Next Generation Space Defense

MILSATMAGAZINE

May 2023

Cover image is courtesy of SES Space & Defense

Publishing Operations

Silvano Payne
Publisher + Executive Writer

Simon Payne
Chief Technical Officer

Hartley G. Lesser
Editorial Director

Pattie Lesser
Executive Editor

Donald McGee
Production Manager

Teresa Sanderson
Operations Director

Sean Payne
Business Development Manager

Dan Makinster
Technical Advisor

Chris Forrester
Senior Columnist

Karl Fuchs
Senior Contributor, iDirect Government

Authors

Michael Clonts

Karl Fuchs

Rick Lober

David Pesgraves

Lisa Sodders

Dispatches

Features

Advertisers

MilsatMagazine is published 11 times per year by SatNews Publishers, 800 Siesta Way, Sonoma, California - 94576 - USA — Phone: (707) 939-9306 / Fax: (707) 939-9235

RESILIENT & SECURE END-TO-END **COMMAND THE ADVANTAGE**

When U.S. Defense and Federal agencies need resilient and secure end-to-end communications for maritime, airborne, and ground-mobility operations anywhere in the world, they put their trust in SES Space & Defense. As an industry leader for over 40 years, SES Space & Defense supports the most demanding U.S. Government customer requirements with fully integrated Information & Communications Technology Solutions that leverage state-of-the-art multi-band, multi-orbit satellite services. Our unwavering commitment to ensuring resiliency and security in global communications makes SES Space & Defense the only choice when success is critical - **command the advantage.**

SES SPACE & DEFENSE

www.sessd.com

DISPATCHES

AeroVironment introduces VTOL kit for Puma AE UAS

AeroVironment, Inc. has introduced the Puma™ VTOL** (vertical take-off and landing) **kit, designed for plug-and-play integration into Puma 2 AE and Puma 3 AE small unmanned aircraft systems (SUAS).

The optional Puma VTOL kit expands the operational capabilities of the combat-proven Puma system in complex terrain, as neither runway nor large open space are required for launch and recovery of the VTOL-equipped Puma, allowing operators to launch anywhere, anytime.

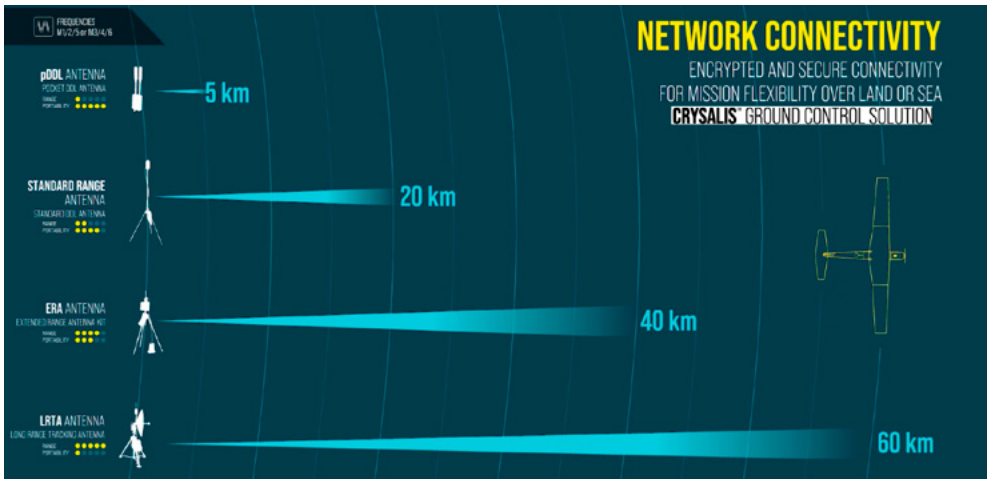
Leveraging AeroVironment's *Crysalis*™ ground control solution, the added VTOL capability now allows a single Puma operator to execute missions and streamline operations through features like one-button launch and recovery.

"*The modern battlefield offers varying types of complex terrain features, both natural and manmade, that can pose challenges to small unit operations and their use of unmanned aircraft. Our new Puma VTOL kit provides the operator with a wider range of launch and land capabilities, enhancing the unit's mission while further safeguarding its personnel during these periods of transitional flight," said . "The VTOL kit converts the Puma AE into a highly precise and agile ISR asset where a single operator can effortlessly launch the aircraft from a small space and attain mission-critical information of enemy forces in a timely manner and land on a desired rooftop or other small, targeted areas*."
— *Shane Hastings*, AeroVironment's vice president and product line general manager for small UAS

Integration of the Puma VTOL kit requires minimal, one-time modifications to the aircraft's airframe by qualified personnel.

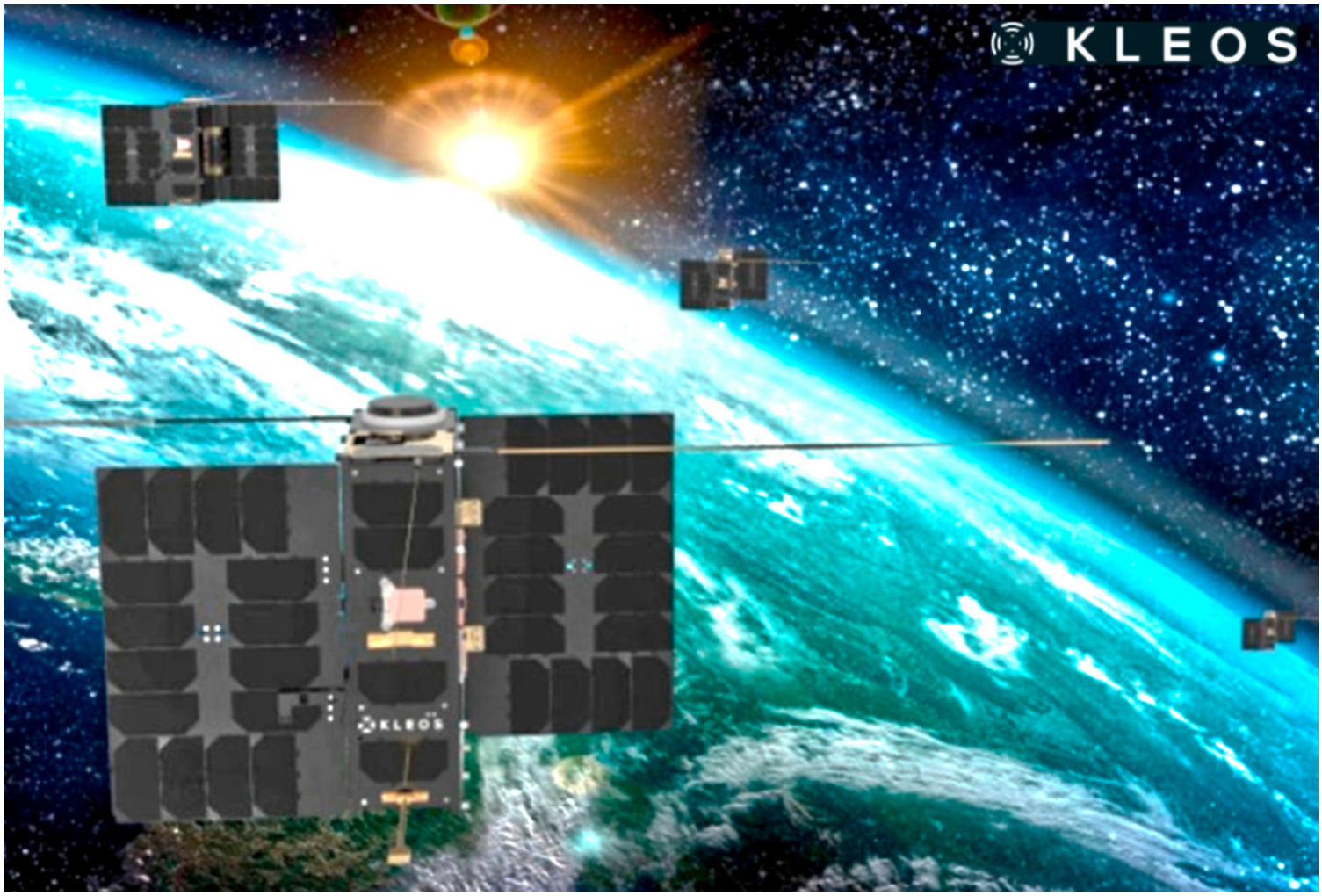
Once modified, the plug-and-play Puma VTOL kit can be easily added or removed in the field within a couple of minutes, allowing operators to quickly transition between a fixed-wing and VTOL platform to suit varying mission needs with a single aircraft.

Available as an add-on option for new Puma 3 AE system orders and as a retrofit kit for already fielded Puma 2 AE and Puma 3 AE aircraft, both fielded and new aircraft can take advantage of this VTOL capability. To learn more about the new operational capabilities of Puma AE and Puma VTOL kit, visit ***www.avinc.com/uas/puma-ae.***



DISPATCHES

Contract extension awarded to Kleos Space by the NRO



***Kleos Space Inc.* (Kleos), a subsidiary of Kleos Space S.A., a space-powered defense and intelligence technology company, last month was awarded the Stage Two option on its current contract with the *National Reconnaissance Office* (NRO) as part of the *Strategic Commercial Enhancements Broad Agency Announcement (SCE BAA) Framework*.**

The NRO is responsible for maintaining global vigilance in times of peace and war.

The agency develops, acquires, launches, and operates innovative space-based surveillance and reconnaissance systems that collect and deliver intelligence to enhance U.S. national security.

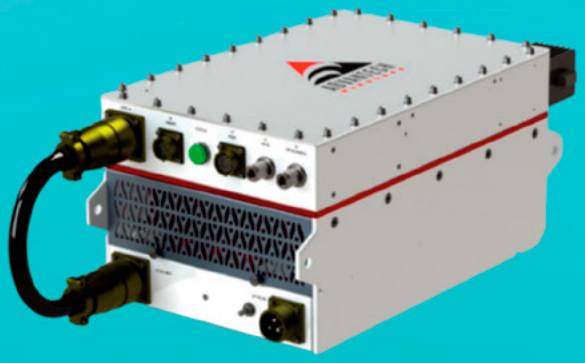
After a multiple-phase proposal process, Kleos was previously awarded the NRO's ***Strategic Commercial Enhancements BAA Framework Stage One*** contract, which focused on the modeling and simulation of Kleos' capabilities to support the U.S. Government's current and future commercial ***radio frequency*** (**RF**) reconnaissance needs. The NRO's SCE Framework continuously evaluates new and emerging commercial capabilities and providers.

Under the Stage Two effort, Kleos will provide insights into how to optimize evolving commercial RF geolocation capability to enhance and augment existing capabilities in a persistent, resilient, cost-effective manner with products that are also easily shareable across the U.S. Government, international partners, and allies.

The newly awarded Second Stage emphasizes tasking, data collection, and direct delivery of data to end-users.

The NRO also exercised an option for future purchases of Kleos data and products to support extended development and experimentation.

ADVANTECH
WIRELESS
A Baylin Technologies Company

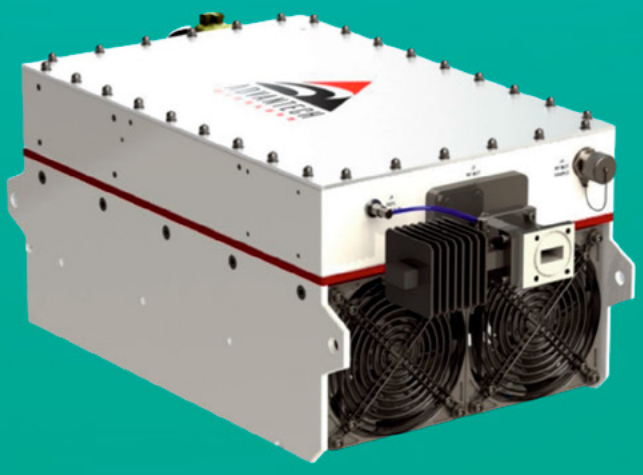


Introducing ***GENESIS*** - the new series of Ku-band SSPAs and BUCs from Advantech Wireless Technologies.

