.

"They have a data diode, where you have secure and unsecure networking, and this controls what information flows from the secure to the unsecure network," Hegarty says. "We are manufacturing a system in partnership with them that does this in a 1U form factor rackmount server setup. We have the capability to apply their algorithms to our equipment, like the Avionics Interface Computer (AIC) — a small-form-factor computing box that people can

use to host all kinds of applications," he says. "It has avionics-specific I/Os, and people can use it as a router or gateway, as a flight-line tester, or as part of a flight-line test setup."

There is more to data security than separating red and black data, however, and avionics test and measurement experts are extending their expertise to include future cyber security threats like software malware and other kinds of data corruption.

Cyber security

"There is a lot of activity related to cyber security," Hegarty says. "In flight line equipment, that is one area of vulnerability because it does offer potential paths to introduce threats in systems, and that is a major concern. A trend is more cyber-secure and cyber-aware solutions going forward."

The compact Avionics Interface Computer (AIC) from Data Device Corp. is a small-form-factor computing box with avionics-specific I/Os that can function as a router or gateway, as a flight-line tester, or as part of a flight-line test system.

Any time that aircraft avionics systems connect to a USB thumb drive, laptop computer, the Internet, or any other outside data path poses the potential for infection from computer viruses, worms, or other malware that could corrupt or steal data, or even enable an adversary to take control of the system. "The threat of cyber attacks, and the need for cyber security to defend against them is huge," says Marvin's Sargeant.

One way Marvin defends against cyber threats is providing no connection between the SmartCan and the Internet. Plus, the latest version of the instrument has built-in cyber security. The device also has a removable SD memory card that users physically can lock away, if necessary.

The SmartCan "can do all the work, like downloading test logs, from a stand-alone computer system," he says. "The interface has been USB. That is still available, and some customers are saying they need to block USB and add Ethernet, which is less susceptible than USB to malware attacks." ←

Army's new electronic warfare (EW) tactical vehicle is first of its kind in years

Elements of the U.S. Army's 1st Cavalry Division have begun testing a new armored vehicle for electronic warfare (EW) that can jam enemy communications systems and other emitters. As potential opponents — especially Russia — invest heavily in similar systems, the service is looking to reinvigorate its own EW capabilities, which largely eroded after the end of the Cold War. Earlier in September 2018, the 1st Cavalry Division's 3rd Brigade Combat Team sent personnel to the Yuma Proving Ground in Arizona for a two-week course in operating the new system, known as the Electronic Warfare Tactical Vehicle (EWTV). The Army's Rapid Equipping Force (REF) first announced plans to build the EWTVs on a prototype basis for field testing in the United States, as well as potentially Europe and South Korea.

GATR Technologies lands $522 million Army contract for inflatable satellite antennas

GATR Technologies Inc. in Huntsville, Ala., won a $522 million U.S. Army order on Friday for inflatable satellite antenna systems. These antennas are mobile, lightweight, and quick to set up in the field for on-the-spot satellite communications (SATCOM) the antennas look like giant rubber balls, and can survive and operate through several hits from small-arms fire. GATR's ground-mounted antennas have tie-downs to point them in the right direction. The antenna inside is reflective fabric. Fans keep the air pressure in the top half slightly higher than in the bottom half, pushing the fabric down into the right shape. ←

Enhancing positioning, navigation, and timing (PNT) for BACN command and control

BY **John Keller**

HANSCOM AIR FORCE BASE, Mass. — Military communications experts at Northrop Grumman Corp. are providing satellite navigation capabilities for a major airborne battlefield communications system to enhance the system's positioning, navigation, and timing (PNT).

Officials of the U.S. Air Force Life Cycle Management Center at Hanscom Air Force Base, Mass., have announced an $80.2 million order to the Northrop Grumman Corp. Mission Systems segment in Middle River, Md., to provide military Global Positioning System (GPS) for the Battlefield Airborne Communications Node (BACN) aboard the Air Force Bombardier E-11A command-and-control aircraft.

The BACN is an electronic payload aboard the E-11A and Air Force RQ-4 Global Hawk large unmanned aerial vehicle (UAV). The E-11A is based on the Bombardier Global Express business jet.

BACN uses the Airborne Executive Processor (AEP) to enable a persistent voice and data gateway in the sky that receives, bridges, and distributes communications among all participants in a battle.

RF and microwave upgrades are expected to enhance positioning, navigation, and timing (PNT) of the Air Force Battlefield Airborne Communications Node (BACN).

The BACN payload aboard the E-11A and Global Hawk helps enable diverse battlefield weapon systems to communicate with each other during in-theater operations where mountainous terrain, large buildings, or other obstructions inhibit line-of-sight communications.

Military leaders found that such obstructions could limit operating units to see only a limited set of the complete picture of the battlefield. The BACN command and control network is designed to provide situational awareness from small ground units in contact up to the highest command levels, Northrop Grumman officials say.

BACN's AEP provides translator and gateway interfaces among all supported communications systems, and forwards intelligence information to the Global Information Grid. By controlling the AEP via a ground station, BACN is radio- and platform-agnostic, Northrop Grumman officials say.

On this order Northrop Grumman will do the work installation and testing at the Bombardier facility in Wichita, Kan., and military testing at Edwards Air Force Base, Calif. The job should be finished by September 2020.

For more information contact ***Northrop Grumman Space & Mission Systems*** *online at* www.northropgrumman.com, *or the* ***Air Force Life Cycle Management Center*** *at* www.wpafb.af.mil/aflcmc.

Electronic warfare (EW) upgrades to boost EA-18G electronic attack

BY **John Keller**

PATUXENT RIVER NAS, Md. — U.S. Navy airborne electronic warfare (EW) experts are working together with the Boeing Co. and Northrop Grumman Corp. to upgrade the AN/ALQ-218 signals intelligence (SIGINT) system aboard the Boeing EA-18G Growler aircraft to provide the system with electronic attack capability.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., have announced a $24.4 million order to the Boeing Defense, Space & Security segment in St. Louis to provide airborne electronic attack system enhancements to the ALQ-218 receiver hardware and communication lines between assemblies to accommodate future planned functional growth and enhancements.

The AN/ALQ-218 from the Northrop Grumman Mission Systems segment in Baltimore is a passive sensor system that functions as a radar warning receiver, electronic support measures, and electronic intelligence.

The system provides airborne situational awareness and signals intelligence (SIGINT) by detecting, identifying, locating, and analyzing sources of radio frequency (RF) emissions.

The AN/ALQ-218 is aboard the EA-18G electronic warfare (EW) jet and the P-8A Poseidon maritime patrol aircraft, and is being considered in the future for unmanned aerial vehicles (UAVs) and submarines.

The Navy EA-18G carrier-based electronic warfare aircraft carries multimode radar detection, suppression, and countermeasure equipment, such as the multiple AN/ALQ-99 radar jamming pods on its wing tips and tail, the AN/ALQ-218 EW receiver, and a communications countermeasures system installed in the plane's gun bay.

Electronic warfare experts from Boeing and Northrop Grumman aim to provide upgrades and enhancements to communications among the Growler's jammers and RF receivers to enable future capabilities like automatic

Boeing is making upgrades to the U.S. Navy EA-18G Growler electronic warfare aircraft to enhance its offensive electronic-attack capability.

jamming of enemy radar and communications systems quickly once detected.

The AN/ALQ-218 can operate on RF bands 0, 1, 2, and band 3, with pulsed and continuous-wave radar with optional communications support, while providing specific emitter identification. It offers enhanced fine frequency measurement to support electronic jamming.

