Next Generation Space Defense

MilsatMagazine

May 2022

COVER IMAGE IS COURTESY OF ADVANTECH WIRELESS

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

Columnists + Contributors

Chris Forrester, Broadgate Publications
Karl Fuchs, iDirect Government
Bob Gough, Goonhilly Earth Station
Rebecca M. Cowen-Hirsch, Inmarsat
Giles Peters, Track24 Defense
Koen Willems, ST Engineering
Mike Young, Envistacom

Authors

Dr. Ang Cui
Dr. Rajeev Gopal
Renee Hatcher
Victoria Samson
Ryan Schradin
Dr. Brian Weeden

Advertisers

2022 MILSAT SYMPOSIUM 32
Advantech Wireless ..... 1 + 5
AvL Technologies 21
Comtech Telecommunications Corp. 3
CPI SATCOM Products 11
EM Solutions, Inc. (EMS) 7
iDirect Government 19
Leonardo DRS 9
ND SATCOM Products GmbH 14
SpaceBridge 23

Dispatches

SpaceX + NROL-85 2
NRO + UK MOD / CACI 3
Spire Global / PAR Technology Corp. + Black Sky 4
DARPA / SIDUS Space 6
U.S. Space Force / Raytheon Intelligence & Space 8
Terran Orbital, Lockheed Martin + SDA / NIC4 15
Gilmour Space / Department of the Air Force 18
GPS Source + U.S. Army / Viasat 19

Features

It's Not Too Late To Secure Space 10
Author: Dr. Ang Cui, Red Balloon Security

5G Stand Alone Networks Set To 12
Transform Defense Comms .....
Author: Dr. Rajeev Gopal, Hughes Network Systems

Accelerating The Future Of Space 16
Author: U.S. Space Systems Command

U.S. Army Advances New Comms Network Baseline ... 20

DISA + U.S. Army Reset Teaming Efforts 22
To Support 24/7 Cyber Mission.....
Author: Renee Hatcher, DISA Cyberspace Ops Directorate

Government Satellite Report: 24
Commercial X-Band Managed Services The Key
To On-Demand Resilient Comms
Author: Ryan Schradin, GSR

Addressing An Accelerating Threat Environment: 26
Missile Warning + Defense
Author: L3Harris editorial

Focus: Viasat Government Systems — 28
A Briefing With Joel Babbitt, Army Business Development
Author: Viasat newsroom team

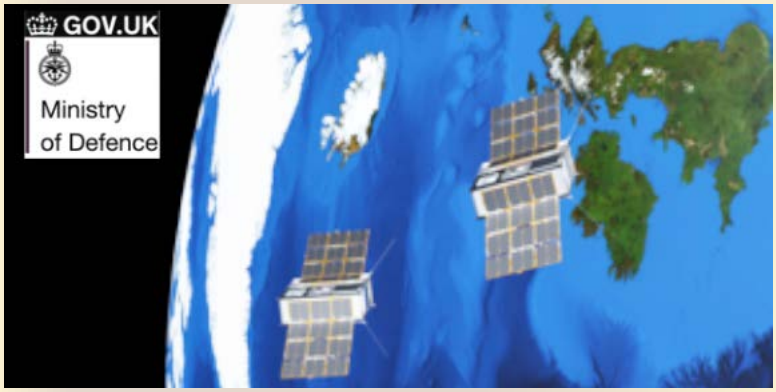
A Secure World Foundation Executive Summary: 30
Global Counterspace Capabilities Report
Authors: Dr. Brian Weeden + Victoria Samson

The Falcon 9 launch of the NROL-85 mission from Vandenberg Space Force Base. Photo courtesy of SpaceX.

A SpaceX Falcon 9 rocket carrying the NROL-85 mission pushed off from Space Launch Complex 4 East (SLC-4E) at Vandenberg Space Force Base in California on Sunday, April17, at 6:13 .m., Pacific Time. NROL-85 is the first NRO mission to reuse a SpaceX rocket booster. NROL-87, launched only two months earlier, was the first NRO launch of a SpaceX Falcon 9 rocket intended to be reused for a future mission.

Additional details via this infolink...

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



MINC seeks to develop software that autonomously configures networks of networks regardless of the communication device or networking resource.

NATIONAL RECONNAISSANCE OFFICE
ABOVE AND BEYOND

NRO Is Partnering With The UK's MOD For The 1st Commercial Rocket Launch From The UK Via Virgin Orbit's Launcher One

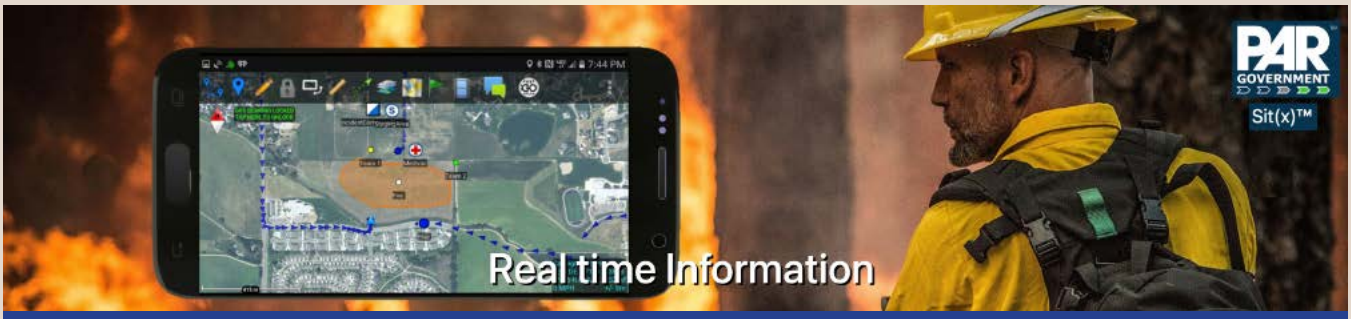
The National Reconnaissance Office (NRO) is partnering with the United Kingdom's Ministry of Defence (UK MOD) on the historic, first commercial rocket to be launched from the UK, as announced at Defence Space 2022 by Defence Procurement Minister Jeremy Quin.
Additional details via this infolink...

CACI Awarded DARPA Contract For Mission Software Development

CACI International Inc. (NYSE: CACI) was awarded a $20.4 million contract to provide technology, research, development, and innovation in support of the Defense Advanced Research Projects Agency (DARPA) Mission-Integrated Network Control (MINC) program.
Additional details via this infolink...

Satellite Data From Spire Global To ID RF + GPS Interferences For Military Applications

Spire Global, Inc. (NYSE: SPIR) has expanded their existing partnership with Slingshot Aerospace. Spire will play a pivotal role in the contract by supplying Slingshot Aerospace with GPS telemetry data, a task underway since the two companies began collaborating in 2021.
Additional details via this infolink...



Near Real-Time Imagery For The TAK Mobile Platform Is Resultant Of The PAR Government + BlackSky Team Up

PAR Technology Corporation (NYSE: PAR) has noted that their wholly-owned subsidiary, PAR Government Systems Corporation (PGSC), has incorporated BlackSky's (NYSE: BKSY) commercial satellite data into the Sit(x)™ cloud-native situational awareness suite.
Additional details via this infolink...

ADVANTECH
WIRELESS
A Baylin Technologies Company

Summit versus Summit II

Though the features between Summit and Summit II are similar, Summit II incorporates the latest in RF and control technologies.