GENESIS epitomizes the latest in hardware and software technologies, making it the most feature-rich satcom SSPA in the industry. Initially available in 200W, and 250W variants, GENESIS delivers a host of high-end features, including some that are unique to the ***GENESIS*** family:

· Secure SNMPv3 interface
· Modular construction – fast production & simple serviceability
· Full M&C capability with embedded Webserver
· Field-removable power supply and fans
· Forward and reflected power monitoring & true RMS power detection
· Device-level monitoring for detailed fault analysis and diagnostics
· Embedded logic to manage multi-amplifier redundant and phase-combined systems, negating the need for any external controllers.

Additional frequency bands and higher power levels based on the ***GENESIS*** platform will become available in the coming months.



L3Harris + BigBear.ai to deliver AI for autonomous surface vessels (ASV)

L3Harris' Arabian Fox outfitted with BigBear.ai's AI-based forecasting, situational awareness analytics, and computer vision capabilities will advance manned-unmanned teaming. Photo By Petty Officer 1st Class Vincent Aguirre

BigBear.ai (NYSE:BBAI) has entered into a teaming agreement with L3Harris Technologies (NYSE:LHX) to deliver advanced autonomous surface vessel (ASV) capabilities and artificial intelligence (AI) for current and future maritime defense programs.

Under the agreement, L3Harris' ASView system will be integrated with BigBear.ai's forecasting computer vision technology to better identify and classify vessels, enhance situational awareness and support manned-unmanned teaming missions.

"Integrating L3Harris' ASView technology and BigBear.ai's AI solutions will increase our ASVs' sophistication by improving contact identification accuracy and pattern-of-life detection for autonomous fleets to inform effective maneuver decisions. Partnering with BigBear.ai reinforces our commitment to delivering dependable and comprehensive autonomous C5ISR-T capabilities to increase survivability and readiness for the fleet."
— Anthony Nigara, President, Maritime, L3Harris

"We are thrilled to partner with L3Harris and combine our cutting-edge AI technology with a key leader in unmanned and autonomous systems. Our advanced AI capabilities enable autonomous vessels to operate with unparalleled efficiency and safety, supporting higher-risk missions, expanding operational reach, and most importantly, saving lives. As the battlespace evolves, autonomous systems will play an increasingly significant role. We look forward to the limitless possibilities that lie ahead."
— Mandy Long, BigBear.ai Chief Executive Officer

Northrop Grumman equipping more USAF platforms with IR countermeasure systems

Northrop Grumman Corporation (NYSE: NOC) continues its work for the U.S. Air Force (USAF) for additional Large Aircraft Infrared Countermeasure (LAIRCM) systems.

Northrop Grumman received the work as part of an existing indefinite delivery, indefinite quantity contract.

The ***LAIRCM*** system defends domestic and international aircrews by detecting, tracking and jamming incoming infrared threats. The system automatically counters advanced infrared missile systems by directing a high-intensity laser beam into the missile seeker.

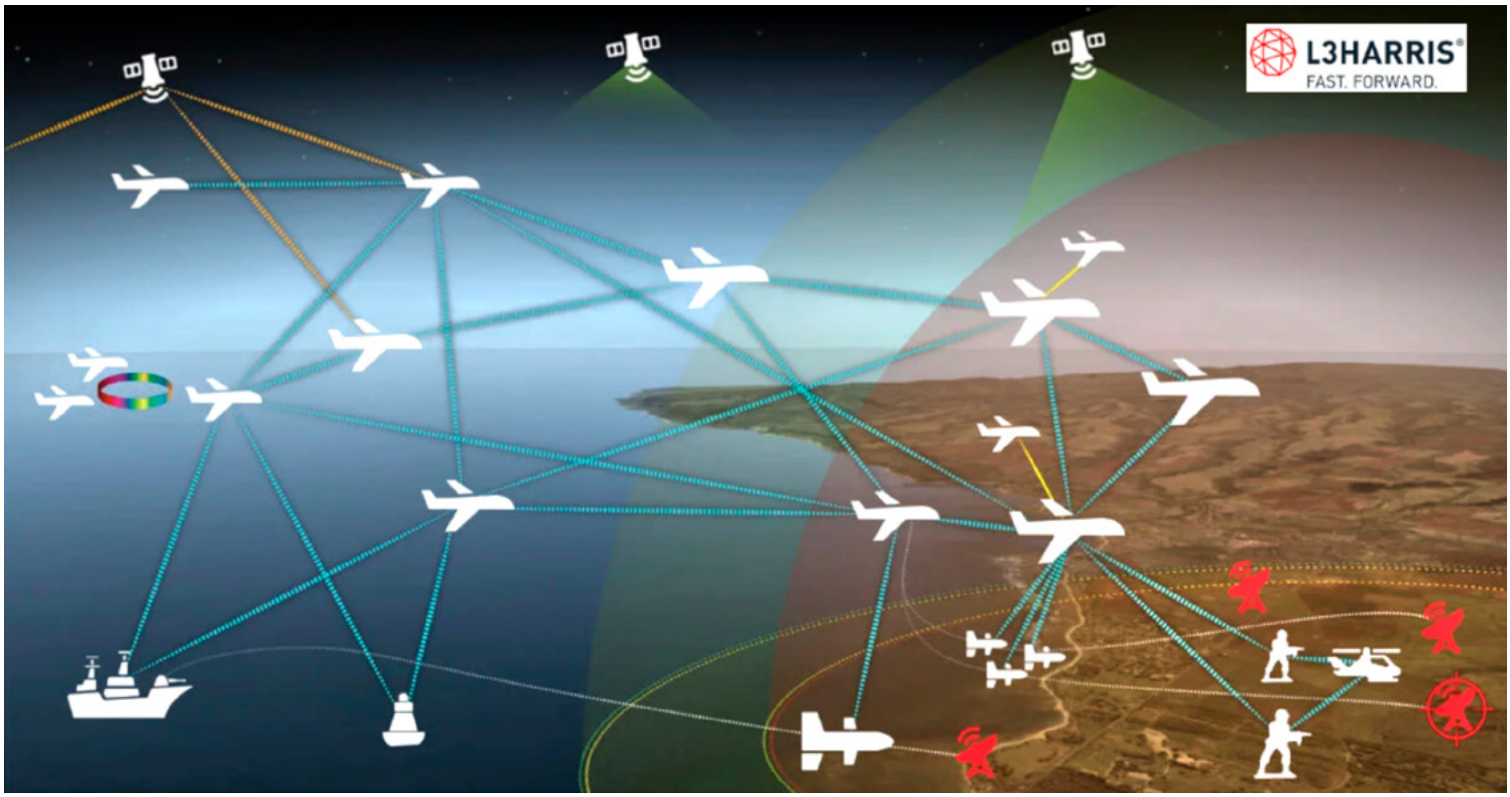
Crucial to keeping aircrews safe, LAIRCM automatically detects emerging missile threats and uses a high-intensity, laser-based countermeasure system to track and defeat missiles
Photo is courtesy of Northrop Grumman.

Under these orders, Northrop Grumman is providing LAIRCM upgrades, modifications and installations on a wide range of U.S. fixed-wing and rotary wing aircraft.

Additionally, this contract covers platforms operated by international customers around the globe.

> *"With its modular, scalable architecture, LAIRCM can adapt to numerous airframes and add technologies that enhance protection capabilities. This proven approach has enabled us to provide the U.S. Air Force and thousands of aircrews with unmatched protection and aircraft survivability equipment that helps them stay safe against emerging threats."*
> *— Bob Gough, vice president, navigation, targeting and survivability, Northrop Grumman*

L3Harris to develop U.S.A.F. Common Tactical Edge Network (CTEN)

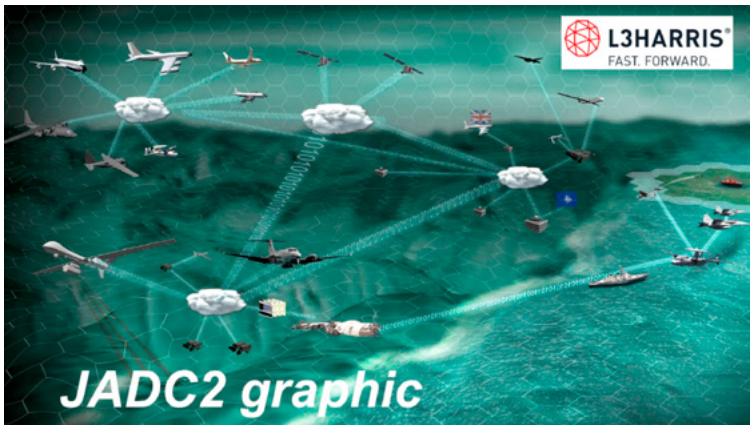


***L3Harris Technologies** (NYSE:LHX) has received a U.S. Air Force (USAF) task order award via the Data Link Enterprise indefinite-delivery, indefinite-quantity (IDIQ) to develop a Common Tactical Edge Network (CTEN) providing an aerial military Internet of Things (IoT) to support the Advanced Battle Management System and Joint All-Domain Command and Control (JADC2) initiatives.*

The system will include a meshed network of defense and commercial resources, enhancing aerial interoperability for U.S. and allied forces by incorporating commercial-like, high-speed data processing and sharing at the tactical edge.

CTEN will initially connect USAF aerial platforms that currently operate with incongruent network architectures with the potential to improve connectivity across the entire joint force.

CTEN's data fusion will enable warfighters controlling multiple platforms to think and operate as one, greatly shortening the decision cycle.



The USAF also named L3Harris as a member of the **CTEN Consortium** in an option under the overarching indefinite-delivery, indefinite-quantity award. As a CTEN Consortium member, L3Harris will collaboratively design the architecture, develop software and conduct systems integration and software maintenance for the CTEN system.

The Data Link Enterprise IDIQ award underscores L3Harris' "***Trusted Disruptor***" support to the U.S. military's JADC2 efforts and the company's more than 40 years of experience developing, delivering and managing secure multi-domain networking solutions for the U.S. military and programs including the **U-2 Dragon Lady**, **MQ-4 Global Hawk**, **MQ-9 Reaper** and **E-4 Advanced Airborne Command Post**.

COMPLETE YOUR **SATCOM** MISSION WITH **iDIRECT GOVERNMENT**

EFFICIENT • SECURE • RESILIENT

iDirect Government

Learn more at idirectgov.com

Marshall Aerospace unveils ARC-Radar

Marshall Aerospace recently unveiled ARC-Radar, a modular sensor suite that allows operators of tactical transport aircraft to rapidly and temporarily outfit their fleet for intelligence, surveillance and reconnaissance (ISR) missions.

ARC-Radar is the first of several products that will be rolled out within the ***Marshall Adaptable Role-fit Capability*** (**ARC**) family in the near future.

Marshall ARC-Radar solves a key logistical problem facing fleet operators: as ISR tasks require complex combinations of sensitive equipment, system installation tends to require extensive and typically permanent modifications to their aircraft or investment in a purpose-built ISR airframe.

By contrast, Marshall ARC-Radar is a role-fit, palletized solution with no permanent integration and no modifications required, using only existing, aircraft power outlets.

The system comprises a two-panel ***Leonardo Osprey 30***, multi-domain, active, ***electronically scanned array*** (**AESA**) surveillance radar, two modified paratroop doors containing a Marshall-designed and manufactured, ultra-low-profile, conformal radome, a rear pallet containing two, articulated radar mounts and ***line-replaceable unit*** (**LRU**) rack, and a forward pallet containing a mission management console.