The contract calls for Boeing to modify 13 sets of WRA-7, WRA-8, WRA-9, as well as 18 AEA gun bay pallets. Boeing also will write technical directives for the Navy and the government of Australia.

The Boeing EA-18G Growler is a specialized version of the two-seat carrier-based F/A-18F Super Hornet jet fighter bomber that is adapted for electronic warfare — specifically jamming enemy radar and communications, as well as attacking enemy radar installations with missiles that home-in on radar signals.

The Grower, which is replacing the Northrop Grumman EA-6B Prowler carrier-based EW aircraft, began production in 2007 and entered operational service in late 2009 with the U.S. Navy. The EA-18G aircraft are based at Whidbey Island Naval Air Station in Oak Harbor, Wash.

The growler is designed for suppression of enemy air defenses; stand-off and escort jamming; non-traditional electronic attack by integrating with ground EW operations; self-protect and time-critical strike support; and cost-effective technology insertion and system upgrades.

The Growler's flight performance is like that of the F/A-18E/F Super Hornet, which enables the Growler to perform escort RF jamming as well as traditional standoff radar jamming and deception. The aircraft has more than 90 percent in common with the standard Super Hornet, sharing airframe, Raytheon AN/APG-79 AESA radar, and weapons like the AN/AYK-22 stores management system.

Most of the Growler's EW attack equipment is mounted on the aircraft's wing tips and in the space that on the Super Hornet houses a 20-millimeter cannon. The Growler has nine weapons stations for weapons and jamming pods.

The Growler's EW gear includes the AN/ALQ-218 wideband receivers on the wingtips, and ALQ-99 high- and low-band tactical jamming pods. The ALQ-218 and ALQ-99 form an EW suite that provides detection and jamming against all known surface-to-air missiles. The aircraft is being readied for future threats with the Raytheon Next-Generation Jammer (NGJ).

The Growler can carry as many as five ALQ-99 jamming pods and two AIM-120 AMRAAM air-to-air missiles or AGM-88 HARM anti-radar missiles. It uses an interference cancellation system that allows radio voice communication during jamming.

The Growler has a crew of two, is 60 feet long with a 45-foot wingspan, and 16 feet high. The twin-engine jet can fly as fast as Mach 1.8, higher than 50,000 feet, and can fly 1,275 miles between refueling.

Boeing is the overall systems integrator for the EA-18G Growler combat jet. The plane's electronic warfare equipment comes primarily from Northrop Grumman Corp. Its future Next-Generation Jammer equipment will come from Raytheon Co., and the jet's onboard mission computers come from the General Dynamics Corp. Advanced Information Systems segment in Minneapolis.

On this order Boeing and its subcontractors will do the work in Baltimore; St. Louis; St. Augustine, Fla.; Bethpage, N.Y.; Patuxent River, Md.; and China Lake, Calif., and should be finished by December 2020.

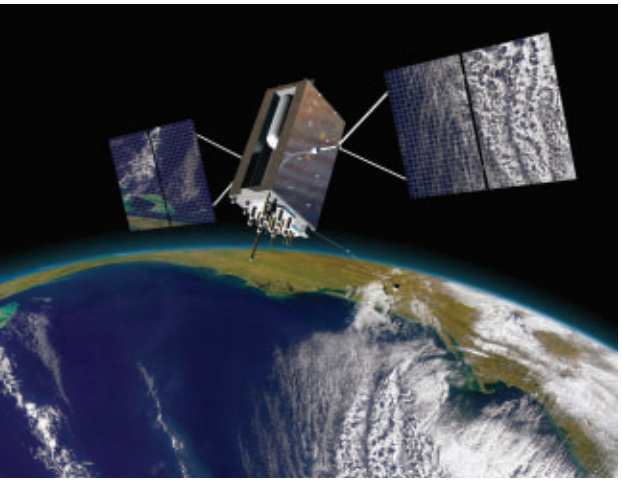
For more information contact ***Boeing Defense, Space & Security*** *online* www.boeing.com/defense, ***Northrop Grumman Mission Systems*** *at* www.northropgrumman.com, *or* ***Naval Air Systems Command*** *at* www.navair.navy.mil.

Lockheed Martin to improve GPS IIIF navigation satellite accuracy and reliability

BY **John Keller**

LOS ANGELES AFB, Calif. — Navigation satellite designers at Lockheed Martin Corp. are moving forward with the nation's latest satellite navigation spacecraft — the Global Positioning System (GPS) Block IIIF.

Officials of the U.S. Air Force Space and Missile Systems Center at Los Angeles Air Force Base, Calif., have announced a $1.4 billion contract to the Lockheed Martin Corp. Space Systems Co. in Littleton, Colo., for costs related to the GPS IIIF satellites — including options to build as many as 22 GPS IIIF spacecraft in future years.



Lockheed Martin is designing the new generation of GPS navigation satellites with improved accuracy and reliability

The GPS IIIF satellites will be the most sophisticated spacecraft in the GPS constellation. The Air Force already is working with Lockheed Martin to build GPS III Block A satellites, the first of which is set for launch this December.

The GPS III satellites will replace aging on-orbit GPS spacecraft, and will improve satellite navigation accuracy, as well as GPS ability to resist attempts to jam their signals to degrade or disable the system's capability. The existing GPS satellite constellation has been operating in orbit since 1995.

This GPS IIIF contract to Lockheed Martin includes non-recurring engineering, space vehicle test bed and simulators, production of GPS IIIF satellites 11 and 12, options to build as many as 22 GPS III space vehicles, as well as satellite storage, launch, and on-orbit support.

The GPS-III satellites also will extend each satellite's design life and add a new civil signal that is interoperable with international global navigation satellite systems. Air Force leaders plan to buy as many as 32 GPS III satellites.

The GPS III program is part of a U.S. positioning, navigation, and timing (PNT) upgrade. The new GPS III constellation will have 500 times the transmission power of the existing GPS system, and will have faster clock update rates.

GPS Block IIIA will have the first 10 GPS III satellites, which will be used to keep the Navstar Global Positioning System operational. GPS IIIF, meanwhile, is the second set of GPS III satellites, and will have 22 space vehicles.

The GPS IIIA satellites will have a fourth civil signal on L1 channel, enhanced reliability, accuracy, and

A Reaper UAV shot down another drone last year in first known unmanned air-to-air kill

A U.S. Reaper unmanned aerial vehicle (UAV) shot down another drone with a missile, the Air Force revealed. The incident, which took place last year and involved an unmanned target drone, was the first case of a drone shooting down another aircraft. The event is a watershed moment in the history of aerial warfare, as the nation's UAV force begins to muscle in on air-to-air combat—previously the exclusive domain of manned aircraft. The test showed the U.S. Air Force that a UAV like the MQ-9 can conduct air-to-air combat, much like its manned fighter brethren such as an F-15 Eagle or F-22 Raptor, says Col. Julian Cheater, commander of the 432nd Wing at Creech Air Force Base, Nev. The effort is key to preparing for the next big aerial war against near-peer threats such as Russia or China, who are advancing their skills not only in their own drone forces but also in hypersonics, electronic warfare (EW), lasers, and missile testing, Cheater says.