The Summit II systems are comprised of modules that are housed in our Taurus SSPA package. As a result, Summit II is approximately 30% smaller and lighter – the perfect solution for antenna-platform mounting.

Taurus provides optimized thermal management and high-efficiency waveguide combining that includes transistor isolation.

Advantech's latest CANBus operating system provides fast inter-component communications as well as the ability to perform device-level diagnostics.

DARPA Seeks Proposals For The DRACO Nuclear-Thermal Rocket In-Space Flight Demo

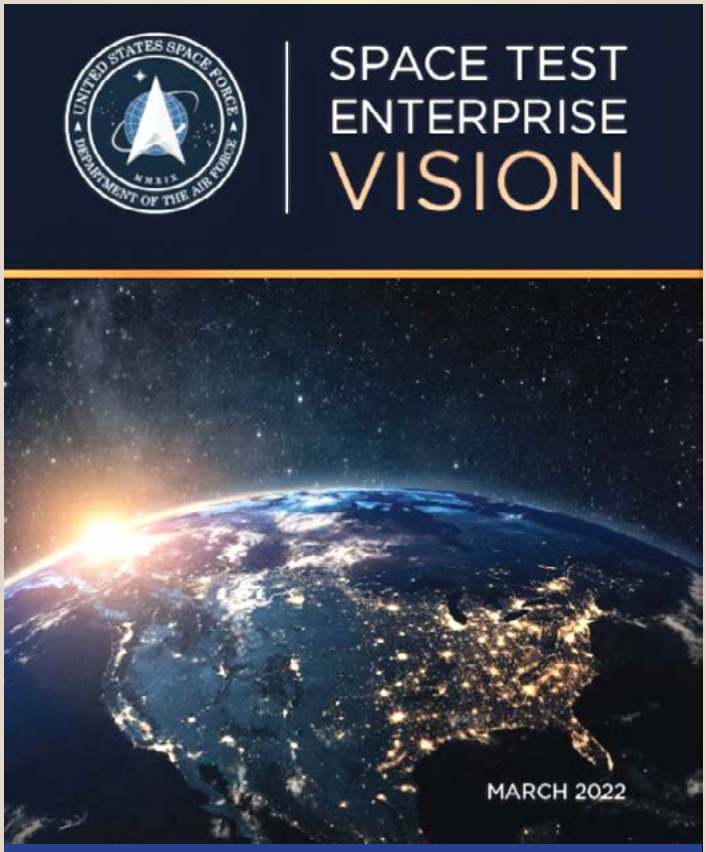
DARPA is seeking proposals for Phases 2 and 3 of the Demonstration Rocket for Agile Cislunar Operations (DRACO) program for the design, development, fabrication, and assembly of a nuclear thermal rocket engine — the goal is to execute an in-space flight demonstration of nuclear thermal propulsion in fiscal year 2026.
Additional details via this infolink...

Sidus Space + Dhruva Space Sign MoU To Further The Commercialization Of Space Tech + Services

Sidus Space, Inc. (NASDAQ:SIDU), a Space-as-a-Service satellite company focused on commercial satellite design, manufacture, launch, and data collection, recently signed a Memorandum of Understanding (MoU) with Dhruva Space Private Limited to further the commercialization of new and innovative space technologies and services.
Additional details via this infolink...

NRO Is Partnering With The UK's MOD For The 1st Commercial Rocket Launch From The UK Via Virgin Orbit's Launcher One

The National Reconnaissance Office (NRO) is partnering with the United Kingdom's Ministry of Defence (UK MOD) on the historic, first commercial rocket to be launched from the UK, as announced at Defence Space 2022 by Defence Procurement Minister Jeremy Quin. ***Additional details via this infolink...***



USSF Space Test Enterprise Vision Integrates Test Across Capability Lifecycles

The U.S. Space Force has released its Space Test Enterprise Vision to communicate the service's intent and provide the amplifying guidance needed to execute the Space Force's test and evaluation mission. ***Additional details via this infolink...***

Continuing Their Support For USAF Geospatial Intelligence Is Raytheon Intelligence & Space

Raytheon Intelligence & Space, a Raytheon Technologies business, has been awarded a five-year indefinite delivery, indefinite quantity (IDIQ) contract to continue Geospatial Intelligence system mission support.
Additional details via this infolink...

IT'S NOT TOO LATE TO SECURE SPACE…

However, time is running out

Author: Dr. Ang Cui, Founder and Chief Executive Officer, Red Balloon Security

The Ukrainian conflict has amplified serious questions about cybersecurity at every link in aerospace deployments. Now is the time for manufacturers, governments,and security providers to align with each other on solutions.

Recent industry conferences have differed from other space trade events of recent years, in that cybersecurity is no longer a sideshow. This is a topic on which most panelists were queried, given the backdrop of the intensifying Ukrainian conflict.

Although the first month of the Russian invasion of the Ukraine did not become an arena of unrestrained cyber warfare that many people feared, the February 2022 ***disruption of a satellite network*** (*which was not restricted to Ukraine*) added urgency to many conversations.

Panelists, when asked about satellite security in Ukraine, Western Europe and the US, gave thoughtful answers that, nonetheless, often lacked actionable details. Most experts presumed that bad cyber actors have a jumpstart on governmental and operators and equipment manufacturers.

This is problematic on two levels. Aerospace and satellite deployments are mission-critical and indispensable to the growth of many industries and technologies. However, ***their attack surfaces have also greatly expanded*** — without corrective action, insufficient security controls will be bolted onto future designs, rather than built *into* them.

However, given the projected expansion of satellite deployments, there is a unique opportunity to build mature security solutions into government and commercial deployments. We can expect an exponential increase in the number of ***Low Earth Orbit*** (**LEO**) satellites, as well as the emergence of small, GEO satellites. This means more methods of connectivity, in space and on the ground, and a corresponding increase in opportunities for cyber malfeasance.

To help stimulate innovation and partnership, here are three messages that should gain traction in 2022 and beyond:

1. ***Don't miss the threat on the ground for the threat in space***

   Much attention has been paid to the threat of signal jamming or spoofing directed at satellite vehicles, which could lead to collisions or disruption of internet access and vital ***industry or governmental communications.*** *But dangerous cyberattacks can focus on any part of a satellite network, including multiple devices that support satellite base stations and communications hubs*

   These assets on the ground can be accessed remotely, or in many cases physically since they often are in isolated locations with variable perimeter security. The objective of such attacks could also be the compromise or destruction of land-based equipment, as seems to be the case with the Viasat/KA-SAT attack, which temporarily disabled thousands of modems in several countries.

   Viasat's analysis *indicates the attacker began by exploiting a VPN device misconfiguration, gained remote access to a segment of the company network, and then sent management commands to thousands of modems at once that overwrote flash memory and temporarily knocked the modems offline. It was a consequential strike that required no knowledge or exploits of a satellite vehicle.*

2. ***End users, manufacturers and security experts must collaborate on advanced solutions***

   The impressive growth of commercial aerospace and satellite deployments complicates efforts to elevate industry security standards. As more business opportunities are built out and scaled, we can expect more players to enter the space and more reliance on increasingly complex supply chains — both of which will elevate cyber risk. The days in which a few established private sector enterprises supplied technology and devices to a few dedicated clients, each of which was a branch of the government, are past.

   Given this new reality, collaboration around industry standards will be essential to satellite network security. As more companies move in, it's critical that established players advocate and fight for high-security standards that reflect the current threat climate. This can help establish benchmarks that exceed current standards, promote accountability, and incorporate security solutions for devices and systems.