Leonardo Osprey

The capabilities of Leonardo's radar, combined with the inherent multi-role flexibility of tactical transport platforms, means that Marshall ARC-Radar's potential applications are remarkably broad, ranging from military ISR land, sea or air missions to applied civilian operations such as search and rescue, humanitarian support, and disaster relief.

Despite being fitted temporarily, the Osprey 30 radar suite maintains full performance during operation.

The entire Marshall system can be fitted or removed in under four hours, guaranteeing minimal aircraft downtime.

No modifications need to be made to the underlying aircraft and there are no performance or handling penalties with the product installed.

The result is that fleet operators are freely able to alter the role of an aircraft on a day-by-day basis.

The role-fit nature of the solution means that operators are not constrained to the availability of a single aircraft.

The system provides significant cost savings by offering the core capability of a dedicated ISR system but with the added flexibility of a transferable multi-mission system using an existing fleet — a potential saving of millions.

The scalable nature of the system also allows for future growth of ISR capability at minimal cost.

"*The unique benefit of this roll-on-roll-off system is that it effectively expands the utilisation of existing assets for multi-mission purposes*. *This means the operator could be transporting troops on a Monday and conducting an ISR mission on a Tuesday with the same aircraft, our solution offers true operational mobility*."

— *Ben Jakubowski,* head of Marshall Aerospace's Future Products team

Marshall ARC-Radar has undergone extensive testing on the ***Lockheed Martin C-130J Super Hercules*** platform. In addition to ground-fit trials, a product proving sortie was recently flown with the aim of testing the capability of the radar. During this flight trial, all radar modes were tested and their performance thoroughly verified by Leonardo representatives on a range of static and moving targets of various sizes over both land and sea.

"*Marshall's system using our Osprey 30 AESA radar demonstrated performance which looked as good as any similar system I have tested to date," commented, who operated the radar during the flight trial. "The Marshall Team should be immensely proud of the innovative product they have developed*."

— *Stan Hargreaves*, Leonardo's Head of Operational Demonstrations

Additionally, the modular format of the Marshall ARC platform will allow multiple interchangeable missions across various C-130 configurations, as well a wider range of military transport aircraft. Likewise, the system's modularity also provides a simplified future upgrade path for a range of sensors and SATVOM solutions as technology evolves.

ND SAT COM

INSTALLING RELIABILITY

SKYWAN – THE NEW DIMENSION IN AIRBORNE SATELLITE COMMUNICATION

www.ndsatcom.com

© AIRBUS HELICOPTERS, BART ROSSELLE

CABSAT

16 – 18 MAY 2023

DUBAI WORLD TRADE CENTRE

ND SATCOM Booth S3-C20

www.ndsatcom.com

DISPATCHES

Mynaric receives order from Loft Federal for CONDOR Mk3 optical comms terminals to support SDA's NExT

***Mynaric** (NASDAQ: MYNA) (FRA: M0YN) recently entered into a definitive agreement for the sale of **CONDOR Mk3** terminals to **Loft Federal**, a subsidiary of **Loft Orbital**.*

Loft Federal was selected to produce, deploy and operate NExT — the ***Space Development Agency's (SDA) Experimental Testbed*** — and will use the terminals to support secure and reliable communications. Terminal deliveries are primarily scheduled for the first half of 2024. The order announced today was received in late 2022 and was already accounted for in the previously disclosed optical communications terminal backlog as of December 31, 2022.

NExT – SDA's Experimental Testbed will demonstrate warfighter utility of emerging mission partner satellite payloads prior to potential incorporation in future tranches. The program will leverage the low latency data transfer and *Beyond Line-Of-Sight* (**BLOS**) *command and control* (C&C) infrastructure established by the ***Proliferated Warfighter Space Architecture*** to field and connect additional space vehicles with different mission payload configurations.

Mynaric's CONDOR Mk3 optical communications terminal is specifically designed as a key communication and data transfer system built for mass deployment as part of government and commercial satellite constellations and offers full compatibility with the ***Space Development Agency***'s (**SDA**) interoperability standard. It has previously been selected by Northrop Grumman for the SDA's Tranche 1 Transport and Tracking Layers.

Additionally, ***Capella Space*** ordered the terminal for commercial *synthetic aperture radar* (**SAR**) satellites, by ***WARPSPACE*** for a satellite data relay network and others. It's predecessor, the *CONDOR Mk2*, was recently delivered to ***Telesat Government Solutions*** as part of the ***DARPA Blackjack*** program. In addition, Mynaric was named a key development partner for Phase 1 of ***DARPA's Space-BACN*** program extending the company's success in the U.S. Government satellite communication market.

> ***"We look forward to working with Loft Federal on this key U.S. Government project and demonstrating the advantages of laser communications for transmitting high volumes of critical data when and where it is needed. Laser communications technology is critical to the network infrastructure in the proliferated low earth orbit environment and beyond and we applaud the U.S. Government for leading the adoption of the technology."***
> ***— Tina Ghataore, Chief Commercial Officer of Mynaric***

> ***"The CONDOR Mk3 terminal enables us to provide reliable performance on Longbow, our turnkey satellite platform. By using technologies like these that are commercial and produced at scale, we can deliver fast and simple operations on orbit for SDA NExT."***
> ***— John Eterno, General Manager at Loft Federal***

In July of last year, Northrop Grumman Corporation won a competition to build and deploy a proliferated LEO constellation of 14 satellites with infrared sensors for the Space Development Agency's (SDA) Tranche 1 Tracking Layer (T1TRK). Image is courtesy of Northrop Grumman.

Lockheed Martin selected as the preferred bidder for the Australian Defense Satellite Comms System

Lockheed Martin (NYSE: LMT) has been selected by the Commonwealth of Australia as the preferred bidder for Project JP9102, the Australian Defence Satellite Communications System.

The multi-billion dollar JP9102 project will provide the *Australian Defence Force* (ADF) with a sovereign, military satellite communications (MILSATCOM) system defined by its extensibility, agility and resilience. Lockheed Martin will leverage its experience in space-based mission solutions and networks for its JP9102 offer.

Lockheed Martin has assembled a diverse team of Australian companies including *Inovor Technologies*, *EM Solutions*, *AV-Comm*, *Linfox*, *Shoal Group*, *Ronson Gears*, *Calytrix Technologies*, *Conscia*, *Clearbox Systems*, *DXC* and *Blacktree Technology* to deliver ground and control segments and beyond for JP9102.

Lockheed Martin has also partnered with the Victorian Government to establish Victoria as the engineering and technical hub for the company's JP9102 solution, an investment that will create more than 200 advanced space industry jobs in the state.

As another example of the priority placed on workforce development, Lockheed Martin Australia recently launched a space-focused education program with STEM Punks, a STEM education initiative to educate, upskill and inspire Australia's future workforce.

> *"We are proud to be selected as the preferred bidder to deliver this critical capability to the Australian Defence Force. This capability will provide the Australian Defence Force with robust connectivity and reliable information when and where they need it, and by extension, contribute further to the growth and development of Australia's defence and space industries."*
> *— Warren McDonald, Chief Executive, Lockheed Martin Australia and New Zealand.*

NAVAIR tests nexgen MILSATCOM for USMC MQ-25 H-1 UAS

The Marine Corps' UH-1Y helicopter completed an initial flight to test the data transmission of the new Mobile User Objective System (MUOS) MILSATCOM capability for the MQ-25 Stingray at Pax River.

The team at the ***Dedicated Unmanned Carrier Aviation*** (**UCA**) ***Development Environment*** (**DUDE**) lab at Webster Outlying Field in St. Inigoes, Maryland, and the ***Communications Systems Integration Laboratory*** (**CSIL**) at Pax River, transmitted data using unique test equipment to the UH-1Y during flight, proving MOUS connectivity, resilience, and viability using a maneuvering aircraft.

MUOS is a MILSATCOM system that provides global connectivity to military networks.

The next generation of this system works much faster and has additional payloads that support new waveform capabilities and compatibility with the legacy UHF SATCOM systems.

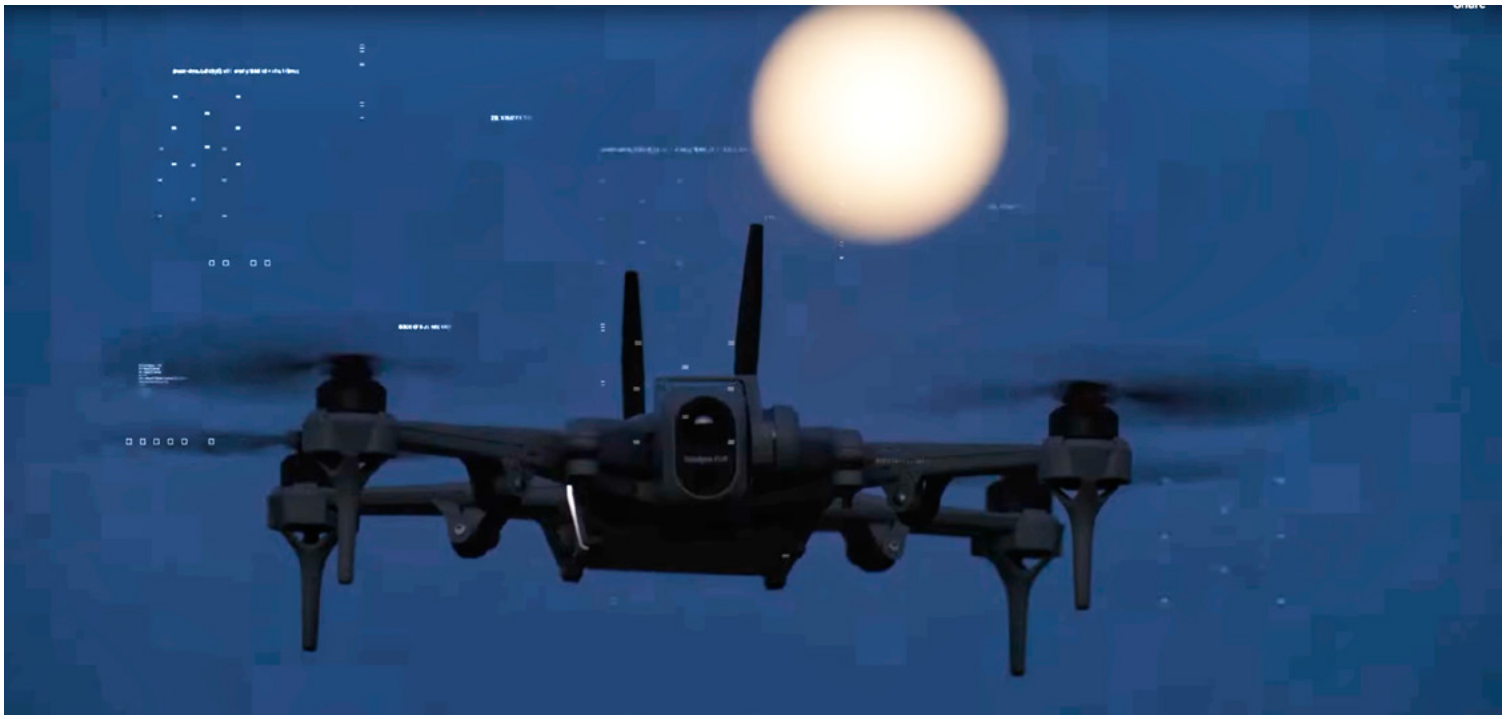
The MQ-25 Stingray will be the world's first operational, carrier-based, unmanned aircraft that will provide aerial refueling as well as ***intelligence, surveillance and reconnaissance*** (**ISR**) capabilities that will enhance the carrier air wing and carrier strike group.