Hypersonic missile intended for Russian SU-57 jet fighter has range of 200 miles

Russia is set to add a hypersonic missile to its arsenal which can hit targets almost 200 miles away, Moscow's official media outlet has reported. The R-37M missile is designed to target enemy aircraft and can travel at Mach 6 — more than 4,500 miles per hour. It is an upgrade on a Soviet-era weapon first launched in 1985. The latest missile, which will be fired from the planned Russian SU-57 stealth jets, is said to be equipped with an active-seeker homing system to blast enemy planes out of the sky. The new air-to-air missile is intended to target enemy fighter jets as well as Airborne Warning and Control System (AWACS) planes such as those deployed by the U.S. ←

integrity, no intentional signal degradation for national security (also called selective availability), and a 15-year life span. The GPS IIIF satellites will have all the GPS IIIA features, including laser reflectors and search-and-rescue payloads.

The enhanced reliability and anti-jam features of the GPS III satellites are expected to benefit U.S. and allied military forces, which increasingly rely on satellite-guided munitions, as well as civilian agencies and private business. U.S. and European aviation authorities have big plans to base future commercial aircraft navigation and guidance on signals from the GPS and other satellite-based positioning systems.

Future upgrades to GPS IIIF satellites could include cross-linking capabilities and spot beams to enable operators to boost the power of satellite signals so that the spacecraft can provide reliable service even in difficult or degraded conditions.

GPS IIIF satellites may receive upgrades with spacecraft numbers 1 to 6, more upgrades with satellites 7 to 12, upgrades in satellites 13 to 18, and additional upgrades in satellites 19 to 22.

The GPS III team is led by the Global Positioning Systems Directorate at the Air Force Space and Missile Systems Center. Lockheed Martin is the GPS III prime contractor with teammates Harris Corp. (formerly Exelis), General Dynamics, Infinity Systems Engineering, Honeywell, ATK, and other subcontractors.

Air Force Space Command's 2nd Space Operations Squadron (2SOPS), based at Schriever Air Force Base, Colo., manages and operates the GPS constellation for civil and military users. On this contract Lockheed Martin will do the work on GPS IIIF in Littleton, Colo., and should be finished by August 2027. ←

For more information contact ***Lockheed Martin Corp. Space Systems*** *online at* www.lockheedmartin.com, *or the* ***Air Force Space and Missile Systems Center*** *at* www.afspc.af.mil.

Northrop Grumman to provide components for MQ-4C maritime search radar

BY **John Keller**

PATUXENT RIVER NAS, Md. — Northrop Grumman Corp. will provide crucial electronic components for the U.S. Navy's maritime search radar aboard the MQ-4C Triton long-range ocean patrol unmanned aerial vehicle (UAV) under terms of a $64.8 million order.

Northrop Grumman will provide important components for the MQ-4C Triton's Multi-Function Active Sensor (MFAS) radar to keep the maritime patrol UAV in the air.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., are asking the Northrop Grumman Mission Systems segment in Linthicum Heights, Md., to provide components for the Triton UAV's Multi-Function Active Sensor (MFAS).

The MFAS is the Triton's maritime search radar that provides the UAV with a 360-degree view of a large geographic area while providing all-weather coverage for detecting, classifying, tracking, and identifying points of interest. MFAS is separate from the Triton's air-to-air radar.

The Triton performs maritime surveillance missions for as long as 24 hours at altitudes of more than 10 miles to enable coverage out to 2,000 nautical miles. The UAV's suite of sensors can detect and classify different types of ships automatically.

The Triton is a crucial component of the Navy's 21st century strategy for conducting surveillance of surface ship and submarine traffic in the vast Pacific and other oceans around the globe. The MQ-4C Triton UAV works together with the Navy's P-8A Poseidon manned maritime patrol aircraft.

Northrop Grumman will prove six antenna group assemblies, six wideband receivers and exciters, 10 radar signal processors (RSP), two antenna drive electronics, and two RSP external power supplies for the MFAS. This order supports low-rate initial production 3 organizational level maintenance for the Triton MFAS.

Along with the air-to-air and MFAS radar systems, the MQ-4C also will carry an electro-optical/infrared (EO/IR) sensor that will provide still imagery and full-motion video of potential threats; an electronic support measures package to identify and geolocate radar threat signals; and an Automatic Identification System (AIS) that will detect and track vessels equipped with AIS transponders.

The MQ-4C Triton is designed to provide combat information to military authorities like the expeditionary strike group, carrier strike group, and the joint forces maritime component commander. The Triton air vehicle is based on the U.S. Air Force RQ-4B Global Hawk, while its sensors are based on components and systems already fielded in the U.S. military.

The large unmanned aircraft provides intelligence for large ocean areas to maintain the common operational and tactical picture of the maritime battle space. The Triton feeds intelligence, surveillance, and reconnaissance (ISR) data to the Global Information Grid (GIG), and can work alone or together with other aircraft and surface ships.

The MQ-4C Triton's ability to perform persistent ISR within a practical range of 2,000 nautical miles enables the P-8A aircraft to focus on anti-surface ship warfare, anti-submarine warfare (ASW), and multi-intelligence. The Triton can fly as far as 8,200 nautical miles without refueling.

Triton aircraft and support facilities are being based domestically at Point Mugu Naval Air Station near Ventura, Calif., and at Jacksonville Naval Air Station, Fla. Triton UAVs also will be forward-deployed to Kadena Air Base, Japan; Andersen Air Force Base, Guam; Sigonella Naval Air Station, Italy; as well as at installations on the islands of Hawaii and Diego Garcia.

On this order Northrop Grumman will do the work in Linthicum, Baltimore, Annapolis, and Hampstead, Md.; Andover, Mass.; Exeter, N.H.; San Diego; and Stafford Springs, Conn.; as well as other locations inside and outside of the Continental U.S., and should be finished by June 2022. ←

For more information contact ***Northrop Grumman Mission Systems*** *online at* www.northropgrumman.com, *or* ***Naval Air Systems Command*** *at* www.navair.navy.mil.

Thermal imaging used in Planet Earth II could be used by British Army tanks

In the BBC's Planet Earth II nature documentary series, David Attenborough's team used advanced thermal imaging cameras developed by aerospace company Leonardo to track a pack of leopards hunting in the darkened streets of Mumbai. Now, that exact same technology could be built into the British Army's main battle tank. BAE Systems is bidding for a contract to upgrade the Challenger II battle tanks, and Leonardo's advanced night vision tech is a key part of its plan. Instead of detecting light, Leonardo's cameras sense heat emitted by all objects with a temperature above absolute zero (-273C). Each pixel in the sensor is 1/12 the thickness of a human hair, and can detect changes as small as 1/50 of a centigrade, producing extremely sharp images. Leonardo's electro-optical thermal imaging technology has found a wealth of uses – both military and civilian. In addition to other nature programs, including Autumnwatch and The Great British Year, it's proved valuable in international sports. During the Ashes Test Series in Australia, it was used to determine whether the ball had struck the batsman, bat, or pads by detecting the friction of impact.

Next-gen electro-optical tracking sensor could help avoid friendly fire target accidents

There may soon be a new infrared detection sensor on the market that can better scrutinize friendly forces on the ground and shrink the time it takes to identify targets of opportunity. UTC Aerospace Systems in Westford, Mass., is testing

Northrop Grumman to provide LAIRCM laser-based missile-defense for large aircraft

BY **John Keller**

PATUXENT RIVER NAS, Md. — Missile-defense experts at Northrop Grumman Corp. will install laser-based missile-defense systems for large military aircraft under terms of a $210.5 million U.S. Navy order.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., are asking engineers at the Northrop Grumman Mission Systems segment in Rolling Meadows, Ill., to provide the electro-optical Large Aircraft Infrared Counter Measures (LAIRCM) for a variety of U.S. military aircraft.