   The U.S. government will remain hugely influential, due to the power of its purse, decades of aerospace engagement, and history of collaboration with industry leaders. It can actually incentivize commercial suppliers to invest in advanced security controls by demanding them — and it most certainly should do so.

There is also a need for rigorous testing of new security deployments in controlled environments, such as red vs. blue exercises that can provide training for military operators and opportunities for them to work with device manufacturers to integrate security technology with new and legacy SATCOM equipment. Ideally, this training should include commercial equipment manufacturers, equipment operators, and security experts. Securing space will require a highly collaborative, multi-disciplinary approach: No one body of experts has all the answers.

3. ***Expand regulations to cover embedded systems***

Government regulators have created timely responses to growing threats to SATCOM networks. CISA issued an ***alert for service providers and customers*** *(and a second* ***in collaboration with the FBI****), while NIST has pushed to update* ***its guidelines for SATCOM cybersecurity risk management.***

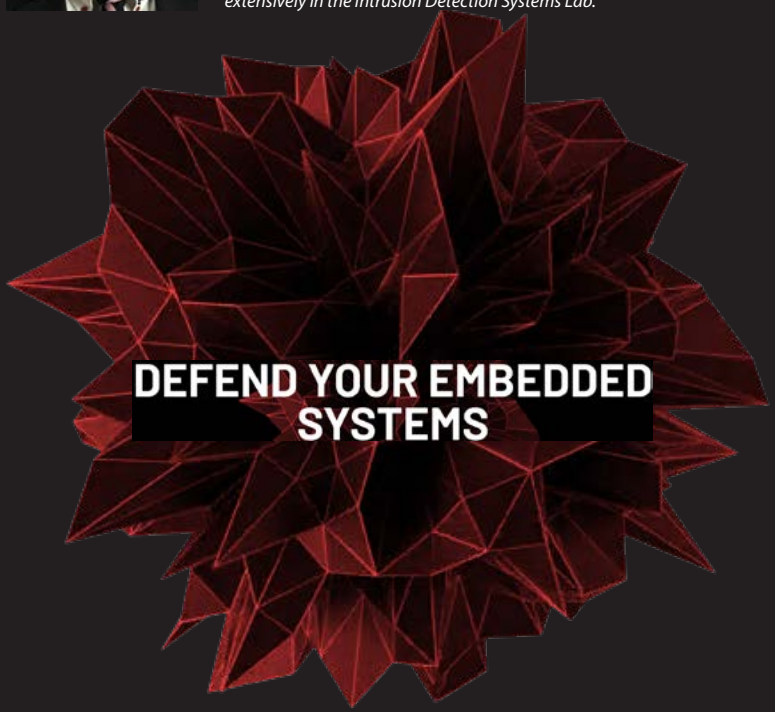
Although welcome, these documents focus on network based security controls that, are essential, but not sufficient to meet current threats. Like other recent directives, they do not adequately address security challenges in embedded systems and the devices that support them. What guidance there is focuses on network controls: also essential, also unable to provide a comprehensive security posture.

For decades, security policy has exempted special purpose and embedded systems as being too difficult to secure while maintaining real-time performance. It is time for policy to catch up with technology and mandate the levels of security controls that are now feasible for aerospace, and many other industries.

There is still time to get it right when it comes to space security, but the longer commercial and government interests wait, the harder it will be to walk back the time that has already passed.

To paraphrase a sage from another era, "*The best time to plant a tree was 20 years ago.*" **The next best time to address satellite cybersecurity is now.**

Dr. Ang Cui is the Founder and CEO of Red Balloon Security, a leading cybersecurity provider and research firm that specializes in the protection of embedded devices across all industries, and which was named "One of 11 Cybersecurity Startups to Bet Your Career on in 2022" by Business Insider. In addition to publishing innovative research, he frequently provides commentary and thought leadership on the most pressing challenges in cybersecurity today. Dr. Cui earned a Ph.D. in computer science from Columbia University, where he worked extensively in the Intrusion Detection Systems Lab.



5G STAND ALONE NETWORKS SET TO TRANSFORM DEFENSE COMMS

Author: Dr. Rajeev Gopal, Vice President, Advanced Systems, Hughes Network Systems, LLC

Mention the term "5G network" and, for most people, what comes to mind is the latest generation of cell phone technology that wireless providers are introducing as they gradually add new equipment and antennas.

However, that same 5G technology that supports public cell networks can be adapted for private applications and these private 5G networks promise to transform how the ***U.S. Department of Defense (DoD)*** manages its military installations, maintains its equipment, deploys its troops, and defends the country.

The main advantage of 5G over earlier generations of wireless technology is that it provides more bandwidth at higher speeds, lower latency and includes an edge cloud. 5G can thus support next generation applications, such as augmented reality and virtual reality, for a larger number of devices than has ever before been possible. It's like having robust, faster and more powerful Wi-Fi everywhere.

Under a new 5G initiative, the DoD and commercial companies have been testing private 5G networks at several military installations. These highly secure, private networks can eventually be deployed on the battlefield, aboard ships and at military installations anywhere in the world. The testing done to date of these standalone 5G networks has been positive. But as the DoD starts to move beyond testing, military planners would be wise to keep *three essential considerations* in mind.

First, using consumer-grade 5G network equipment for such routine commercial operations will not provide the level of ***quality of service*** (**QoS**) or network assurance that may be required. The equipment needs to be designed specifically for standalone 5G network operations and configured for specific QoS objectives.

Second, the local military 5G networks need to be connected to the wider world to meet connectivity needs. The only way to do this from a Pacific-island, a ship or a remote tactical location is via satellite — both ***geostationary*** (**GEO**) and ***Low Earth Orbit*** (**LEO**). A space component must be part of any 5G planning for worldwide connectivity as well as network resiliency.

Finally, it should be noted that the public 5G networks, such as those designed by commercial incumbents, require large operations centers and staff to operate. Standalone 5G networks also must have management and security with significant automation for efficient operations. Even for just 100 people, a managed network is vital and can be cost effective with automated operations.

The advantages of 5G for defense applications are many — employing the new ***5G radio*** (**5G NR**) access network and a 5G network core, these 5G networks are software-based and independent of existing 4G LTE standards — and, therefore, "*standalone*" from older technologies (*vs. "non-standalone" 5G networks that incorporate a 4G LTE RAN and network core*).

Not only are these standalone 5G networks secure, portable and easy to set up, they can link multiple types of devices from a wide range of manufacturers at the same time over several low, mid and high spectrum bands. Using GEO and LEO satellites, a standalone 5G network can be connected to other ships, aircraft, or distant ground stations, with a private cloud supporting tasks and applications ranging from *morale/welfare/recreation* to the *mission critical.*

Test demonstrations over the past year have shown the DoD how these networks can be used in a number of military operations. The military services are continuing these tests, working out ways wherein 5G networks can be deployed for activities ranging from "*smart*" warehouse management, flightline operations at military bases leading toward distributed command and control for multi-domain operations.

At ***Hughes***, the company is involved in one such project at the ***Whidbey Island Naval Air Station*** in Washington state that will demonstrate how a standalone 5G network, with local edge cloud, can be used to support base operations, aircraft maintenance, and flight traffic management. The off-the-shelf components are sourced from U.S. companies and will fit into small, transportable racks.