MQ-25 Stingray.
Photo is courtesy of Boeing.

"This type of testing is a way to show how two very different programs can team up and develop capabilities together."
— Capt. Daniel Fucito, Unmanned Carrier Aviation (PMA-268) program manager

"Testing MUOS with H-1 will facilitate the MQ-25 test infrastructure development and ensure MUOS connectivity configuration It also provides an opportunity for the PMA-268 program team to observe MUOS flight characteristics."
— Ray Belcher, MQ-25 Integrated Test Team communications lead

Red Cat receives high-speed drones order for Ukranian deployment



Red Cat Holdings, Inc. (Nasdaq: RCAT) will fulfill a purchase order to provide 200, long-range, high-speed FPV (first-person view) drones to Ukrainian drone pilots who are currently engaged in conflict with Russia.

The FPV drones will be delivered to Ukraine in June.

The drones to be shipped have the highest power-to-weight ratio in the drone industry, offering increased maneuverability, especially when combined with the FPV functionality of the drones.

These FPV drones can also fly in GPS-denied and GPS-jammed battlefield conditions.

Officially launched last month, the Teal 2 is designed to Dominate the Night™ and is equipped with Teledyne FLIR's new Hadron 640R sensor.

This provides end-users with the highest resolution thermal imaging in a small (Group 1) form factor and is optimized for nighttime operations.

Red Cat's other technology partners for the Teal 2 include ***Athena AI***, ***Reveal Technolog,*** and ***Tomahawk Robotics***.

"*Fortunately, Red Cat has the U.S. manufacturing capacity required to quickly deliver on such orders. We are pleased to provide our product to Ukrainian drone pilots, and we look forward to continuing to engage with them, including by providing our new nighttime drone, the Teal 2. Much of drone activity is performed at night, and the Teal 2 is at the forefront of nighttime drone capabilities*."
— *Jeff Thompson*, Red Cat CEO

USSF + DISA award million$$ CTC contract to SES Space & Defense

SES Space & Defense will provide MILSATCOM capabilities in support of the U.S. Army Warfighter Information Network-Tactical (WINT-T) training activities.

The five-year, *Commercial Satellite Communications* (***COMSATCOM***) *Transponded Capacity* (***CTC***) contract worth $27.54 million has been awarded to SES Space & Defense by the ***U.S. Space Force's Commercial SATCOM Communication Office*** (**CSCO**) through ***Defense Information Systems Agency***'s (**DISA**) ***Defense Information Technology Contracting Organization*** (**DITCO**).

Leveraging SES's global satellite fleet, SES Space & Defense will provide capabilities for the ***U.S. Army Network Enterprise Technology Command*** (**NETCOM**) and the ***U.S. Army Forces Command*** (**FORSCOM**) units to train and prepare a combat-ready, globally responsive Total Force.

This will allow the U.S. Army to continue to build and sustain combatant command readiness requirements, as well as enable research and development activities for testing new applications for mobile missions.

> ***"SES Space & Defense has a longstanding relationship with the U.S. Army and has been supporting the WIN-T program's evolving needs for over a decade. As the U.S. DoD adopts new and more advanced information technology capabilities, it is key that we support them with the much-needed resilient and secure satellite communications in multiple orbits and bands. Combine that with our extensive experience in network integration, we can ensure our customers' advantage in any critical mission scenarios."***
> *— David Fields, SES Space & Defense President and CEO*

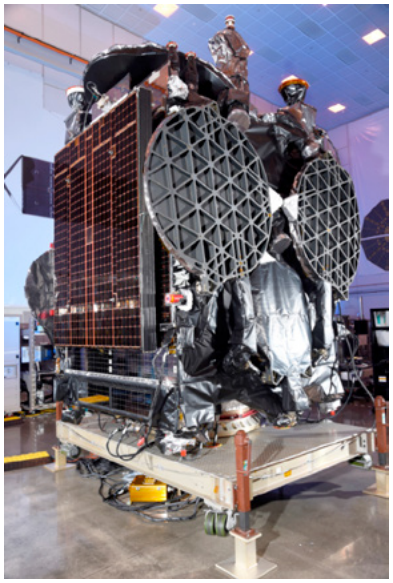


Photo of the SES GovSat-1 satellite, courtesy of Northrop Grumman

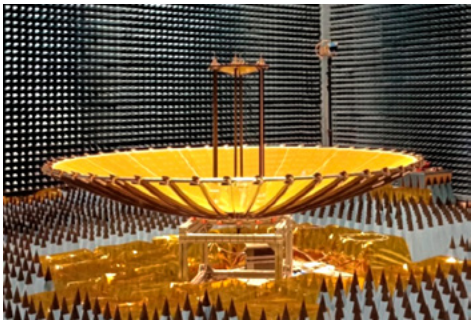
SSTL + Oxford Space Systems to launch the CarbSAR in orbit demo mission to showcase wrapped rib antenna

Surrey Satellite Technology Ltd. (SSTL) and Oxford Space Systems (OSS) have confirmed a partnership to build and launch an OSS Wrapped Rib Antenna mounted to an SSTL CarbSAR satellite.

The In Orbit Demonstration mission advances both companies' abilities, with OSS gaining space heritage, and SSTL building its ability to integrate capability from new suppliers. The work has been jointly funded by **OSS**, **SSTL**, **Airbus Defence and Space**, the ***National Security Strategic Investment Fund*** (**NSSIF** — *HM Government's corporate venturing arm for national security and defence technologies*) and the **MoD**, and is proving a ground breaking ***Synthetic Aperture Radar*** (**SAR**) concept that may be of significant interest to UK defence *intelligence, surveillance and reconnaissance* (**ISR**) strategies in the near to medium term future.

Surveillance, change detection and "*big data*" analytics applications are driving interest in spaceborne SAR data, to support day/night and all-weather imaging at a rate faster than can be achieved with any individual satellite. This drives demand for much smaller radar satellites that can be launched within a limited launch volume in groups, however it is still desirable to retain a large antenna for better quality imagery.

Having a large, scalable, stowable and lightweight, reflector antenna provides a number of benefits in designing small radar satellites for particular applications. A reflector antenna can also significantly simplify the radar electronics, making it ideal



for implementing radar on much smaller spacecraft, such as SSTL's ***CarbSAR*** platform.

The ***Oxford Space Systems Wrapped Rib Antenna for Synthetic Aperture Radar*** (SAR) enables high resolution imaging from smallsat EO missions, irrespective of weather conditions or daylight. These antennas deploy carbon-fiber ribs from a central hub to form a 3m diameter parabolic dish supporting a high performing metal mesh reflector surface.

This UK developed, antenna technology has a uniquely compact, stowed configuration and achieves a highly, cost-efficient performance when deployed in orbit. The antenna has successfully completed an extensive ground based test program, including a radio frequency (RF) test campaign and is now ready to demonstrate its performance in orbit.

Carbonite is the latest in a long range of 100 kg. class smallsat platforms that SSTL has been building in Guildford, UK, since the early 1980's. Carbonite-1 launched in 2015 was an innovative development mission based on a commercially available optical telescope.

The range was always designed to be multi-sensor and has evolved to feature a standard set of core platform avionics available now with either a high resolution optical, medium resolution multi-spectral, mid-wave infra-red or SAR payload. CarbSAR — delivering high-resolution, X-band SAR imagery — sees the SAR electronics embedded with the standard Carbonite satellite core avionics in an elegant combination with the stowable OSS antenna.

"This In Orbit Demonstration mission will allow us to build on our relationship with SSTL and accelerate our product development and industrialization program for the game changing Wrapped Rib SAR antenna. The support of NSSIF is a huge vote of confidence in the technology and the capability of Oxford Space Systems to support future UK requirements."
— Sean Sutcliffe. CEO, Oxford Space Systems)"

"Announcing a new satellite mission is one of the most exciting things we get to do here at SSTL. And that excitement is amplified when the mission in question is CarbSAR, a variant of our Carbonite range, and a mission part-funded by our Shareholder Airbus Defence & Space. CarbSAR is a compelling UK success story on its own, as well as a necessary step towards the bigger spacecraft required for the UK's Space ambitions. The integration of our latest generation 100Kg Satellite platform and SAR electronics with OSS's revolutionary wrapped rib antenna is a mission we will be very proud to launch."
— Andrew Cawthorne, Business Development Director at SSTL.

Boeing's new military satellite integrates anti-jam payload for enhanced battlefield comms

***Boeing** [NYSE: BA] recently unveiled the company's Protected Wideband Satellite (PWS) design that features Boeing's Protected Tactical SATCOM Prototype (PTS-P) payload hosted aboard the U.S. Space Force's Wideband Global SATCOM (WGS)-11 spacecraft.*

The combination of military satellite communications (MILSATCOM) and anti-jam capabilities underpin the PWS design.

Both programs are based on Boeing's 702X software-driven technology enabling real-time and automated beam-forming for improved stand-off performance and signal protection.

The program is scheduled for launch in 2024, with on-orbit testing slated for 2025.

After on-orbit demonstration, the PTS-P payload will be available to transition for operational use.

The PTS-P design features automated anti-jam capabilities, including jammer geolocation, real-time adaptive nulling, frequency hopping and other techniques, harnessing the power of the U.S. military's ***Protected Tactical Waveform*** (**PTW**) to ensure the warfighter can stay connected in a contested environment.

By flying PTS-P on the WGS-11 spacecraft as part of the WGS constellation, PWS works seamlessly with all the existing WGS user terminals, while allowing gradual fielding of PTW modems in a theater of operation.

WGS provides the ***Department of Defense*** with a broad majority of tactical communications going through the constellation that currently includes 10 satellites.

"The joint force is relying on us to deploy capabilities that enable secure communications in a prolific jamming environment. We also need mission-relevant speed and affordability, while being mindful of the evolving threat in the battlefield. The Boeing PTS-Prototype payload hosted on WGS-11 is an exciting leap forward for new warfighter capabilities." — Charlotte Gerhart, Space Systems Command's Tactical SATCOM division chief at the U.S. Space Force

"The Protected Wideband Satellite combines significantly upgraded WGS capability with PTS-P's automated anti-jam features. This capability sets the stage for future generations of protected wideband systems that can operate in both legacy transponded and new onboard processed modes." — Michelle Parker, vice president of Boeing's Space Mission Systems

702X: The more cost-effective, software defined satellite. Images are courtesy of Boeing.

iDirect Government showcases new modem for nexgen terminal design

iDirect Government (iDirectGov) showcased their 450mp integrator kit at the 2023 Special Operations Forces (SOF) Week that was held from May 8-11, in Tampa, Florida.

The integrator kit is the first phase in the much-anticipated launch of the 450mp multi-waveform, multi-orbit, ***Software Defined Radio*** (SDR) / modem.

The 450mp features an innovative modular three board design: *radio (RF) module*, *common compute (digital) module* and *carrier board*.

The SDR capabilities will enable support of multiple waveforms via a single compute platform.

The waveforms are not limited to transponder satellite links but include ***Common Data Link*** (**CDL**) and other point-to-point links.

The design of the 450mp allows integrators to use iDirectGov's carrier board or choose to design their own custom board, a powerful option for optimizing the size and shape of a remote or developing the most advanced man portable terminals.

Furthermore, the industry standard digital interface of the 450mp common compute module enables a direct digital interface to RF transmitters and receivers.

The 450mp SDR focuses on security, resiliency and mobility—the key elements of iDirectGov's next generation ***EVOLUTION*** platform. The man portable, first of multiple form factors in the 4-Series SDR suite, will support GEO, MEO, HEO and LEO orbits and a variety of waveforms which are essential for network resiliency for voice, data and video defense communications.