Northrop Grumman is providing the U.S. Navy with the electro-optical Large Aircraft Infrared Counter Measures (LAIRCM) for large military aircraft like the P-8A Poseidon, shown above.

LAIRCM automatically detects a missile launch, determines if it is a threat, and activates a high-intensity laser-based countermeasure system to track and defeat the missile, Northrop Grumman officials say.

This order covers LAIRCM production for the U.S. Navy, Air Force, Army, Special Operations Command, and government of the United Kingdom.

The system is for large aircraft like the U.S. Navy P-8A Poseidon maritime patrol jet and the Marine Corps CH-53 Super Stallion large helicopter. LAIRCM also can go aboard the U.S. Air Force C-5, C-17, C-37, and C-40 cargo and utility jets; C-130H and MC-130W four-engine utility turboprop aircraft, the CV-22 tiltrotor aircraft, and the KC-46 aerial refueling jet.

The order involves 466 advanced threat warning sensors; 15 LAIRCM signal processor replacements; 30 control indicator units; 62 replaceable control indicator units; 114 to 2,103 signal processors; 161 infrared missile warning sensors; 245 Guardian laser transmitter assemblies; 20 multi-role electro-optical end-to-end test sets; 125 shipping containers; 56 high-capacity cards; 16 smart connector assemblies; 381 personal computer memory cards; international association cards; and 11 battery kits.

LAIRCM focuses its high-intensity laser energy at the infrared seeker head of incoming missiles to blind the missile and force it off its target. The system is designed to protect large aircraft from shoulder-fired, vehicle-launched, and other infrared-guided missiles when the planes are operating close to the ground, such as during takeoffs, landings, and low-level operations like aerial refueling.

Initial LAIRCM systems equipped C-17 and C-130 aircraft as a stop-gap measure, using an ultraviolet sensor, a countermeasure processor, and a small laser turret assembly.

Later-model LAIRCM systems use a smaller laser turret, and operate in the infrared region. Compared to first-phase LAIRCM systems, the newer models provide better resolution,

better performance in optical clutter, and increased range of detection.

In the future military leaders are trying to develop aircraft-protection infrared countermeasures able to detect and classify incoming missiles, then emit a custom jamming energy to defeat them.

On this order Northrop Grumman will do the work in Rolling Meadows, Ill.; Goleta, Calif.; Longmont, Colo.; Columbia, Md.; and at various locations within and outside of the continental U.S., and should be finished by October 2020. ←

For more information contact ***Northrop Grumman Mission Systems*** *online at* www.northropgrumman.com*, or* ***Naval Air Systems Command*** *at* www.navair.navy.mil.

Army surveys industry for persistent surveillance multispectral sensor

BY **John Keller**

FORT BELVOIR, Va. — U.S. Army electro-optics researchers are surveying industry to find companies able to design a multispectral sensor from existing products for persistent surveillance to identify walking humans and vehicles at mid- to long ranges.

Officials of the Army Contracting Command at Aberdeen Proving Ground, Md., have issued a sources-sought notice (W909MY-19-R-E001) for the EO/IR Sensor Characterization for Persistent Surveillance System–Ground (PSS-G) component of the Army's Ground-Based Operational Surveillance System (Expeditionary) (G-BOSS(E)) project.

Army researchers want to find companies able to design a gimbal-mounted integrated electro-optical sensor payload that blends mid-wave and short-wave infrared sensors, laser range finder, and laser pointer.

The Army Contracting Command is issuing the sources-sought notice on behalf of the Product Management Force Protection Systems segment of the Army Night Vision and Electronic Sensors Directorate (NVESD) at Fort Belvoir, Va., for this electro-optical sensor project.

Army researchers are looking for companies able to design a multispectral sensor able to identify walking humans and vehicles at mid- to long ranges.

From industry, the Army wants to the know the maximum range of each sensor in the integrated electro-optical sensor payload at a standard atmosphere in which a human and vehicle can be identified with 90-percent probability.

Researchers also want to know about the zoom field of view of each persistent surveillance *[PAGE 38]*

a next-generation short-wave infrared (SWIR) camera sensor that can see laser strobes in real time. The electro-optical system — already deployed with U.S. military testing units — is a multi-mode tracking SWIR sensor. The company developed the sensor to prevent fratricide, reduce talk on target, and promote covert communications. UTC's multi-mode tracking sensor can pick up designators as well as markers from friendly forces. The more platforms equipped with the sensor — from tanks, to fixed-wing aircraft, helicopters, and even ships — the more streamlined target identification becomes.

Raytheon delivers first of SeeMe small satellites for launch this year from SpaceX rocket

Raytheon delivered the first Space Enabled Effects for Military Engagements (SeeMe), satellite to the U.S. Defense Advanced Research Projects Agency (DARPA). Assembled on the company's missile production lines, the new SeeMe satellite aims to provide greater situational awareness to soldiers on the ground. DARPA's SeeMe program is designed to show that small satellites can be built affordably to give small squads timely tactical imagery directly from a small satellite. A future constellation of small satellites could deliver high-resolution images of precise locations of interest to the soldier's handheld device. Using its automated missile production lines, Raytheon can build large numbers of these small satellites quickly and affordably. DARPA will integrate the Raytheon-built SeeMe satellite onto a Spaceflight Industries payload that will be launched into Low Earth Orbit (LEO) on a SpaceX rocket later this year. ←

L-3 EO Sonoma to integrate large-area UAV sensor payloads for small platforms

BY **John Keller**

STENNIS SPACE CENTER, Miss. — Electro-optical sensors experts at the L-3 Technologies Sonoma EO segment in Santa Rosa, Calif., are developing high-resolution day and nighttime sensor payloads for small unmanned aerial vehicles (UAVs) under terms of a U.S. Navy research contract.

Officials of the U.S. Naval Research Laboratory (NRL) at Stennis Space Center, Miss., are asking L-3 EO Sonoma to build and test a large-area airborne sensor that can operate even from hand-launched UAVs. It's part of NRL's Tactical Infrared Night Surveillance System (TNWAS) project.

L-3 EO Sonoma engineers will develop a UAV sensor payload able to conduct precise, large-area, high-resolution day and nighttime surveillance of large areas in a configuration meeting the extremely tight size, weight, and power constraints of the Navy and U.S. Marine Corps Small Tactical Unmanned Air System (STUAS) aircraft. The contract is for $930,110.

STUAS aircraft include the 2.8-pound AeroVironment RQ-12A Wasp IV; the 4.7-pound AeroVironment RQ-11B Raven; the 13.5-pound AeroVironment RQ-20B Puma; the 48-pound Boeing Insitu ScanEagle; the 75-pound Textron AAI Aerosonde; and the 135-pound Boeing Insitu RQ-21A Blackjack.

NRL already has sponsored development of the TNWAS infrared sensor, which is designed to operate together with an NRL-developed video processor to comprise the TNWAS airborne surveillance system, which went through ground testing last December.

The TNWAS infrared sensor integrates components like the optics and pointing mirror assembly from the Office of Naval Research (ONR) UltraWide Optics program; and the integrated Dewar cooler assembly (IDCA) from the ONR 8K Focal Plane Array program.