The technical term used to augment these standalone enterprise 5G networks with edge cloud is "***multi-access edge computing***," or **MEC**. The components include a containerized software server that supports authenticated users and applications. A GEO/LEO link with management system can control hand-offs across wide area transports, thus augmenting the overall security and network management capability. Using ***Artificial / Machine Language*** (**AI/ML**) techniques across the network and edge cloud further improves efficiency and resiliency.

The impact of standalone 5G networks on defense applications is potentially game-changing, due to the high data rates and low latency of the networks. For instance, for aircraft maintenance on board a carrier or at an airfield, a mechanic looking at a jet engine can wear a pair of augmented-reality glasses that connect via 5G to display instructions of the steps to take and how to do each task. If the mechanic runs into a problem, a picture is taken that is quickly compared to thousands of pictures in a database to help diagnose the issue. Or, the mechanic can connect to a factory engineer and get instructions on solving a problem.

Other ways 5G deployments can improve base operations include 5G-connected robots that can patrol a runway collecting small bits of debris that could be sucked into jet engines, causing immeasurable damage. That is an analog job now executed by a person with a walkie-talkie driving around in a truck.

Similarly, imagine an airfield where, during a mission, airplanes land to refuel and then take-off every minute. Instead of managing the process with walkie-talkies and phones, the base can intelligently and safely automate when and where the refueling trucks should go, thanks to 5G connectivity.

Bases aren't the only place where 5G technology can be used to support operations; the battlefield can also benefit. For example, in a recent demonstration for the U.S. Army, a leading defense contractor attached 5G antennas to a fleet of small drones that flew above a truck convoy for several miles around a test range. With a human driving the lead truck, the drones in the air controlled a convoy of autonomous trucks that followed behind.

Obviously, the security of these standalone networks must be a top priority for the DoD and its commercial suppliers. Yet, security can be a challenge when connecting devices from many different manufacturers and users, especially when using commercial, off-the-shelf components.

To shore up security and build the necessary resiliency, these networks should be purpose-built, even when making use of commercial technologies and approaches. Moreover, the networks must be designed with what is called ***zero-trust architecture***, wherein every component on the network meets the requirements for role-based access control even when within the security perimeter.

The challenge is designing the network software in order for the components to work together seamlessly to support the wide range of devices that will be connecting to one another. For security, management data, user data and control data all run on different paths within the network. The software monitors everything and the networks self-correct to resolve most issues. In addition, the architecture must be compatible with the ***National Security Agency's Commercial Solutions for Classified*** (**CSfC**) standard.

These custom 5G networks will transform the nation's warfighting capabilities. And while the necessary 5G technology and commercial expertise are available today, the deployments must be designed specifically for the implementation; connect to wide area satellite networks for access and resiliency; and make use of managed network operations and automations for added assurance and operational excellence.

With the correct equipment, security, satellite connections and network management, standalone 5G technology will dramatically improve the capabilities of the U.S. military.

www.hughes.com

HUGHES

Dr. Rajeev Gopal

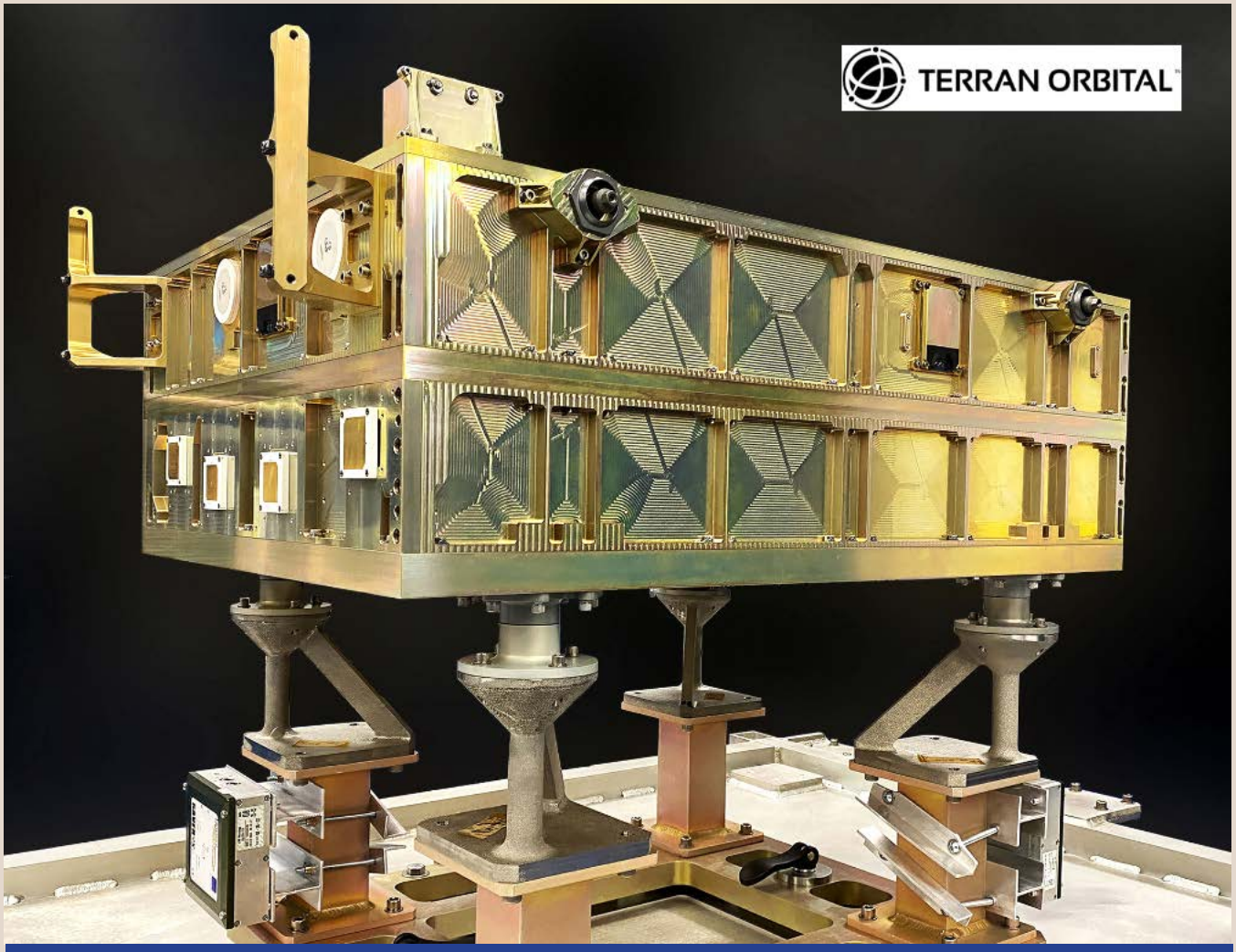
Dr. Rajeev Gopal, vice president, at Hughes Network Systems, LLC (HUGHES), leads the company's advanced engineering programs, developing innovative solutions for resilient and protected communications in defense applications. Dr. Gopal's work spans Low Earth Orbit (LEO) and Geostationary Orbit (GEO) High-Throughput Satellite (HTS) technologies, leveraging artificial intelligence (AI), machine learning (ML), cloud, and cyber security innovations. In more than 25 years at Hughes, Dr. Gopal has held a variety of leadership roles in satellite network systems engineering and software development. Most recently, he has focused on AI/ML, software-defined networking, 5G, and enterprise management architectures. Prior to joining Hughes, Dr. Gopal led automation projects for clinical and cancer research and development at CTIS.