> *"The flexibility of the 450mp is truly a game changer. We now offer a common compute platform which can host a myriad of waveforms, provide a digital interface to RF equipment, and provide terminal integrators the ability to develop truly bespoke communication platforms and backed by as many as 16 hours of engineering support. This is a game changer for military satellite modem integrators and their future terminals."*
> *— Karl Fuchs, iDirectGov senior vice president of technology*

ACCESS TO RF SPACE DOMAIN AWARENESS (SDA) THROUGH THE SPACE ISAC WATCH CENTER

Author: Michael Clonts, Director of Space Domain Initiatives, Kratos

In Norse mythology, two ravens served Odin, the God of War. They flew out daily to collect information and update Odin on global sightings of enemies and other relevant activities. Their insight provided context, awareness and foresight that enabled Odin to make effective decisions.

Woodcut image of the Norse god Odin sitting on a throne with his two ravens.

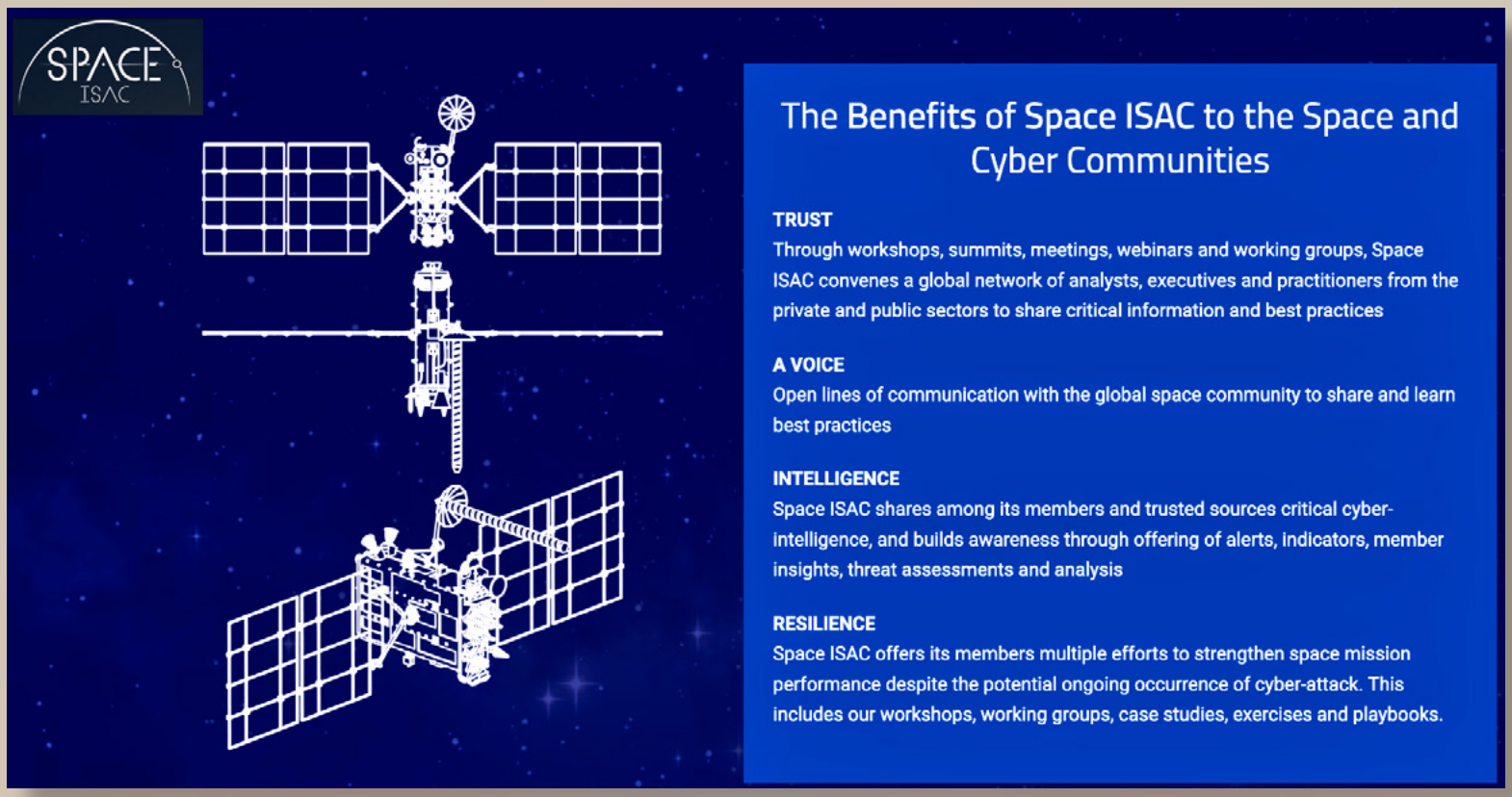
Like the ravens, our military and commercial space operations rely on information collectors. *RF sensors*, *radar* and *Earth Observation* (EO) collect data for situational awareness and better decision-making.

Unlike the ravens, who only served Odin, today's intelligence supports many interests, as global data and services related to space are critically important for strategic military reasons, as well as growing commercial dependence.

Real-time Insight To Work Through Threats

In March of 2023, the public and private ***Space Information Sharing and Analysis Center*** (**Space ISAC**) announced the opening of a new operational **Watch Center** that focuses on detecting and sharing cyber threat information, as well as real-time insights on various other threats to satellite systems.

Partnering with more than 30 government agencies and a member base of 64 organizations worldwide, the Watch Center will receive real-time data from member companies, such as ***Kratos***.



Erin Miller, Executive Director of the Space ISAC, said, "*By sharing information on disruptions to space systems through the Watch Center, we are creating a unified front against potential threats*."

Correlated Space + Terrestrial Data

Kratos' contributions to the Watch Center include access to ***RF Space Domain Awareness*** (**SDA**) data from the ***Kratos Global Sensor Network*** (**KGSN**), a global deployment of more than 140 RF sensors capable of pinpointing satellite locations within 100 meters.

Users access the network through a cloud-based ***Common Operating Picture*** (COP) showing data from both space and terrestrial assets. The RF COP is just one of the tools helping the Watch Center improve visibility of attacks on space-based assets. Examples of insights available within the Kratos' RF COP include:

- *Precision ephemeris for space traffic management and orbital slot verification*
- *Multi-transponder spectrum monitoring and signal characterization*
- *Detection and characterization of EMI and jamming*
- *Satellite maneuver detection and real-time alerting*
- *Rendezvous and proximity operations monitoring*

Geolocation Of Terrestrial Transmitters

Frank Backes, Senior Vice President of Kratos Space, said, "*We are seeing much more aggressive activity. Adversarial nations have launched satellites that can get close enough to listen in on signals other satellites are sending, and in some cases, threaten those satellites. For private companies to face that threat alone is a big task*."

The Watch Center represents the global space community's efforts to assist companies with a collaborative environment of commercial and government experts.

Kratos RF COP Reveals RF Data in Real-time

RF Data Fills the Gap

Kratos' RF SDA services augment today's traditional resources with tools for understanding and responding to emerging on-orbit threats for military and commercial entities.

RF-based SDA is unique in that it fills key gaps in traditional SDA systems such as radar and electro-optical. By capturing native radio frequency signals, objects in space can be located, identified, characterized and tracked to analyze satellite missions and operations, and provide response capability to threats and challenges in space.

Kratos RF COP reveals RF data in real-time.
Image is courtesy of the company.

SDA has become vital to mission success given the increase in commercial space activity and the escalating number of international actors influencing the dynamic theater.

While electro-optical sensors continue to improve in performance, they are still subject to solar exclusion windows during which satellites cannot be observed. Spacecraft operators know this and schedule operations to capitalize on it. In addition to solar exclusions, cloud coverage blinds electro-optical telescopes, while passive RF sensors operate 24/7 in all weather.

To be clear, passive RF sensing complements SDA — it does not replace other sensors. RF sensors can only observe objects that are transmitting, so it's useful for active spacecraft but are blind to space debris.

Commercial + Military Interests

Analysts at Kratos have been using RF SDA to closely track the Russian spy satellite, ***Luch Olymp*** (*www.kratosdefense.com/constellations/articles/espionage-in-orbit-satellite-or-spy*). The satellite, ostensibly part of a civilian data relay constellation, exhibits unusual behavior leading experts to conclude its mission is signals intelligence.

RF observations confirm Luch Olymp transits the GEO belt, frequently stopping near military and commercial satellites, presumably capturing their communications.

After a 63,000 km relocation in August of 2022, it is holding a steady longitude of 18 degrees West, a slot co-located with ***Intelsat 37E***. This extended stay represents one of Luch Olymp's longest periods without relocation.

The ongoing conflict in Ukraine may influence this satellite positioning. Luch Olymp's current orbital slot supports trans-Atlantic traffic from Europe, North America and Africa, hosting a variety of users that may be of interest to the Russian government.

Based on observed offensive actions in the space domain since February 2022, this longitude appears to support Russian strategic operations in Ukraine.

At the grand opening of the Watch Center, Commander of *U.S. Space Operations Command*, *Lt. Gen Whiting,* said, "*By monitoring both space and terrestrial activities, we can defend collectively against adversaries and reduce response times from months to minutes — an unprecedented achievement*."

Whiting reemphasized the importance of coordinated cyberthreat sharing at the recent **Space Symposium**, saying that the Watch Center will help ensure information is not siloed among commercial and military operators.

Space Force leaders have publicly acknowledged that cybersecurity is the soft underbelly of global space networks, which was exposed in the 2022 cyberattack on a commercial SATCOM provider.

As space becomes an increasingly contested domain, the Watch Center is enabling military and commercial operators to share threat intelligence to better detect, deter and withstand adversarial cyberattacks.

Kratos owns and operates the world's most precise global commercial ground network of RF sensors. Strategically positioned apertures around the globe enable precise and persistent RF sensing, providing insight for missions in defense, intelligence and commercial operations. The global network covers L-, S-, C-, X- and Ku-bands. Kratos' state-of-the-art OpenSpace® Platform manages and controls the status of the global network.