Now L-3 EO Sonoma experts will find ways to stabilize the sensor's sight line against effects of UAV motion and vibration; provide precise measurement of sight line direction to support geolocation of ground objects; and integrate the sensor with the NRL video processor. Then company experts will demonstrate the integrated system in truck-based and airborne tests.

The contract's first phase focuses on collecting high-quality imagery and determining sight line pointing direction in a mobile ground environment.

L-3 EO Sonoma is developing wide-area electro-optical sensor payloads suitable for even hand-launched unmanned aircraft.

This involves completing the L-3-developed TNWAS sensor controller computer to communicate with the NRL payload system computer.

If these tests satisfy Navy requirements, then L-3 EO Sonoma engineers will integrated the sensor system aboard a remotely operated aircraft that functions vial data links. ←

For more information contact ***L-3 EO Sonoma*** *online at* www2.l3t.com/sonomaeo, *or the* ***Naval Research Lab at Stennis Space Center*** *at* www.nrl.navy.mil/field-sites/stennis.

[FROM PAGE 37] sensor; imagery and video standards to which the sensor conforms; integrated sensor packaging; whether it has an active illuminator; cooling methods; spectral ranges; hardware control and data interfaces; system size and weight; levels of ruggedization; cyber security standards; built-in test; and reliability, availability, and maintainability.

A multispectral sensor captures image data in 3 to 15 separate wavelengths to extract information the human eye fails to capture with its receptors for red, green and blue. It usually provides a combination of imaging in the visible-light, near infrared, short-wave infrared, mid-wave infrared, and long-wave infrared spectral bands into one image.

The military typically uses multispectral sensors for target tracking, land mine detection, ballistic missile detection, and space-based imaging.

Companies interested were asked to email responses no later than 16 Oct 2018 to the Army's Crystal Pressley, contract specialist, at crystal.d.pressley.civ@mail.mil. For questions or concerns contact Crystal Pressley by email at crystal.d.pressley.civ@mail.mil, or by phone at 703-704-0860. ←

More information is online at https://www.fbo.gov/notices/938d0006915990c918b9da7e-46c2b8ca.

PRODUCT applications

UNMANNED VEHICLES

AeroVironment to build small UAVs with surveillance unmanned sensor payloads

U.S. Southern Command warfighters needed small hand-launched unmanned aerial vehicles (UAVs) for a variety of reconnaissance and intelligence missions. They found their solution from AeroVironment Inc. Monrovia, Calif.

Officials of the U.S. Air Force Acquisition Management and Integration Center at Joint Base Langley-Eustis, Va., have announced a $13 million contract to AeroVironment for Raven RQ-11B small unmanned aircraft systems.

These unmanned systems are for the U.S. Southern Command Area of Responsibility, which includes Central America, South America and Caribbean nations. The contract includes UAVs, spares kits, ancillary equipment, and recurring training.

The RQ-11B Raven small hand-launched UAV is designed for rapid deployment and high mobility for military applications requiring low-altitude surveillance and reconnaissance.

It can be operated manually or programmed for autonomous operation, using the system's advanced avionics and GPS navigation to provide aerial observation, day or night, at line-of-sight ranges to six miles.

The Raven is available with an optional stabilized gimbaled payload, and delivers real-time color or infrared imagery to ground control and remote viewing stations. The Raven is the most widely used unmanned aircraft system in the world today, AeroVironment officials say.

Raven unmanned sensor payloads include dual forward- and side-look electro-optical camera nose, electronic pan, tilt, and zoom with stabilization, forward and side-look infrared camera nose.

The UAV has a maximum range of 6.2 miles, mission duration of 60 to 90 minutes, operates at speeds of 17 to 44 knots at altitudes of 100 to 500 feet. The unmanned aircraft is 3 feet long, has a wingspan of 4.5 feet, and weighs 4.2 pounds. It is hand-launched and has a deep-stall landing.

On this contract AeroVironment will do the work in the U.S. Southern Command Area of Responsibility, and should be finished by September 2028. For more information contact **AeroVironment** online at *www.avinc.com*, or the **Air Force Acquisition Management and Integration Center** at *www.facebook.com/AirForceAMIC*.

WEAPONS SIGHTS

Navy picks Nightforce Optics daylight rifle sights for U.S. Special Operations

U.S. Navy special operations experts are asking electro-optics engineers at Nightforce Optics Inc. in Orofino, Idaho, to provide U.S. Special Operations Command with rifle scopes for near-range engagements out to and beyond the maximum effective range of the weapons.

Officials of the Naval Surface Warfare Center in Crane, Ind., are awarding a potential $21.2 million contract to Nightforce to build Squad-Variable Powered Scopes (S-VPS) in support of U.S. Special Operations Command. The initial

contract is for $15.8 million, and includes the S-VPS, spare parts, and training.

The S-VPS is the Nightforce ATACR 1-8X24 F1 low-power electro-optical variable rifle scope that includes ED glass, daylight illumination, an intelligent reticle, low-profile adjustments, and a field of view at 1x equivalent to open sights, yet more precise, company officials say.

The rifle sight is slightly longer than 10 inches, and weighs 21 ounces. Its daylight visible center red dot allows for rapid engagements.

The sight provides as much as 8x zoom to help locate, identify, and engage targets at the maximum effective range of most rifles. Its intelligent FC-DM first focal plane reticle provides precise hold and hold-off points.

The rifle sight low-profile turrets are capped to prevent accidental adjustment and offer 0.1 mil-radian adjustment. The sight has an

integrated power throw lever to aid in fast magnification adjustments.

On this contract Nightforce will do the work in Orofino, Idaho, and should be finished by September 2023. For more information contact **Nightforce** online at *www.nightforce-optics.com*, or the **Naval Surface Warfare Center-Crane** at *www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Crane.*

EMBEDDED COMPUTING

WOLF video graphics modules help design windowless supersonic aircraft cockpit

Supersonic aircraft designers at the U.S. National Aeronautics and Space Administration (NASA) needed rugged video graphics embedded computing modules to help develop the NASA X-59 Quiet SuperSonic Technology (QueSST) aircraft. They found their solution from WOLF Advanced Technology in Whitchurch-Stouffville, Ontario.

Researchers at the NASA Armstrong Research Center at Edwards Air Force Base, Calif., have chosen two WOLF video graphics modules to provide video capture, processing, encoding, and dis-

play capabilities to help enable NASA's windowless cockpit display system. The X-59 is designed to reduce sonic boom noise.

NASA experts are using the WOLF XMC-E9171-VO (WOLF-3196) and the XMC-FGX2-SDI-8IO (WOLF-3180), video graphics modules in the QueSST initiative to replace a front windshield with video display technology.

The XMC-E9171-VO features an AMD Radeon graphics processing unit (GPU), a chip-down rugged design that meets the MIL-810 specification, can handle as many as five 4K displays using Display Port 1.4, and supports high dynamic range video with 10-bit color depth.

The XMC-FGX2-SDI-8IO is WOLF's second-generation Frame Grabber eXtreme (FGX). The embedded computing module enables as many as eight 3G/HD-SDI or four 12G-SDI inputs and outputs; two analog inputs and outputs; a PCI Express Gen4 interface that can handle data as fast as 15.75 gigabytes per second; ultra-low-latency H.265 encoding; and support for direct user access to FPGA HDL logic for encryption, analysis, and image recognition. A 10-Gigabit Ethernet LAN interface is also supported.