Dr. Gopal holds several patents and has published more than 40 technical papers. A member of the IEEE 5G World Forum, he serves on the editorial board of Wiley's International Journal of Satellite Communications and Networking (IJSCN). Dr. Gopal earned a Doctor of Philosophy Degree in Computer Science from Vanderbilt University in Nashville, Tennessee, and a Bachelor of Engineering Degree in Electrical Engineering from the Birla Institute of Technology & Science (BITS) in Pilani, India. Consumers, businesses, governments and communities around the world benefit from the connected experiences enabled by Hughes technologies and services.

*To learn more, visit our website at **www.hughes.com** or follow us on **Twitter** @ **HughesConnects** and on **LinkedIn** at **www.linkedin.com/company/HughesConnects**.*

MULTI-BAND FLYAWAY TERMINAL MFT 1500 +++ SEVERE STORMS ++ GALE-FORCE WINDS +++ READY TO COMMUNICATE ANYTIME

Making Missions Possible



Terran Orbital Delivers First Bus to Lockheed Martin in Support of SDAs Transport Layer Tranche 0

Terran Orbital Corporation (NYSE: LLAP) has delivered the first of ten satellite buses to Lockheed Martin in support of the Space Development Agency's Tranche 0 Transport. ***Additional details via this infolink...***

U.S. Space Force Space Systems Command Awards SATCOM Prototype Contract To NIC4

NIC4, a subsidiary of Network Innovations, has been awarded a Service Provider Registry (SPR) prototype, a component of the SATCOM Enterprise Management and Control (EM&C). ***Additional details via this infolink...***

SPACE SYSTEMS COMMAND
— ACCELERATING THE FUTURE OF SPACE —

New SSC innovation and prototyping Delta combines acquisition, Prototyping, Testing and space operations to outpace the threat

Author: Space Systems Command

At Space Systems Command (SSC), "innovation" isn't just a trendy buzzword.

Colonel Joseph J. Roth

"*In order to outpace increasing threats from adversaries, innovation has to mean something*," said Col. ***Joseph J. Roth***, director, ***SSC Innovation & Prototyping***.

It can't just mean "*something new*," — it needs to be something that makes a fundamental, positive impact, enhancing U.S. national security in space, Roth said.

Innovation & Prototyping is one of the acquisition deltas within ***Space Systems Command***'s new ***Space Domain Awareness and Combat Power*** program executive office portfolio. The organization is supported by more than 650 government, military, and contractor personnel.

"*Our mission is to develop innovative experiments, on-orbit demonstrations and prototypes for SSC and the U.S. Space Force, so we can make informed decisions on the future architecture*," ***Roth*** said. "*We do the whole acquisition lifecycle for prototypes all in one organization from development, integration and on-orbit testing and operations with a great skill mix of acquirers, cyber professionals, testers, intel specialists and space operators. We are basically here to support SSC's program executive officers, the Air Force Research Lab's technology executive officer and other mission partners to drive innovation throughout the USSF. Our job isn't just to fly these cool experimental and prototype spacecraft. The ultimate goal is to transition those capabilities to the warfighter and end user.*"

After the Cold War, Roth said, the United States had the luxury of about 20 years where space was a peaceful environment, "*but our adversaries have seen the economic and military benefits space provides us and they're getting very bold and aggressive to take away that advantage. The reason we have the U.S. Space Force is not because it's a great organizational idea - although it was - it's because of the rising threat from China and Russia.*"

One of the unique elements of Innovation & Prototyping is that it is geographically dispersed: its headquarters are at ***Kirtland Air Force Base*** in *Albuquerque*, New Mexico, with operating locations at ***Schriever Space Force Base***, Colorado; ***Los Angeles Air Force Base***; and at ***NASA's Johnson Space Center*** in *Houston*, Texas.

Included under this new portfolio is the ***U.S. Department of Defense Space Test Program*** (**STP**), operating out of Kirtland and Houston.

Craig R. Lamb

"*STP is the longest-running space program in the U.S. Department of Defense and is the second-longest program in the DoD, after the B-52 program*," said ***Craig R. Lamb***, director, ***DoD Human Spaceflight Payloads***. "*Since its inception in 1965, the Space Test Program has sent 643 experimental scientific payloads into space since 1965 – many of them to the International Space Station. Ground-breaking technologies including GPS, Defense Support Program and Overhead Persistent Infrared were first tested and developed via the Space Test Program. We fly experiments and prototypes to test out concepts and burn down risk for the enterprise, but the key thing is we can go from an idea to a prototype that can launch in two years or less. You'll see the whole development cycle of this payload or prototype spacecraft, and then we can integrate it with the launch vehicle and get it on-orbit.*"

"*One of the big Vanguard experiments we are supporting is with the Air Force Research Lab (AFRL) and it's called Navigation and Technology Experiment No. 3 or NST-3*," ***Roth*** said.

The first two NTS experiments were done in the 1970s, and this experiment is testing what may become the first major upgrade to GPS technology in more than 40 years, using ***software-defined radios*** (**SDRs**) flying at ***Geosynchronous Orbit*** (**GEO**), instead of ***Medium Earth Orbit*** (**MEO**), paving the way for more resilient, multi-layer, PNT (***Position Navigation & Timing***) architecture. This experiment is flown from one of the 10 operations floors on at the ***Research, Development, Test & Evaluation Support Complex*** (**RSC**) at ***Kirtland AFB***.

"*Last summer, we just stood up the Rendezvous and Proximity (REPR) Satellite Operations Center, within the RSC, which contains a new ops floor which is multi-mission and multi-level security*," ***Roth*** said. "*This new ops center was designed with the operator in mind and we can fly a lot of different satellites at different classifications.*"

REPR is the USSF's only prototype satellite command and control operations center that operates 24 hours a day, and 7 days a week. The 5,930 square foot, $17 million state-of-the-art facility can accommodate more than 50 highly skilled operators and support personnel to command and control multiple missions simultaneously.

"*A key part of our mission is to provide enterprise enablers like the Long Duration Propulsive ESPA (LDPE) payload satellite,*" ***Roth*** added. "*LDPE uses the Evolved Expendable Launch Vehicle Secondary Payload Adapter Ring – it's a ring-shaped adapter between the launch vehicle and the launch vehicle payload that is converted into a fully functioning satellite with the ability to host six or more ESPA-class payloads or small satellites. This concept — originally developed by the Air Force Research Lab (AFRL) — takes advantage of the extra throw weight of launch vehicles and gives the Space Force a very flexible and modular system where we can plug a variety of payloads on this single spacecraft bus. We launched the first LDPE mission, LDPE-1, last December. It's on-orbit now and we're flying it out of the new REPR ops floor.*"

"*Our operations team is now used to the technology on the new REPR ops floor, so we're ready to take on the next missions for multi-mission ops on one floor,*" said Capt. ***Maggie Jones***, the assistant director of Operations for the Prototype Operations Branch. "*The architecture and logistics we have here on the ops floor is amazing. Our operators can easily and seamlessly switch between different information systems and different classification levels, so there is capacity for mission expansion in this facility. Right now we're getting into a groove operating the LDPE-1 mission, and this year we expect to add the LDPE-2, LDPE-3a, and Tetra-1 missions to the same ops floor.*"

The REPR Satellite Operations Center is supported by the ***Mobile Range Flight*** (**MRF**) at *Manzano Mountain*, which provides both in-garrison and deployable satellite command and control. The MRF employs and maintains a variety of mobile communications, command and control antennas as well as logistical capabilities allowing for global deployment and real-time reach-back to the RSC or other customer satellite operations centers.