Global Interests, Common Goal

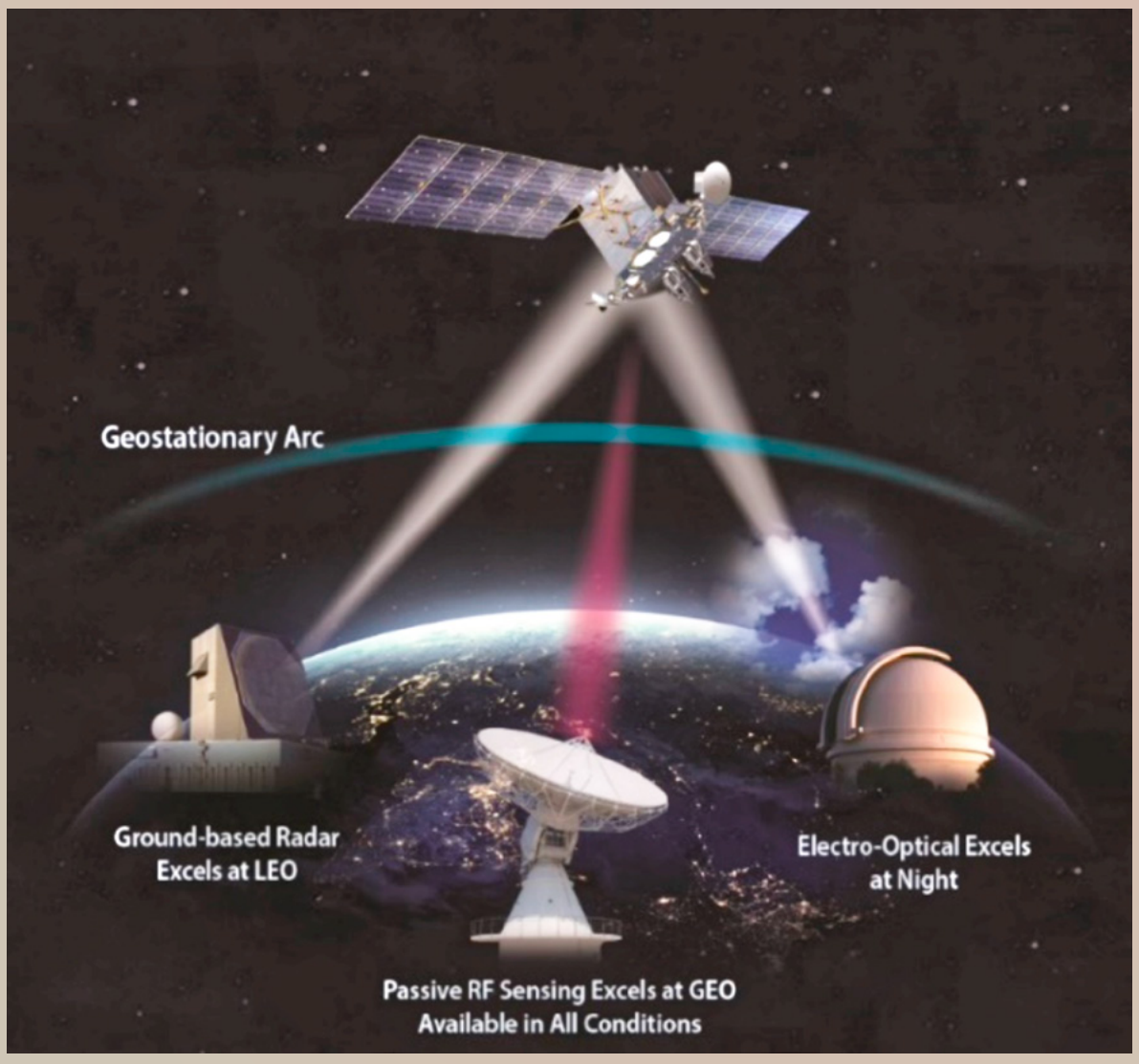
Effective intelligence to understand the global space and cyber operating environment depends on having the right information, at the right time.

The ravens provided situational data to Odin, enabling him to have greater understanding about his adversaries and his world in general. In our real world, intelligence must accommodate more than one global interest. Having platforms such as the Space ISAC Watch Center, that can share situational awareness data with multiple entities with common global interests, is essential to defending our space assets.

Author Michael Clonts is the Director of Space Domain Initiatives at Kratos. He shares experience from a 20-year career in satellite communications, signal monitoring, software engineering, and product management.

Please visit ***this direct link*** for more information on ***Kratos SDA*** services.

For more information about ***Luch Olymp***, visit ***Kratos Constellations*** and read "***Espionage in Orbit: Satellite or Spy?***"



Advanced Networking Tools Enhance RPA Resiliency

Author: Rick Lober, Vice President and General Manager, Defense and Government Systems Division, Hughes + Senior Columnist for SatNews Publishers

Over the past decade, commercial providers have played an instrumental role in helping the U.S. military make the best use of remotely piloted aircraft capabilities.

These firms have built the aircraft, developed sophisticated sensors as well as the electronics used in flying the planes, and provided the satellite bandwidth needed to operate RPAs on distant missions from half-way around the world.

However, military forces flying RPAs have faced a challenge in preventing the satellite signals from being jammed in hostile environments. Techniques, such as frequency hopping or blocking certain frequencies, have been developed with some success, but adversaries continue to find ways around many of these efforts.

Now companies that specialize in terrestrial and space networks are developing software that takes anti-jamming capabilities to a whole new level. With such software built into an aircraft's electronics, it can change not only the frequency of the signals flowing to and from the RPA, but also switch from one frequency band to another, from one satellite to another, from one constellation to another and even from one waveform to another.

New network management software can move a signal from K-band to X-band, from an Intelsat satellite to a government WGS spacecraft, from an O3B satellite in ***Medium Earth Orbit*** (**MEO**) to a OneWeb satellite in ***Low Earth Orbit*** (**LEO**) — all in a matter of milliseconds. A hostile jammer would not even know where to look to find the RPA signal.

Hughes began the development of this capability a few years ago under a demonstration study with the ***U.S. Air Force*** (**USAF**). We did a pilot program for the military and continued to develop the technology on our own to build into our overall network management system. We call the resulting software agent our ***Smart Network Edge***. Such network management software is continuing to evolve and is being looked at by several branches of the military.

Traditionally, the connection to the RPA is controlled from the ground. When jamming is detected, the network and its operators look for ways around it to maintain the link to the RPA. In the past, this has sometimes even involved an old-fashioned phone call from one ground operator to another to switch frequencies.

Smart new solutions are moving the anti-jamming control from the ground station to the terminal inside the RPA, automating the entire process with machine learning and artificial intelligence capabilities built into the network management software. The RPA then controls the process, directing the incoming and outgoing data flow to the clearest, most efficient path.

RPAs use two different connections when in operation. One is the ***Command & Control*** (**C2**) signals from the pilot on the ground flying the aircraft and operating its weapons systems. The other is for the video and other sensor feeds going mostly from the RPA to ground analysts making decisions based on the data being collected.

When applied to either or both of these connections, the network software detects and prevents jamming as well as directs data to the most efficient path for the data transmission in question.

For example, it might use a GEO satellite if the signal lag known as latency is not important. Or, it might use a LEO satellite when low latency is an important factor.

The satellite orbit selected also affects the data flow as the antenna on the RPA is so small. When connected to a distant GEO satellite, the throughput might only be around 12 megabits per second, while a closer MEO satellite would provide 70 Mbps and a LEO constellation around 100 Mbps—speeds that can make all the difference in critical military and humanitarian decisions.

We have worked on developing our Smart Network Edge software with ***General Atomics Aeronautical Systems*** ***(GA-ASI)***, a leading developer of RPAs and manufacturer of the well-known ***MQ-9 Reaper***, sometimes called the ***Predator B***. We engaged in a demonstration late last year and installed our network manager on GA-ASI's new, ***MQ-9B SkyGuardian*** RPA. In the demonstration, the software switched signals smoothly between GEO and MEO satellites operated by the commercial provider, that being ***SES***.

The next milestone we and others are working toward is the full integration of communications on RPAs with direct sequence spreading, combining the data signal with a high data rate bit sequence to improve jam resiliency and reduce the probability of intercept and exploitation. With this capability, engineers will be able to configure a signal so that it virtually disappears, making jamming all but impossible.

Multi-orbit and multi-spectrum connectivity makes absolute sense for RPA applications because it ensures greater resiliency for flight operations. Combining multiple transports, with enabling technologies, such as the ***Hughes Smart Network Edge***, and managed services integration, will unlock the value of all these new and existing constellations in primary, alternate, contingency, and emergency (PACE) planning and execution.

General John Raymond, who served as first chief of the U.S. Air Force Space Command before retiring late last year, emphasized that he measured military readiness on the ability to "***fight tonight***." Ensuring secure communications with RPAs is a vital part of that readiness.

www.hughes.com

*Author Rick Lober is the Vice President and General Manager, **Defense and Government Systems Division** at **Hughes Network Systems, LLC** (HUGHES) and leads the company in serving U.S. and allied defense and intelligence organizations worldwide with advanced SATCOM solutions, commercial and Department of Defense (DoD) purpose-built systems, network management and software defined networking, ground and airborne communications on the move, 5G terrestrial and all company classified programs. Mr. Lober brings 25+ years of experience with COTS and full MIL comms and intelligence programs. He is also a Senior Contributor for **MilsatMagazine**.*

HACK-A-SAT 2023: MOONLIGHTER

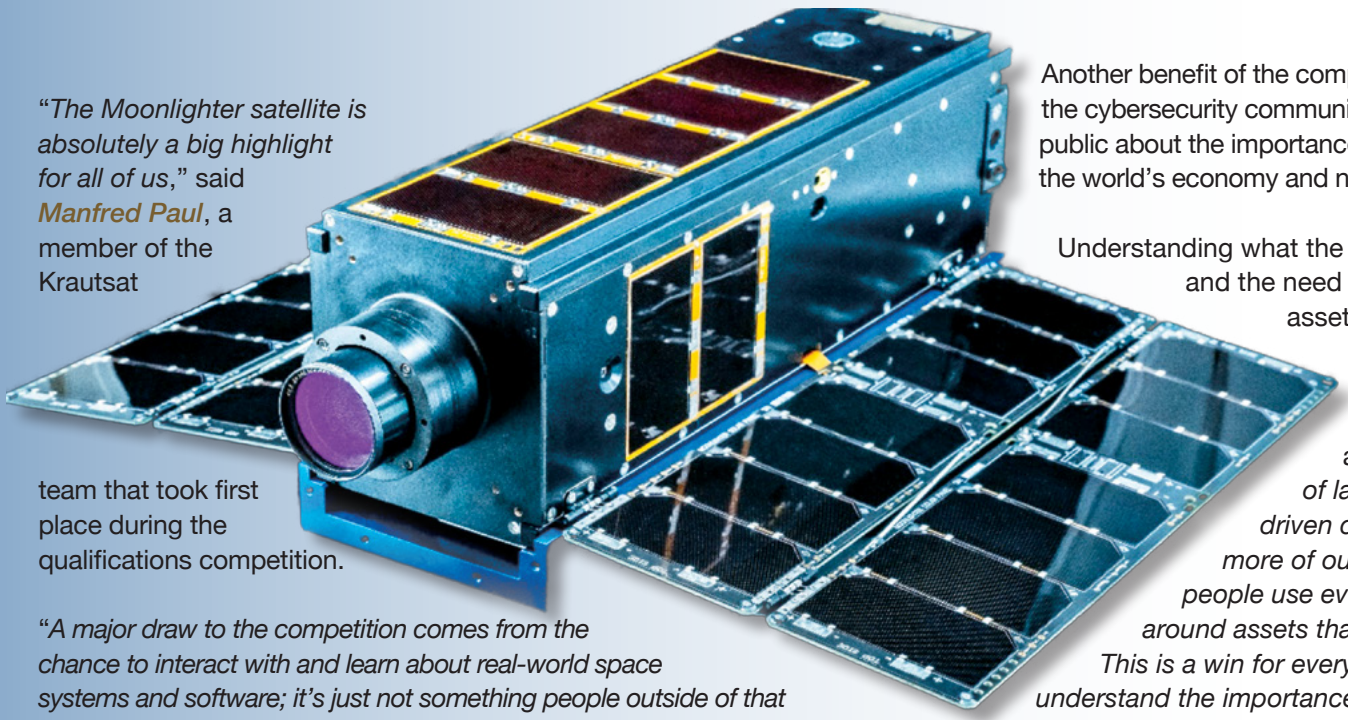
Author: Lisa Sodders, Space Systems Command Public Affairs

The fourth iteration of cybersecurity challenge poses the ultimate test: who can hack a satellite in space?

Five teams in the annual Space Systems Command co-sponsored Hack-A-Sat cybersecurity competition this August (HAS4) will face the ultimate challenge: hack an active satellite in space.

The Moonlighter, a 3U CubeSat satellite built by the Aerospace Corporation, will be launched this summer on a Space X Falcon 9 rocket as part of an International Space Station (ISS) resupply mission. Moonlighter, which weighs approximately 11 pounds and is almost 12 inches long, will be put into a Low Earth Orbit (LEO), awaiting the final HAS4 competition at DEF CON 31, August 11 to 13, in Las Vegas.

The winning team will receive a $50,000 prize and will also have bragging rights that are truly — out of this world.