"The X-59 QueSST aircraft will represent a step forward in supersonic aircraft flight, and the products we've chosen from WOLF will help us deliver the visual data our pilots require to meet our mission criteria," says Trey Arthur, aerospace engineer at NASA. For more information contact **WOLF Advanced Technology** online at *https://wolfadvancedtechnology.com*, or the **NASA Armstrong Research Center** at *www.nasa.gov/centers/armstrong.*

LASER EYE PROTECTION

Air Force orders pilot eye protection from military and civil laser attacks

U.S. Air Force flight safety experts needed laser eye protection for aircraft pilots and air crews against dazzling and blinding laser weapons. They found their solution from Gentex Corp. in Carbondale, Pa., and Teledyne Scientific & Imaging LLC in Thousand Oaks, Calif.

Officials of the Air Force Life Cycle Management Center at Wright-Patterson Air Force Base, Ohio, announced contracts each worth as much as $98.3 million to the two companies for laser eye protection.

Gentex and Teledyne Scientific will develop and build different variants and sizes of laser eye protection to safeguard air crews against emerging laser attacks like laser dazzlers and lasers intended to blind or cause permanent eye injury.

Military, commercial, and general-aviation aircraft pilots in recent years have come under increasing threats from ground-based lasers, ranging from common laser pointers to sophisticated laser dazzlers from hostile military forces.

Sometimes these lasers cause temporary blindness and disorientation — particularly at night — when the eyesight of air crews has adjusted to darkness. Other cases can cause permanent blindness or eye injury, depending on the type and strength of the laser.

Several recent examples attest to the laser threats that military and civil aircraft pilots face. Earlier this spring U.S. military officials reported that personnel at a Chinese military base in Djibouti in Eastern Africa used lasers to interfere with U.S. military aircraft at a nearby American base, causing injuries to U.S. pilots and prompting the U.S. to launch a formal diplomatic protest.

Last June U.S. officials reported that U.S. military pilots flying over the East China Sea had been targeted by blinding laser attacks from shore sites and from fishing boats more than 20 times over the previous 10 months.

In fact, the number of laser attacks on U.S. pilots in the Middle East and South China Sea areas could top the roughly 600 incidents reported in 2016 and match 2015, when about 700 incidents were reported in the Middle East, officials say.

Gentex makes the dazzle laser defense visor for mounting to flight helmets to protect civil and military pilots from a variety of laser attacks. These visors are designed to protect pilots from low-intensity lasers without compromising visual acuity.

Teledyne Scientific, meanwhile, makes the aircrew laser eye protection (ALEP) devices, of which more than 10,000 have been delivered to the Air Force, company officials say.

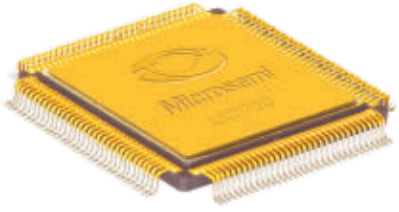
On these contracts, Gentex will do the work in Simpson, Pa.; and Teledyne Scientific will to the work in Thousand Oaks, Calif. Both companies should be finished by September 2024.

For more information contact Gentex Corp. online at *https://gentexcorp.com*, **Teledyne Scientific & Imaging** at *www.teledyne-si.com*, or the **Air Force Life Cycle Management Center** at *www.wpafb.af.mil/aflcmc.* ←

SPACE ELECTRONICS

Radiation-tolerant motor controller for space introduced by Microsemi

Microsemi Corp. in Aliso Viejo, Calif., is introducing production prototypes of the LX7720 radiation-tolerant motor controller for satellite manufacturers sensitive to area and weight challenges. The LX7720 radiation-tolerant motor controller



can help reduce weight and board space relative to conventional discrete motor control circuits. As the second member of the SSM family, the LX7720 works with a field programmable gate array (FPGA) and complements Microsemi's other components for demanding space applications. Additional target applications include motor driver servo control, linear actuator servo control and driving stepper, brushless direct current (BLDC), and permanent-magnet synchronous (PMSM) motors on satellite buses for solar panel deployment and driving reaction wheels. For more information contact **Microsemi** online at *www.microsemi.com*.

GPGPU PROCESSING

GPGPU XMC embedded computing modules for harsh environments introduced by EIZO

EIZO Rugged Solutions Inc. in Altamonte Springs, Fla., is introducing a family of chip-down NVIDIA Quadro P2000 (GP107) based switched mezzanine card (XMC) graphics/GPGPU embedded computing cards for harsh environments in military and avionics applications. The MIL-STD-810G-certified Condor NVP2000x modules are based on general-purpose graphics-processing units (GPGPU), and bring the CUDA software-development platform to small package XMCs to deliver 2.3 trillion floating point operations per second (teraFLOPs) of processing power. EIZO's XMC cards feature H.265/H.264 hardware encode/decode capability and provide a minimum 7-year life cycle support to customers. The boards can be factory configured to a power rating between 25 and 50 Watts. While the current variants feature DisplayPort++, EIZO also can customize cards to support DVI, SDI, Composite, STANAG 3350, RS-170, RS-343, and VGA outputs. For more information contact **EIZO Rugged Solutions** online at *www.eizorugged.com*.

GPGPU EMBEDDED COMPUTING

GPGPU embedded computing for video and machine autonomy introduced by Aitech

Aitech Defense Systems Inc. in Chatsworth, Calif., is introducing the A177 Twister ultra-compact rugged embedded computing system based on general-purpose graphics processing unit (GPGPU) technology for video capture, processing, and overlay uses in industrial environments. The compact supercomputer is for autonomous aircraft, military ground vehicles, robotics, automation, and optical inspection systems. Based on the powerful NVIDIA Jetson TX2 system-on-module (SoM), the A177 Twister uses the CUDA programming language and deep learning acceleration to handle managing several data and video streams. The small

form factor (SFF) supercomputer has 256 CUDA cores to reach more than 1 trillion floating point operations per second (teraFLOPS). It consumes 17 Watts of power, weighs less than 2.2 pounds, and measures 5.9 by 5.8 by 2.5 inches. The embedded computing system is designed to bring local processing in closer with a system's sensors. Its IP67-rated and fanless design also is for rugged and remote outdoor applications like security and surveillance systems, mining and excavating operations, and complex marine and boating applications like weather condition analysis and navigation. For more information contact **Aitech** online at *www.rugged.com*.

SIGNAL PROCESSING

RF system-on-chip (RFSoC) for signal processing introduced by Pentek

Pentek Inc. in Upper Saddle River, N.J., is introducing the Quartz model 5950 Zynq UltraScale+ radio frequency system-on-chip (RFSoC) 3U VPX board and the model 6001 Zynq UltraScale+ QuartzXM eXpress module for aerospace and defense applications. The Quartz model 5950 Zynq UltraScale+ RFSoC 3U VPX board and the model 6001 Zynq UltraScale+ QuartzXM eXpress module support wideband RF analog I/O signals