These assets are used to augment access to space for R&D missions and to support test campaigns for future missions and ground command and control architectures. They are also critical assets in a time of increasing competition for use of the USSF's ***Satellite Control Network***.

Innovation & Prototyping also works to harness the creativity and new technology of emerging companies through organizations such as ***SpaceWERX*** and the ***Space Enterprise Consortium*** (**SpEC**), which is also part of the ***Space Domain Awareness and Combat Power*** portfolio. SpaceWERX, a subsidiary of the Air Force's ***AFWERX***, is one of the innovation arms of USSF and is modeled after the AFWERX unit, working to match commercial space industry technologies with military needs.

SpEC uses **OTA** (***Other Transaction Authority***), a DoD contracting mechanism) contracts to bridge the gap between military acquisitions and commercial space startups and small companies, particularly those who have never previously worked with the DoD. The consortium now has close to 800 members, 78% of which are non-traditional, and has executed more than $1 billion of total contract value over the past year, ***Roth*** said.

"*We're really trying to leverage the commercial marketplace right now*," ***Roth*** explained. "*There's a second Space Renaissance going on right now, with a lot of investment from venture capital and innovative startup companies that are doing amazing things. How can we leverage commercial industry to help us so that we can buy a product or service from them so that we are positioned to develop and build only those military unique capabilities that we have to within the U.S. Space Force?*"

Lt. Col. ***Dave Sampayan***, Materiel Leader of SSC's ***Innovation Developmen***t branch, added, "*We are challenging the paradigms of small satellite prototyping. Our Tetra program develops a series of small satellite technology risk-reduction experimental vehicles acquired under the Space Enterprise Consortium (SpEC) contract. Tetra prototypes will enable SSC to mature and transition new technologies and develop techniques, tactics, and procedures for space operations.*"

According to ***Adrian Wheelock***, AFRL/RVEP project lead, "*AFRL is excited to partner with SSC on the Tetra Program in order to test out multi-agent collaboration on up to three Tetra-5 spacecraft.*"

"*Additionally, Tetra-5 will be the first USSF on-orbit fluid transfer refueling demonstration*," said Maj. ***Krista Roth***, SSC's Tetra program manager.

"*Innovation & Prototyping is 'leading the charge' with our key mission partners to outpace the threat and we are now organized to maximize all these unique components to develop and deliver next-generation space capabilities more rapidly, more efficiently and more effectively than ever. Semper Supra!*" ***Roth*** said.

To ensure SSC continues to lead the way in space innovation and delivering cutting-edge capabilities to the warfighter, SSC has opened the Front Door program.

This initiative will serve as a one-stop portal to help companies connect with the correct SSC organizations to make it easier for them to connect and do business with the USSF.

Captain Robert "Murph" Busbee

"*SSC Front Door is a commercially facing initiative intended to help startups and non-traditional vendors navigate the labyrinth of the government acquisition process. It serves as the literal first step in connecting solutions to the appropriate opportunity and serves to help companies validate a product market fit within Space Systems Command.*"

"*For startups and non-traditionals, finding the way to connect with the appropriate DoD customer is difficult and costly both financially and manpower wise. The Front Door serves as the starting point to get connected with SSC, routed to an appropriate opportunity and connected with end users or government customers who would directly benefit from that startup's solution.* "-- Capt. ***Robert "Murph" Busbee***, chief, Atlas X business innovation, SSC

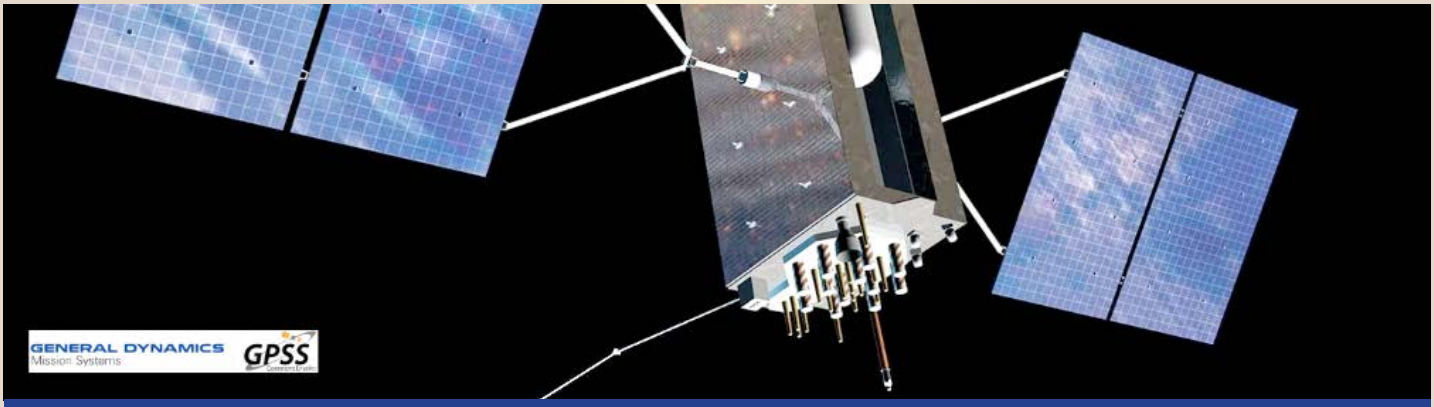
Contact Space Systems Command at ***SSC@spaceforce.mil*** follow on ***LinkedIn***.

Gilmour Space Wins Million$$ Contract To Build and + Launch Prototype Australian Defence Satellite

Australia's largest space company, Gilmour Space Technologies, has been selected to develop and launch a new sovereign surveillance satellite for the Department of Defence, as part of the government's $7 billion investment in new space capabilities. ***Additional details via this infolink...***

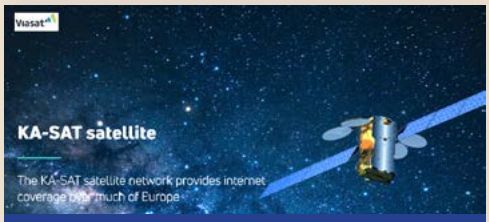
New Dept. Of The Air Force Assistant Secretary For Space Acquisition + Integration Named

Frank Calvelli has been sworn in as Assistant Secretary of the Air Force for Space Acquisition and Integration during a Pentagon ceremony, following his confirmation to the role by the U.S. Senate on April 28th.
Additional details via this infolink...



GPS Source Provides U.S. Army With Modernized Military GPS For Patriot Missile Systems

GPS Source, a subsidiary of General Dynamics Mission Systems, has delivered Assured Positioning, Navigation and Timing (APNT) systems with integrated Military GPS User Equipment (MGUE) receiver cards to the U.S. Army DEVCOM AvMC and PEO Missiles & Space — the initial systems will be used to evaluate the performance of Patriot missile batteries with modernized GPS hardware solutions.
Additional details via this infolink...



Viasat Donates Satellite High-Speed Internet To Ukrainian Refugees Via Partnership With The Košice Region of Slovakia

Viasat Inc. (NASDAQ: VSAT) and the Košice region, Slovakia, have partnered to provide free, high-speed internet to Ukrainian refugees in Eastern Slovakia using Viasat's proven, satellite-enabled, Community Internet system — Viasat Community Internet (VCI) sites are being installed across Eastern Slovakia in areas of greatest need for refugee connectivity.
Additional details via this infolink...