"*The Moonlighter satellite is absolutely a big highlight for all of us*," said ***Manfred Paul***, a member of the Krautsat team that took first place during the qualifications competition.

"*A major draw to the competition comes from the chance to interact with and learn about real-world space systems and software; it's just not something people outside of that field get to 'play around' with very often*."

Wyatt Neal, one of the members of ***SpaceBitsRUs***, the third-place qualifications finishing team, said, "*To say the team is excited is an understatement! Everyone is really pumped just to see what's going to happen; we know the competition is already designed to be challenging and space just makes everything harder*."

Hack-A-Sat is a ***Capture the Flag*** (**CTF**) competition that is designed to inspire the world's top cybersecurity talent to develop the skills necessary to help reduce vulnerabilities and build more secure space systems, organizers said.

This is the fourth year for the competition, sponsored by the ***U.S. Department of the Air Force***, ***Space Systems Command*** (**SSC**) and the ***Air Force Research Laboratory*** (**AFRL**).

"*The cost/benefit for this competition is far better than what we've seen in the past*," said ***Capt. Kevin J. Bernert***, ***SSC Hack-A-Sat Program Manager***. "*Traditionally, to put something on at this scale and get this much information out of it, would cost a lot more. We can actually observe these competitors using tactics, techniques and procedures that can help inform future space vehicle design to make them more secure. If there are any vulnerabilities that we spot, we can take that into consideration for future space systems*."

Another benefit of the competition is educating the cybersecurity community and the general public about the importance of space assets to the world's economy and national security.

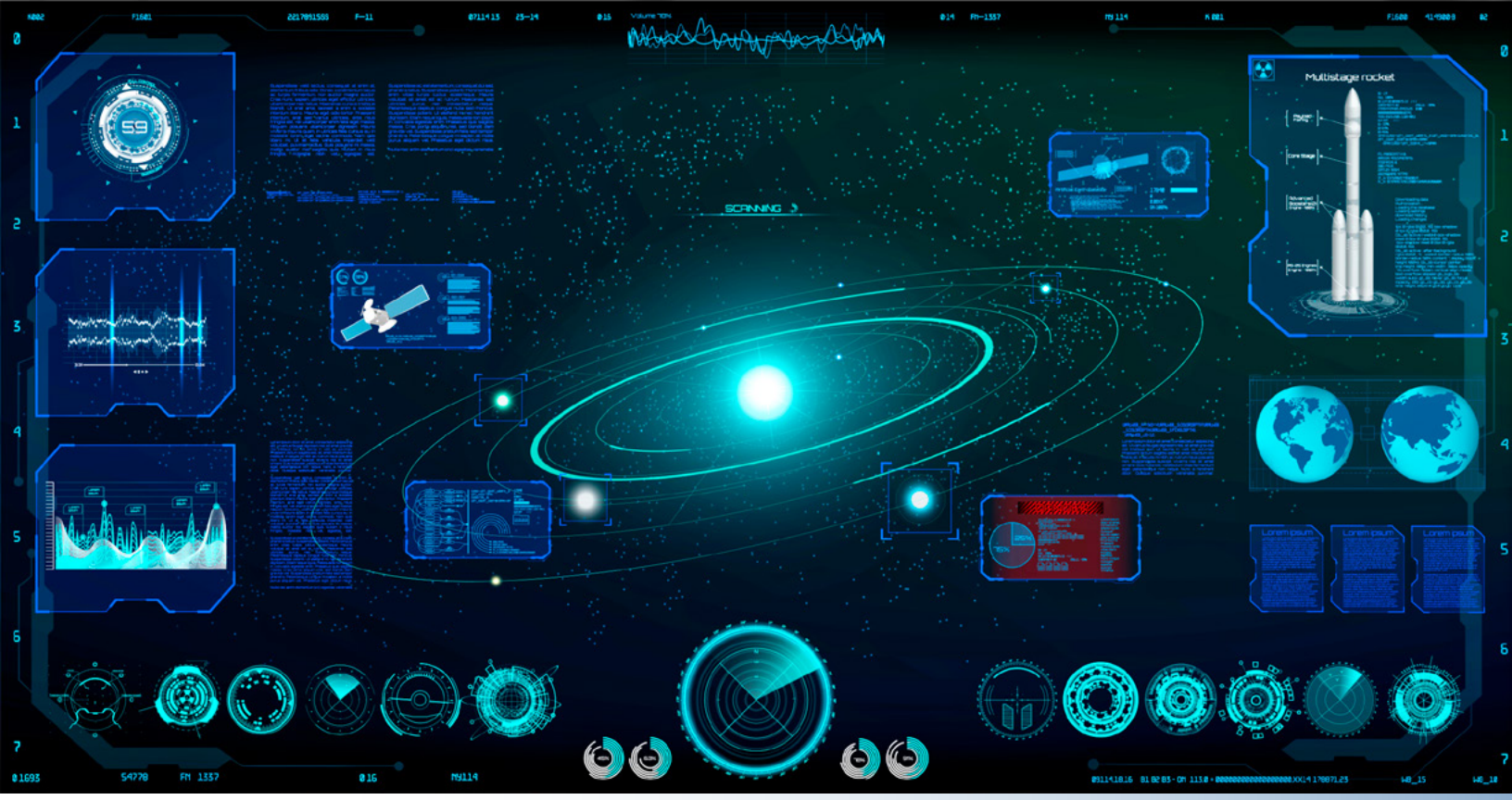
Understanding what the vulnerabilities are, and the need to protect those assets, "*especially as space is becoming easier to access*," ***Bernert*** said, adding, "*The cost of launching is getting driven down, and a lot more of our infrastructure that people use every day revolves around assets that are in space. This is a win for everybody if people understand the importance of securing all those systems — not just the military, but commercial, as well.*

Bernert continued, "*The space industry itself is growing rapidly because everything is becoming more reliant on space. We want to excite people and show them the tie-in between all the cyber-security principles that you're practicing on the ground and how they can be applied to our space systems, too*."

"*For us, the biggest thing we gain is the internal networking opportunities for the team and the chance to work and collaborate with people we wouldn't normally get to interact with,*" ***Wyatt Neal*** said. *"The competition is so fast-paced and it allows the team to rapidly innovate on effective but imperfect solutions and then learn how to improve them collaboratively. This type of competition also gives us the chance to really challenge our members from all different skill sets to learn, teach and grow*."

"One goal the competition has definitely succeeded in is bringing people from cybersecurity and space-related fields together," ***Manfred Paul*** added. "*We've made a lot of new contacts, and also had a lot of exchange of knowledge in both directions – many of those from the cybersecurity side probably didn't know much about orbit calculations and attitude control systems a few years ago. Hack-A-Sat forces you to learn about those things, while still applying the 'hacker mindset' to them. Also, the contest makes it easy to rediscover that certain fascination of space. Personally, Hack-A-Sat sometimes makes me want to go outside, look up in the night sky and thing about how much more there is out there to explore — and hack!*"

Image above: The Moonlighter satellite, courtesy of The Aerospace Corporation.



Hack-A-Sat Teams can range from one person to 100 people or more in number. This year, more than 725 teams comprised of 2,700+ individuals from all over the world competed in the qualification rounds that were conducted from April 1-2.

The top five teams are:

- *Krautsat, a 75-member team made up of mostly German CTF teams and people with backgrounds in space science*
- *mhackeroni, an Italian team that had its best finish*
- *SpaceBitsRUs, a team made up of about 120 Northrop Grumman employees from across the company, which won second place and $30,000 in last year's HAS3*
- *Poland Can Into Space, the $50,000 first-place winner of last year's HAS3*
- *jmp fs: [rcx]*

Many are repeat participants in the annual challenge.

For example, a team named ***Solar Wine*** placed 3rd and won a $20,000 prize last year and the year before, that team was the first place winner.

Poland Can Into Space took second place in 2021 and ***DiceGang*** came in third.

In 2020, the ***Poland Can Into Space*** and ***FluxRepeatRocket*** were among the top three winners and now, three years later, several members of ***FluxRepeatRocket*** are part of team ***Krautsat***.

During the April 2023 qualification rounds, teams logged in to ***quals.2023.hackasat.com*** and completed a number of challenges over a two-day period, said ***Mark Werremeyer***, senior software engineer with ***Cromulence***, the cybersecurity company that designed and hosted the HAS competition.

On the website, competitors could see a scoreboard which listed the challenges with links to access them, and occasionally, files to help them accomplish the task, Werremeyer said.

These challenges required skills in in *RISC-V ROP chaining*, *heap exploitation*, *satellite communications*, *phased array antennas*, *maneuvering into Mars orbit*, *cracking crypto*, *speculative execution*, and *space math*.

Some challenges were asynchronous in nature, similar to satellite operations where commands must be scheduled and the resulting telemetry is available only at a future contact.

If completed correctly, the system rewarded the team with a "***flag***" — a long sequence of random characters tied to that team, which they then submitted to score points.

Wyatt Neal described this year's qualification rounds as "***Intense!*** *I think the hosts aimed to bring the different engineering disciplines together. Some of the challenges could not be solved by a single skill set – you had to blend several disciplines together. A really great example of that was getting our reverse engineers talking with the orbital teams over a ranging filter challenge*."

Despite the competition name, hacking isn't the only skill required. Successful teams need to have people who understand *orbital mechanics*, *radio frequency* (RF) *communications*, *satellite operations*, *astrophysics*, and *reverse engineering*, as well as the ability to exploit development and vulnerability research, *Capt. Bernert* said

He added, "*The teams that really fare the best are the ones that have members all of those areas. Some people can be experts on radio frequency communications or orbital mechanics, but if they don't have the knack for reverse engineering or exploit development, they'll be able to solve some challenges but not all of them*."

Just as space operations is a 24/7 field, the competition ran from 10:00 a.m. on a Saturday to 4:00 p.m. on the following day, requiring teams to work in shifts and manage their sleep, *Werremeyer* said.

He noted, "*Depending on which challenges are coming up, they try and make sure their crypto expert or their space math expert will get some sleep when those challenges aren't active and then come back to solve them when those challenges do unlock*.

"*For HAS2, we had a flat sat built for each team and they would have to control that satellite and solve challenges on it. But it was a flat sat, sitting on, basically, a desk with the other flat sats. Last year, for HAS3, we did full digital twins and emulated the satellite's hardware — that hardware was running the flight software we built for those spacecraft. Each team had their own digital twin spacecraft in a simulated space physics environment and they could command it, attack other satellites and defend their own satellites*.

"*This year, the big difference is we're launching the Moonlighter spacecraft, so we'll have one actual, physical spacecraft that will be part of the game and teams will have to solve challenges on that*," *Werremeyer* said.

While competitors will be able to access Moonlighter, the satellite has a "*sandbox*" portion for the competition, and other controls that the HAS team can use to make sure its batteries are still charged and communications run smoothly, said *Aaron Myrick*, project leader at ***The Aerospace Corporation***, the only federally funded research and development center for the entire space enterprise.

The satellite has no propulsion unit on board — hackers won't be able to send the smallsat careening out of its orbit or into another satellite, *Myrick* said.

Moonlighter is comprised of a camera that will use the stars to calculate a vehicle orientation; a payload camera; a set of circuit boards that include a power routing board, attitude control board and the command and data handling computer, a GPS antenna to receive signals for position and time; a radio antenna to send telemetry and receive commands from ground operators; a payload radio to send telemetry and receive commands from ground operators over a high-speed link; a gyro to measure the rate and acceleration of the satellite's rotation in multiple directions; X-Axis, Y-Axis and Z-Axis reaction wheels, to adjust the pointing of the satellite along the X, Y and Z axis when the wheel speed or direction changes; and a sun sensor to measure the light received to aid in determining the direction of the sun.