STATEMENT OF OWNERSHIP, MANAGEMENT, AND CIRCULATION

1. Publication title: Military & Aerospace Electronics. **2. Publication number:** 005-901 **3. Filing date:** October 1, 2018. **4. Issue frequency:** Monthly. **5. Number of issues published annually:** 12. **6. Annual subscription price:** $185.00. **7. Complete mailing address of known office of publication:** PennWell Corporation, 1421 South Sheridan Rd., Tulsa, OK 74112, Tulsa County. **7a. Contact person:** Traci Huntsman. **7b. Telephone:** 918-831-9435. **8. Complete mailing address of headquarters or general business office of publisher:** PennWell Corporation, 61 Spit Brook Rd., Ste. 501, Nashua, NH 03060. **9. Full names and complete mailing addresses of Publisher, Editor and Managing Editor:** Publisher: Alan Bergstein, 61 Spit Brook Rd., Ste. 501, Nashua, NH 03060. Editor: John Keller, 61 Spit Brook Rd., Ste. 501, Nashua, NH 03060. Managing Editor: John Keller, 61 Spit Brook Rd., Ste. 501, Nashua, NH 03060. **10. Owner:** PennWell Corporation, 1421 South Sheridan Rd., Tulsa, OK 74112, Tulsa County. **11. Known Bondholders, Mortgages, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities:** None. **12.** N/A. **13. Publication Title:** Military & Aerospace Electronics. **14. Issue Date for Circulation Data:** September 2018. **15. Extent and Nature of Circulation:**

	Average No. copies each issue during preceding 12 months:	No. copies of single issue published nearest to filing date:
a. Total number of copies	22,292	23,015
b. Legitimate paid and/or requested distribution		
1. Outside county paid/requested mail subscriptions stated on PS form 3541	19,291	19,983
2. In-county paid/requested mail subscriptions stated on PS form 3541	0	0
3. Sales through dealers and carriers, street vendors, counter sales, and other paid or requested distribution outside USPS®	107	118
4. Requested copies distributed by other mail classes through the USPS®	0	0
c. Total paid and/or requested circulation	19,398	20,101
d. Non-requested distribution		
1. Outside county nonrequested copies stated on PS form 3541	1,217	1,221
2. In-county nonrequested copies stated on PS form 3541	0	0
3. Nonreqeusted copies distributed through the USPS by other classes of mail	0	0
4. Nonrequested copies distributed outside the mail	201	205
e. Total nonrequested distribution	1,418	1,426
f. Total Distribution	20,816	21,527
g. Copies not Distributed	1,476	1,488
h. Total	22,292	23,015
i. Percent paid and/or requested circulation	93.19%	93.38%
16. Electronic Copy Circulation		
a. Requested and Paid Electronic Copies	16,145	15,069
b. Total requested and paid print copies + requested/paid electronic copies	35,543	35,170
c. Total requested copy distribution + requested/paid electronic copies	36,961	36,596
d. Percent paid and/or requested circulation	96.16%	96.10%

☑ I certify that 50% of all my distributed copies (electronic and print) are legitimate requests or paid copies.

17. Publication of Statement of Ownership: Will be printed in the November 2018 issue of this publication.

18. Signature and title of Editor, Publisher, Business Manager, or Owner: Traci Huntsman, Manager Corporate Assets and Postal Compliance. **Date:** 10/01/2018.

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

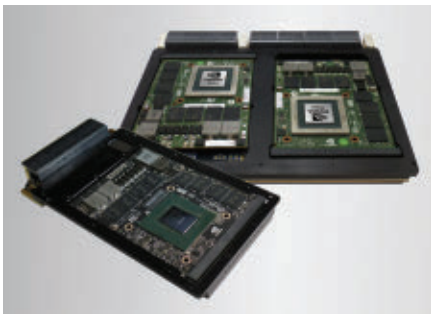
with eight 4 GHz A/D converters, eight 6.4 GHz D/A converters, and multi-core ARM processors. For 3U VPX systems, the Quartz model 5950 uses Pentek's Navigator design suite to speed software and IP development. For small- or high-density deployed systems, the same IP and software can transfer to the model 6001 QuartzXM eXpress embedded computing module to support applications that require custom-form-factors and small size, weight, and power consumption (SWaP). The Pentek Quartz architecture embodies a streamlined approach to field-programmable gate array (FPGA) boards, simplifying the design to reduce power and cost, while still providing high-performance FPGA resources. For more information contact **Pentek** online at *www.pentek.com*.

EMBEDDED COMPUTING

VPX boards for radar and electronic warfare introduced by Curtiss-Wright

The Curtiss-Wright Corp. Defense Solutions division in Ashburn, Va., is introducing the rugged VPX3-4924 and VPX6-4944 open-architecture high performance embedded computing (HPEC) processors for use in compute intensive intelligence, surveillance, and reconnaissance (ISR) and electronic warfare (EW) systems. The NVIDIA Tesla Pascal. (P6) 16-nanometer general-purpose graphics processing unit (GPGPU)-based OpenVPX modules are for sensor fusion or large swath video mapping, that require teraFLOPs of accelerated processing. With their on-device support for NVIDIA high-performance compute (HPC) mode, these high-performance embedded computing (HPEC) engines can ingest data generated by modern radar, SIGINT, and EO/IR sensors.

The VPX3-4924 module, a 3U OpenVPX

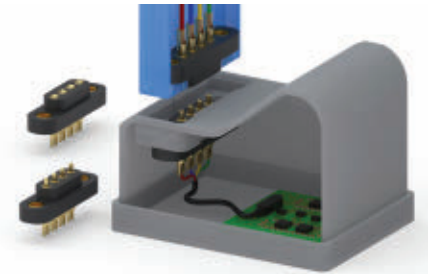


GPGPU Processor, features one Tesla P6 GPU and delivers 6.2 teraFLOPs performance. For more demanding signal processing applications, the 6U form factor VPX6-4944 deploys dual Tesla P6s, doubling available compute power to 12.4 teraFLOPs. For more information contact **Curtiss-Wright Defense Solutions** online at *www.curtisswrightds.com*.

BOARD CONNECTORS

Rugged connector for cable terminations and quick connects introduced by Mill-Max

Mill-Max Manufacturing Co. in Oyster Bay, N.Y., is introducing the 868-series rugged 4-millimeter-pitch connector with wire termination spring-loaded and target connectors for mounting into product housings for docking stations, cable terminations, heavy-duty quick connects, and panel mount equipment. The 868 connectors include solder-cups to accommodate wire



and cable attachment along with flanged insulators and fastening options. They are for wire termination, with uniformly aligned solder-cup pins to facilitate efficient soldering of wires as thick as 16 AWG. The 868-22-00X-00-0X1101 spring-loaded connectors have heavy-duty spring pins with 0.05-inch-diameter plungers that resist bending and binding during the application of side loads. The gold-plated stainless-steel spring on the connector ensures reliable operation to 1 million cycles and is less prone to stress relaxation when operating at high temperatures over time (to 260 degrees Celsius for one hour, to 180 C for 24 hours). For more information contact **Mill-Max** online at *www.mill-max.com/PR688*.