The 50th Expeditionary Signal Battalion (Enhanced) and 63rd Expeditionary Signal Battalion conducted a combined Large Scale Combat Operations (LSCO) communications exercise on Fort Bragg, North Carolina last year — the Lion Brigade achieved their goal of pushing the boundaries of a line of sight network to give the XVIII Airborne Corps and Fort Bragg redundancy and flexibility in a satellite communications denied environment. U.S. Army photo by Capt. Eric Messmer.

U.S. ARMY ADVANCES NEW COMMS NETWORK BASELINE

Authors: Claire Heininger and Amy Walker

From current support operations in Europe, to experimentation with emerging technologies at Project Convergence, leaders say it is clear that the U.S. Army must rely on an integrated, adaptive communications network to accomplish its missions.

"*The network is the backbone of everything we do, and data is our new ammunition*," said Lt. Gen. ***James Richardson***, Acting Commanding General of Army Futures Command, or AFC. "*All of the experimentation we are doing today is informing where we are going for the future.*"

The Army took an important step forward in delivering that network with the completion of the critical design review for ***Capability Set 23,*** or **CS23**. CS23 aligns more than 40 systems — from Soldier radios and satellite terminals to mission command software and network operations tools — into a system of systems that increases network resiliency, capacity and convergence. Informed by test and experimentation, while balancing capabilities' technical maturity, operational relevance and affordability, the critical design review is the acquisition event that finalizes the capability set design and authorizes limited production of CS23 systems.

"*Capability Set 23 is not a singular, monolithic program — it is a compilation of many programs that come together to provide an operationally useful capability*," said Maj. Gen. ***Robert Collins***, Program Executive Officer for Command, Control, and Communications — Tactical, or **PEO C3T**, the organization that leads the capability set process, along with AFC's Network Cross-Functional Team. "*It has been a tremendous collective team effort.*"

The Army's two-year network capability set delivery cycle is designed to enable consistent modernization driven by Soldier-led experimentation, commercial technology progress and overarching Army strategy — as well as ***Department of Defense*** initiatives such as Joint All-Domain Command and Control, or **JADC2**.

The Army is simultaneously fielding and developing several capability sets: **CS21** is fielding, **CS23** is in near-term development, **CS25** is in technology maturation and prototyping, and **CS27** design goals are being developed. While CS21 focused on Infantry formations at Brigade and below, Capability Sets 23 and 25 and beyond are increasingly targeting network modernization for mounted formations, as well as the Division level as the Army transitions to the Division as unit of action.

"*From an operational perspective, what you're really starting to see is how the Army wants to fight in the future be baked into each iteration of the Capability Sets*," said Lt. Gen. ***John Morrison*** Jr., Deputy Chief of Staff, G-6.

As the Army evolves to more data-centric, expeditionary and dispersed operations, Capability Set 23 will also deliver a foundational tactical data fabric that will provide commanders with relevant data at the point of need, as well as *Mission Partner Environment* data exchange capability that increases interoperability with coalition partners.

"*We need to create a data centric environment, a cloud environment, a backbone that we can reach to for our data and render that data to our commanders so they can make informed decisions*," said Brig. Gen. ***Jeth Rey***, Director of the Network CFT.

Capability Set 23 also increases integration of ***electronic warfare*** (**EW**), intelligence, fires and sustainment capabilities into the network. It introduces high-throughput, low-latency satellite communications through commercial services and non-traditional orbits to provide additional communications options for commanders. For ***Stryker*** formations such as the **2nd Cavalry Regiment** — which has participated throughout the CS23 design and assessment process and will be the first mounted unit equipped with CS23 — the new technology improves digital voice and data communications for mounted and dismounted operations.

"*This allows Soldiers to maintain their communications while inside the vehicles, and as they dismount the vehicles, they maintain that connectivity throughout their mission*," said ***Mindy Gabbert***, Deputy Project Manager for Capability Set Development at PEO C3T.

Capability Sets use synchronized Soldier touchpoints, developmental and operational tests and experiments, such as ***Project Convergence*** and ***CyberQuest,*** in order to fully vet and integrate systems so they are prepared for fielding. This ensures that input from the operational force, including lessons-learned from units supporting operations in Europe, is captured in the iterative design process.

"*Tactical level Soldier/operator feedback more clearly informs and defines capability requirements*," said Maj. ***Todd M. Klinzing-Donaldson***, head communications and network officer for the ***2nd Armored Brigade Combat Team***, ***3rd Infantry Division***, whose unit executed an Armor formation networking pilot earlier this year. "*Our unit experimented with three unique equipment sets, focused on creating a more robust upper tactical internet capability that would build a better common operational picture for the unit commander.*"

Feedback from the pilot event is already informing Capability Set 25, which will extend the network to Armor formations and continue to incorporate commercial solutions that enable the future network to be transport-agnostic, data-centric and underpinned by modernized security architecture and cyber resiliency. In parallel, the next step for Capability Set 23 will be a two-phase operational demo with the 2nd Cavalry Regiment that will take place staring in June, which will inform final CS23 fielding decisions to take place in Fiscal Year 2023.

COMMS ON THE MOVE

Designed, tested and proven for today's soldier communicator.

Field Configurable X-, Ku- & Ka-band

Multi-orbit LEO/MEO/GEO

Platforms for Land, Sea, Air

Open & Closed Loop Tracking

Flexibility that ensures resilient communications over satellite in battlefield environments

AvL TECHNOLOGIES

See our new COTM terminal at SOFIC ✦ Booth 229

DISA + U.S. ARMY RESET TEAMING EFFORTS TO SUPPORT 24/7 CYBER MISSION

Author: Renee Hatcher, Digital Communications, DISA Cyberspace Ops Directorate

Approximately 50 members of the Defense Information Systems Agency Army Reserve Element, a unit of reservist soldiers, met with DISA leadership at Fort George G. Meade in March to support DISA's no-fail mission to enable lethality in defense of our nation.

The Directorate, comprised of about 2,300 personnel in more than 10 countries and 13 states, hosted the soldiers for a day of operational briefings, leadership engagements and an awards presentation. The leadership engagement was the unit's first time back at DISA headquarters since before the COVID-19 pandemic.

"*We've proven over the last few years that we can maintain relationships virtually*," said ***Joe Wassel***, the head of DISA's Cyberspace Operations Directorate. "*But, when you are building relationships, getting knee-to-knee makes a big difference.*"

Throughout the day, soldiers practiced defending and protecting the DISA portion of the ***Department of Defense Information Network***. They shared skills and expertise in systems administration, technical support, network services, cyber defense infrastructure support, vulnerability management, and cyber defense analysis, which is a force multiplier for DISA.

The Defense Information Systems Agency's (DISA) Defense Information Systems Network (DISN) serves all branches of the military services, the executive branch, the combatant commands, 14 DoD agencies, and nine field activities.

"*This is a special group of folks who have already served our nation, have their own lives now, and yet they choose to keep serving*," said ***Joe Wassel***, head of DISA's Cyberspace Operations Directorate. "*Coming together with them was very powerful. It was important to me to make sure they know who we are, why we are here and what we're about.*"

DISA Army Reserve Element training coordinator, Master Sgt. ***Shakira Hicks***, joined the Army in 2004 and has been with the unit since March 2016. Hicks ensures that soldiers are prepared for the *Cyber Network Defenders course* and that they continue to build their skillset. She wanted to be part of DISA to align her military experience with her civilian career in cybersecurity as an information systems security engineer lead/technical program manager.