"*This satellite is unique because we have built it from the ground up to be a cyber-experimentation test bed*," ***Myrick*** said. "*In a lot of satellite designs, we have a payload for a mission — whether that's imaging or communication — but in this case, what we're trying to do is test out different cyber technologies using a space platform. We had to design almost the entire vehicle and ground segment in a different way than would normally have been completed*.

"*It was almost a little bit backwards as we're trying to think of the ways we want the vehicle to go into a type of failure conditions, different ways to attack the vehicle and then be able to recover from those*," ***Myrick*** added, noting that Aerospace began designing the satellite in 2021. "*That was very important in the concept design: making sure everything is recoverable, and sometimes from different pathways*."

"*For me, it was an interesting progression in my career because we've done some cyber exercises in the past and used end-of-life or residual ops satellites*," ***Myrick*** said. "*In those exercises, we couldn't really do a lot with the vehicle as they just weren't designed for cyber exercises. As we're designing Moonlighter from the ground up, we're able to do all of the things we've wanted to do. It's one thing to do these things on a digital twin and flat sats, but when you're doing things on-orbit and it's real, that just brings it to an entirely different level. There's going to be lessons learned out of this for all who are involved in this exercise. I'm excited to get this opportunity to do this — there's no bigger stage than this for a hacker competition*."

In the past, space was a much more benign environment and the United States could orbit satellites without worrying about any threats, other than natural phenomena.

"*A lot of the space-grade hardware was honestly boutique and hard to acquire*," ***Myrick*** said. "*However, today, many of the Low Earth orbit constellations use automotive or industrial grade components because they survive just fine in LEO and that's driven down the cost and also their availability; however, at the same time, this has driven the need to have more cyber-resilient systems*."

Aerospace will continue to operate Moonlighter after the competition, ***Myrick*** said, noting, "*Eventually, the vehicle will acquire enough atmospheric drag that it will burn up in the atmosphere — we estimate its lifetime at about a year and a half. We are talking with various government organizations within the U.S. Space Force to become involved in activities beyond Hack-A-Sat*."

How will organizers manage to top HAS4 next year? ***Bernert*** said the details are still being worked out and the team will also be taking feedback from HAS4 participants into account. He said, "*People tell us, 'This stuff is really, really hard,' which is good. It's not meant to be easy, because space is hard*."

Follow along on ***Twitter*** ***@hack_a_sat***.

Space Systems Command is the U.S. Space Force Field Command responsible for acquiring and delivering resilient war fighting capabilities to protect our nation's strategic advantage in and from space. The Command manages an $15 billion space acquisition budget for the Department of Defense and works in partnership with joint forces, industry, government agencies, academic and allied organizations to accelerate innovation and outpace emerging threats. Our actions today are making the world a better space for tomorrow.

Contact Space Systems Command at ***SSC@spaceforce.mil — also,*** *follow on* ***LinkedIn***

Subject matter experts contributing to this article: From left to right:

Mark Werremeyer, senior software engineer with Cromulence

Aaron Myrick, project leader at The Aerospace Corporation

Capt. Kevin Bernert, SSC Hack-A-Sat Program Manager

SatNews

CONNECTIONS ON EARTH FOR CONNECTIONS IN SPACE

JOIN US ONLINE!

Free subscriptions and access
Timely news and editorials
Complete archives

satnews.com/reg

SatMagazine | MilsatMagazine | SatNews.com

GOVERNMENT SATELLITE REPORT (GSR)

How AI can accelerate military decision-making in space

Author: David Pesgraves

As the number of deployed satellites continues to grow at stunning rates, it is becoming increasingly difficult for the military to analyze the deluge of inbound data it receives from its space assets in relevant, decision-making timeframes.

By adopting technologies such as artificial intelligence (AI) throughout its space architecture, the military can transform how it analyzes its data in ways that can ensure the delivery of critical information to key decision-makers at the speed of conflict before adversaries strike.

Recently, ***artificial intelligence*** (AI) and satellite experts across commercial industry convened during a special panel entitled, "***How AI and Space Technologies Combine to Benefit the Critical Mission***," to explore the different applications, benefits and some threats AI can deliver to the U.S. military's space initiatives.

Space, The Military + AI

One fact that all the panelists agreed on was that AI, in general, is a technology meant to extract humans out of routine operational functions.

According to ***SpiderOak*** and ***York Space Systems***' *Charles Beames*, "*What it does is it replaces people. Everything we do in space, we do it for the data. And a big part of creating data is doing the analytics to make [data] useful. Rather than having thousands of people looking at each piece of data, they can deploy these great algorithms... that can actually be a huge force multiplier.*"

Lockheed Martin's *Johnathon Caldwell* brought up the point that the relevance of data has a short lifespan, as speed is a dominant factor in the space domain. "*With the sensors we have on-orbit and with people in the loop, we have a hard time today keeping up with analyzing the data*," explained Caldwell. "*The human factor is the limiting factor.*"

He explained that as commercial industry and the military build satellite sensors to proliferation, humans on the ground are going to be unable to keep pace with the sheer volume of incoming data.

"*It's not data that policymakers and military leaders need, but rather knowledge and information to be able to make decisions*," said *Caldwell*. "*To process the volume of data that's going to be coming off of the sensors, networks, and systems is going to require us to move into a new era of how we think about looking at that data.*"

When reframing how data is regarded, it is critical to remember that data is not always relevant, and that it will not stay relevant forever. While it's been established that the military and federal government has a problem keeping up with data volumes, they also have a greater issue of sifting through that data — at the speed of conflict — and decide which information is relevant to decision-making.

"*We have to clean the table...and get on to the relevant data*," said *Caldwell*. "*It all happens at such an amazing tempo. The speed of space is already high, and the speed of conflict will amp up the timetable in which decisions need to be made. And it's going to be much quicker than any of us anticipate.*"

AI Can Simplify Data Complexities

By leveraging AI within their space architectures, the federal government and military can have the ability to analyze information faster and automate some of the more routine — yet extremely complex — processes.

According to ***SES Space & Defense***'s *Ram Rao*, at the heart of AI are the complexities involved in network systems. "*Every system is huge*," said *Rao*. "*For example, SES Space & Defense's O3b mPOWER satellites are going to be operational by the end of this year, and each of those satellites will have 5,000 beams. With 11 satellites in tow, the O3b mPOWER constellation will, in total, have 55,000 beams. There has to be resource management systems which can really control all those beams and complexities that come with it*."

Rao explained that the amount of incoming and outgoing data that these satellites will be processing cannot be managed by humans alone. Factors such as power, bandwidth, and interference management, along with beam switching, hopping, shaping, and formatting, will require more than just traditional conventional algorithms, machine learning to handle vast amount of data as well as deep learning algorithms with neural networks adapting and learning from the data.

"*Approaching conventional management methods makes it very difficult to really address the requirements*," explained *Rao*. "*Especially when it comes to the speed of implementing.*" He went on to explain that if the military were to execute a mission and needed to switch from one satellite beam to another beam, data computing must occur extremely fast to ensure seamless mission communications."

Especially in times of crisis or conflict, if adversaries were to target U.S. military or government satellites, AI technology could detect attacks before they occur, and switch services over to other satellites in the same orbit, or in a different orbit altogether.

By being able to sense and elude an enemy's jamming, interference or degradation of U.S. space assets, the military would have created a resilient space architecture that is capable of denying any attempts adversaries were to make to interrupt critical missions.

"*SES Space & Defense's specialization is end-to-end connectivity, which includes space, satellites, and ground systems*," said *Rao*. "*If there is a degradation or jamming trend that is occurring on-orbit, AI could alert human operators to the trend and ensure that those kinds of critical issues are addressed. Managing those things and making sure that the satellites and systems are healthy is very important. That can be done, but not just through manual, higher-level monitoring. It has to be at a very low – and very intelligent – level. That is an example of when AI becomes critically important*."

To learn about how artificial intelligence is becoming the key to protecting the U.S. Army's space assets, ***select this link...***

This article first appeared in Government Satellite Reportz and is republished with permission of GSR and SES Space & Defense.

David Pesgraves

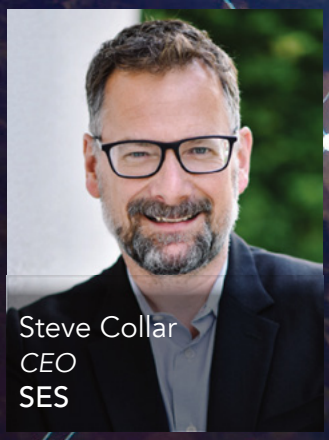
Author David Presgraves is a Staff Writer for GovSat Report, in addition to several other online publications dedicated to defense, military, and federal government agency technologies.

SILICON VALLEY SPACE WEEK: *PART I*

SATELLITE INNOVATION

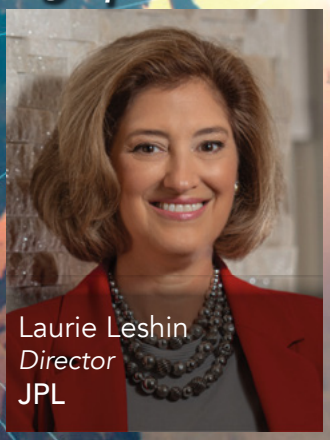
THE MEETING PLACE FOR SATELLITE INDUSTRY LEADERS

Featured Preceding Speakers



Steve Collar
CEO
SES

Mark Dankberg
Chairman of the Board, CEO and Co-Founder
Viasat



Laurie Leshin
Director
JPL

Robert Lightfoot
Executive Vice President, Space
Lockheed Martin

Exhibitors & Sponsors

SATINNOVATION.COM
OCTOBER 17 - 18, 2023

SILICON VALLEY SPACE WEEK: *PART II*

2023 MILSAT SYMPOSIUM

NEXT-GENERATION SPACE DEFENSE

Featured Preceding Speakers

Maj. Gen. Douglas A. Schiess
U.S. Space Force

Dr. Derek M. Tournear
Director
Space Development Agency (SDA)

Gen. David D. Thompson
Vice Chief of Space Operations
U.S. Space Force

Brig. Gen. Steven Butow
Space Portfolio Director
Defense Innovation Unit - DIU

Exhibitors & Sponsors

ACORDE · acs · AIRBUS U.S. SPACE & DEFENSE · Aitech · ANTARIS · ASTRA · ASTRANIS · Astroscale U.S. · AVL TECHNOLOGIES · BLUE CANYON TECHNOLOGIES · CKC LABORATORIES, INC. Testing the Future · COMTECH · CPI Communications & Power Industries · Deloitte. · dhv technology · etl · Experior Laboratories · FIREFLY · gmv · GVF Satellite. Solutions. The World! · Hogan Lovells · HUGHES · iDIRECT · INTEGRASYS · Kipps DeSanto · KRATOS · Milbank Space Smart · MISSION MICROWAVE · MISSION MICROWAVE · MSUA · mynaric LASER COMMUNICATION. MADE SCALABLE. · NASA · neuraspace · NITAAC · NSR · NovaWurks · NOVELSAT · OPENICE · Optimal Satcom · ORBION · OSK · orolia · PHASEFOUR · Raytheon Intelligence & Space · RBC SIGNALS · REDWIRE · ROCKETLAB · SD satcom direct · SIA · SATLANTIS · SE · SES GOVERNMENT SOLUTIONS · SheppardMullin · SPACEBRIDGE · SpaceLogistics · SN · SPIDEROAK · SPIRIT ELECTRONICS · SQUARE PEG · SSPI · Stephenson Stellar Corporation · TERRAN ORBITAL · United Teleports · GSA · Viasat · VOYAGER SPACE · VPT · WALTON DEFENCE · WARPSPACE · wolfSSL · WTA · XipLink

OCTOBER 19 – 20, 2023

MILSATSHOW.COM