RF AND MICROWAVE

Flexible RF and microwave waveguides for antennas introduced by Pasternack

Pasternack Enterprises Inc. in Irvine, Calif., is introducing a line of twistable and seamless flexible RF and microwave waveguides for DAS systems, base stations, antennas, and test instrumentation. The waveguides operate in the 5.85-to-50-GHz frequency range and cover 10 frequency bands from WR-137 to WR-22. These flexible waveguides have 78 total models — 39 seamless and 39 twistable. All models operate in the same RF and microwave frequency range, are available in lengths of 6 to 36 inches and with UG-style square/round cover and CPR-style flanges. The twistable models can twist in different directions using wound twist flex material. Interlocking brass enables it to slide on itself. These flexible waveguides provide voltage standing wave ratio (VSWR) as low as 1.05:1, insertion loss as low as 0.15 decibels, and max power as high as 1.5 kilowatts. For more information contact **Pasternack** online at *www.pasternack.com.*

ADVERTISERS INDEX

Military & Aerospace Electronics

SUBSCRIPTION INQUIRIES
Phone: 1-800-869-6882 / International Callers: +1 512-982-4277
E-mail: MAEM@kmpsgroup.com
Web: www.mae-subscribe.com

GROUP PUBLISHER Alan Bergstein
603 891-9447 / alanb@pennwell.com

EDITOR-IN-CHIEF John Keller
603 891-9117 / jkeller@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 Debbie Bouley
603 891-9372 / debbieb@pennwell.com

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

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

PennWell
www.pennwell.com

EDITORIAL OFFICES
PennWell Corporation,
Military & Aerospace Electronics
61 Spit Brook Road, Suite 501, Nashua, NH 03060
603 891-0123 / 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
Kaci Wheeler
918 832-9377 / kaciw@pennwell.com

CORPORATE OFFICERS
PRESIDENT AND CHIEF EXECUTIVE OFFICER Mark C. Wilmoth

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

CHIEF OPERATIONS OFFICER, PENNWELL MEDIA Robert Brighouse

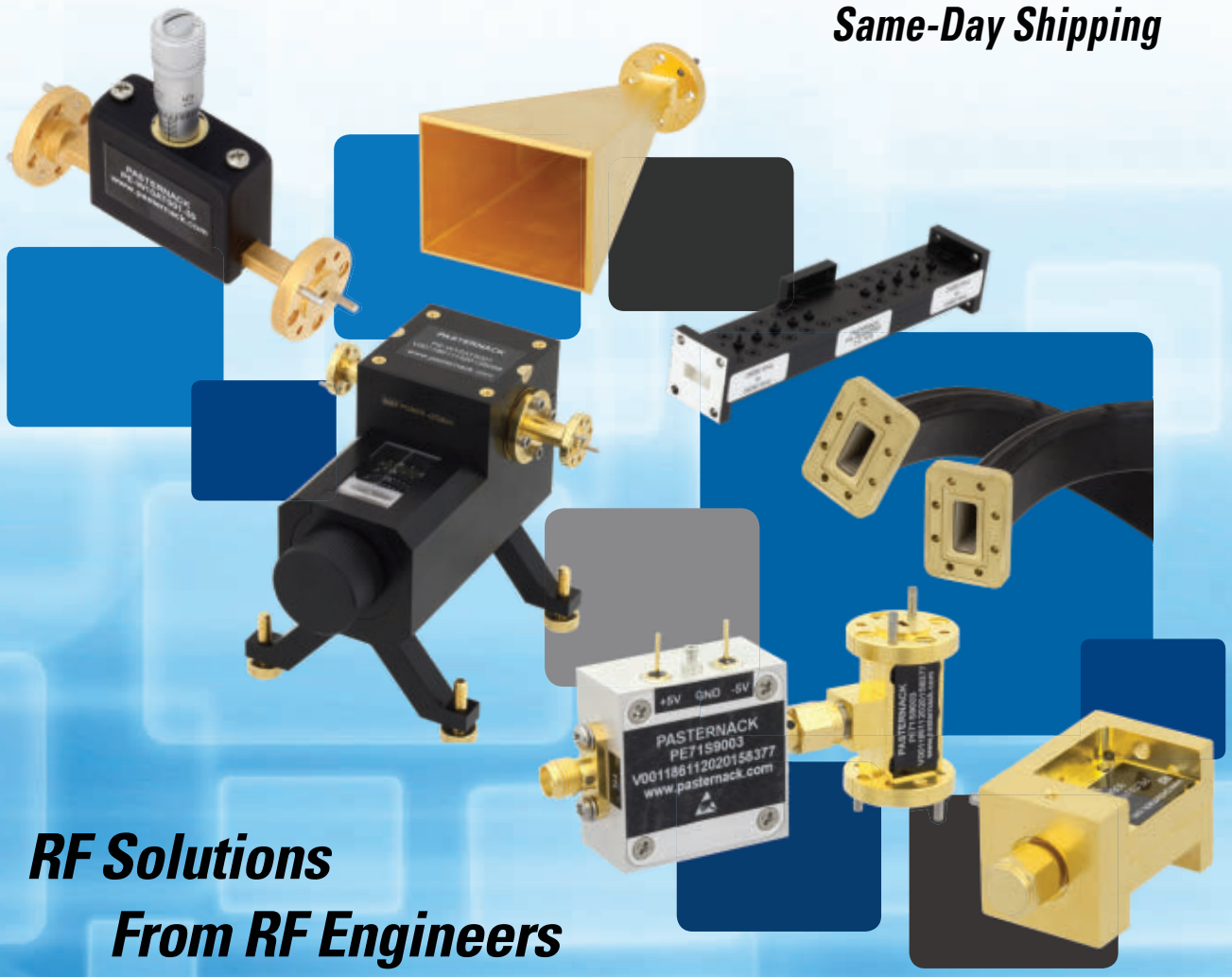
TECHNOLOGY GROUP
SENIOR VICE PRESIDENT/PUBLISHING DIRECTOR & CMO June Griffin

BPA WORLDWIDE Connectiv

Largest In-Stock Selection of

Waveguide Components

All Available for Same-Day Shipping



RF Solutions From RF Engineers

Pasternack's RF Engineering team has assembled the largest selection of in-stock and ready to ship waveguide components covering RF, microwave and millimeter-wave bands up to 110 GHz. With 20 different waveguide categories and over 500 designs including adapters, power amplifiers, detectors, bandpass filters, PIN diode switches, attenuators, horn antennas and more, Pasternack has the waveguide components you are looking for. Whether it's waveguide products or any of the other 40,000 in-stock components we carry, our Application Engineers stand ready to deliver solutions for all your RF project needs.

866.727.8376
visit pasternack.com today!

PASTERNACK®
THE ENGINEER'S RF SOURCE

We didn't break the mold.
We shattered it.

RFSoC | Unparalleled Performance | Unbelievably Fast Integration

The combination of Pentek's new Quartz™ architecture, and the processing power packed into the new Zynq® UltraScale+™ RFSoC FPGA, smashes the boundaries of high-performance embedded computing.

Pre-loaded with a host of IP modules, this OpenVPX board is ready for out-of-the-box integration into high-performance systems. Optical streaming interfaces, a unique modular design and the Navigator™ development platform means fast, high-speed deployment.

- **Powerful Zynq Ultrascale+ FPGA** with built-in wideband A/Ds, D/As & ARM processors
- **Dual Optical 100 GigE** interfaces for extreme system connectivity
- **Robust Factory-installed IP** for DRFM,radar range gate engine, waveform and chirp generation, real-time data acquisition and more
- **QuartzXM™ eXpress Module** speeds migration to other form factors
- **Board Resources** include PCIe Gen.3 x8 and 18 GB DDR4 SDRAM
- **Navigator Design Suite** BSP and FPGA design kit for seamless integration with Xilinx Vivado®

All this plus FREE lifetime applications support!

Model 5950
Eight-Channel A/D & D/A RFSoC in 3U VPX Conduction Cooled

QUARTZ

NAVIGATOR Design Suite

Unleash the Power of the RFSoC. Download the FREE White Paper!
https:/www.pentek.com/go/marfsoc

PENTEK
Setting the Standard for Digital Signal Processing

Pentek, Inc., One Park Way, Upper Saddle River, NJ 07458
Phone: 201-818-5900 • Fax: 201-818-5904 • email: info@pentek.com • www.pentek.com

30 YEARS