Army Lt. Col. Kevin Sturm, commander of the DISA Army Reserve Element, presents Joe Wassel with the first of ARE's newest coin during the unit's drill weekend at agency headquarters in March. Photo by Eric Glisson.

"*DISA has a lethal cyber capability in the Army Reserve Element that has not yet been realized or used*," *Hicks* said. "*I am looking forward to seeing that change and having our soldiers fully engaged in the mission.*"

Some areas where the DISA Army Reserve Element can help the agency continue to meet requirements include preparing secure mobile devices to get them into the field faster, configuring and maintaining internet access points for all of DOD, performing full spectrum cyber analysis to ensure cloud security and to harden networks.

Considering the pace at which cyber technology advances, another way the soldiers plan to support DISA's no-fail mission is to make sure agency playbooks don't get stale. Tactics and procedures written this year might not be relevant next year. Keeping agency playbooks and checklists operationally relevant to DISA's fight is critical to how it operates. This talent-heavy organization is uniquely qualified to help the agency standardize and train the force within cyberspace operations.

The tactical nature of DISA Army Reserve Element's contributions align with the strategic vision of the DISA director to prioritize command and control, and always be ready to fight.

SPACEBRIDGE

CONNECTING OUR MILITARY TO ITS MISSIONS

ASAT II™
Tactical , BLoS
HTS System

For over 30 years, SpaceBridge has striven to provide C4I over SATCOM connectivity by being an innovator, leader, and trusted provider of bold tactical solutions in the military ground segment Satellite technologies.

We live on the cutting edge of what's possible, challenging ourselves to provide products and services that rise to the occasion. In a world of mounting unconventional threats, there is no room for failure or compromise.

We are dedicated to the exploration and implementation of new communication technologies that provide our armed forces with ultra high-performance satellite connectivity products that boast the best security, and highest availability.

Recognized by major players such DISA, SpaceBridge will continue to offer high-throughput solutions at exceptional value.

Contact us today to learn how we can connect you to your beyond line of sight missions.

SpaceBridge.com | info@SpaceBridge.com | +1.514.420.0045
USA | CANADA | LATAM | BRAZIL | EMEA | APAC

GOVERNMENT SATELLITE REPORT

Commercial X-Band managed Services the key to on-demand resilient comms

Author: Ryan Schradin, Executive Editor, Government Satellite Report (GSR)

At a recent Mitchell Spaceflight Institute Spacepower Forum, the Chief of Space Operations for the U.S. Space Force, Gen. John W. "Jay" Raymond, explained that 2022 would be the year that the U.S. Department of Defense (DoD), "…will begin our pivot significantly to a resilient architecture…" Gen. Raymond also explained his intention to shift the U.S. satellite architecture from "… a handful of exquisite capabilities that are very hard to defend to a more robust, more resilient architecture by design."

But why is there such a significant focus on satellite architecture resiliency that it's one of the ***U.S. Space Force***'s largest priorities for the coming year? One only has to look at some of the recent events involving satellite communications in Europe for an answer.

Today's advanced military platforms and systems are all network and software enabled. These systems require connectivity to function as intended and meet warfighter requirements. And satellite is the best way to provide that connectivity in geographic locations where terrestrial networks are either denied, degraded, untrusted, or insecure — like many of the places where the military operates.

But ***satellite communications*** (**SATCOM**) deliver more than advanced IT capabilities to the warfighter. SATCOM is instrumental for ***intelligence, surveillance, and reconnaissance*** (**ISR**), and ***situational awareness*** (**SA**). It's also the main conduit for basic communications services in austere environments.

By distributing military signals over a wide ecosystem of military and commercial satellite resources, it becomes incredibly difficult for adversaries to identify which satellites are carrying military communications and deny them through jamming or kinetic attack.

The near-peer adversaries that America and its coalition partners are confronted with today know that satellite is fundamental and mission-critical for so many military operations — they'll do anything to deny access to the satellite services that are both a basic necessity and a force-multiplier.

We've seen this play out in real-time in the current situation in Eastern Europe. As fighting began, ***one of the first casualties*** was connectivity and communications from terrestrial networks. Then, the satellite service that was used to fill that communications void ***was almost immediately denied by the adversary***.

Regardless of whether this communications disruption was meant to hinder military communications, capabilities, and coordination — or simply to cause confusion and a lack of reliable information for civilians — is secondary. It is evidence that denying SATCOM networks and infrastructure is now a large part of warfare — and will remain so into the future. This is why the military now considers space an austere environment and a warfighting domain.

Augmenting ***military satellite communications*** (**MILSATCOM**) with ***commercial satellite communications*** (**COMSATCOM**) has long been considered a solution for increasing resiliency. By distributing military signals over a wide ecosystem of military and commercial satellite resources, it becomes incredibly difficult for adversaries to identify which satellites are carrying military communications and deny them through jamming or kinetic attack.

Today's advanced military platforms and systems are all network and software enabled. These systems require connectivity to function as intended and meet warfighter requirements — satellite is the best way to provide that connectivity.

But what about coalition partners and allied nations with no readily available, purpose-built, MILSATCOM architecture? How can they get immediate access to resilient, military-grade satellite communications should a threat arise? These are exactly the types of situations that a new generation of commercial X-band satellite solutions was made for.

X-BAND ON DEMAND

X-band and military Ka-band satellite communications have long been trusted by the ***U.S. Department of Defense*** (**DoD**) because of their reliability and

U.S. Marines set up a satellite dish at Joliet Army Training Area in Elwood, Illinois. (Photo by: Marine Corps Lance Cpl. Preston Morris. The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

resilience. As ***Patti Aston***, a Senior Director at ***SES Government Solutions***, recently explained to the ***Government Satellite Report,*** *"…X-band [is] considered more reliable – or more mission-assured for critical operations. And when the lives of tactical operators and warfighters are on the line, the military doesn't want to take the chance that there could be interference or signal loss."*

Access to commercially-delivered X-band and military Ka-band satellite capacity has increased more recently with the introduction of services such as ***tactiXs*** — an end-to-end, managed service that delivers secure, non-preemptible, X-band capabilities to customers on an on-demand basis.

These managed services enable governments and militaries without existing, purpose-built, military satellite resources to quickly and easily gain access to resilient, reliable X-band and military Ka-band satellite communications at a moment's notice. There is no special or proprietary hardware necessary to access the service and no ground infrastructure necessary. COTS X-band terminals are used to gain access. Governments and militaries can simply acquire the satellite services they need — for a specified period of time or for a prescribed amount of data throughput — and begin using them immediately.

The near-peer adversaries that America and its coalition partners are confronted with today know that satellite is fundamental and mission-critical for so many military operations. And they'll do anything to deny access to the satellite services that are both basic necessity and force-multiplier.

"[tactiXs] gives the military user tremendous flexibility and agility. They now have on-demand access to X-band capabilities on an as-needed basis. And they don't have to buy the capacity on a long-term basis," ***Aston*** explained. *"Since [tactiXs] is a managed service, they also don't have to provide the ground infrastructure. The ground stations and teleports – everything necessary to enable access – is provided for them."*

Resilient SATCOM is as essential to today's military as any weapons system or platform being issued to — or deployed with — the warfighter. It provides the connectivity for next-generation, network-enabled systems. It enables ISR and situational awareness. It becomes the backbone of even the most basic of communications services when terrestrial networks are denied.

Commercial X-band managed services can ensure that the connectivity governments and militaries need is available immediately. They also can deliver the resiliency and reliability necessary for mission-critical communications.

For additional information on ***tactiXs***, ***select this direct infolink...***

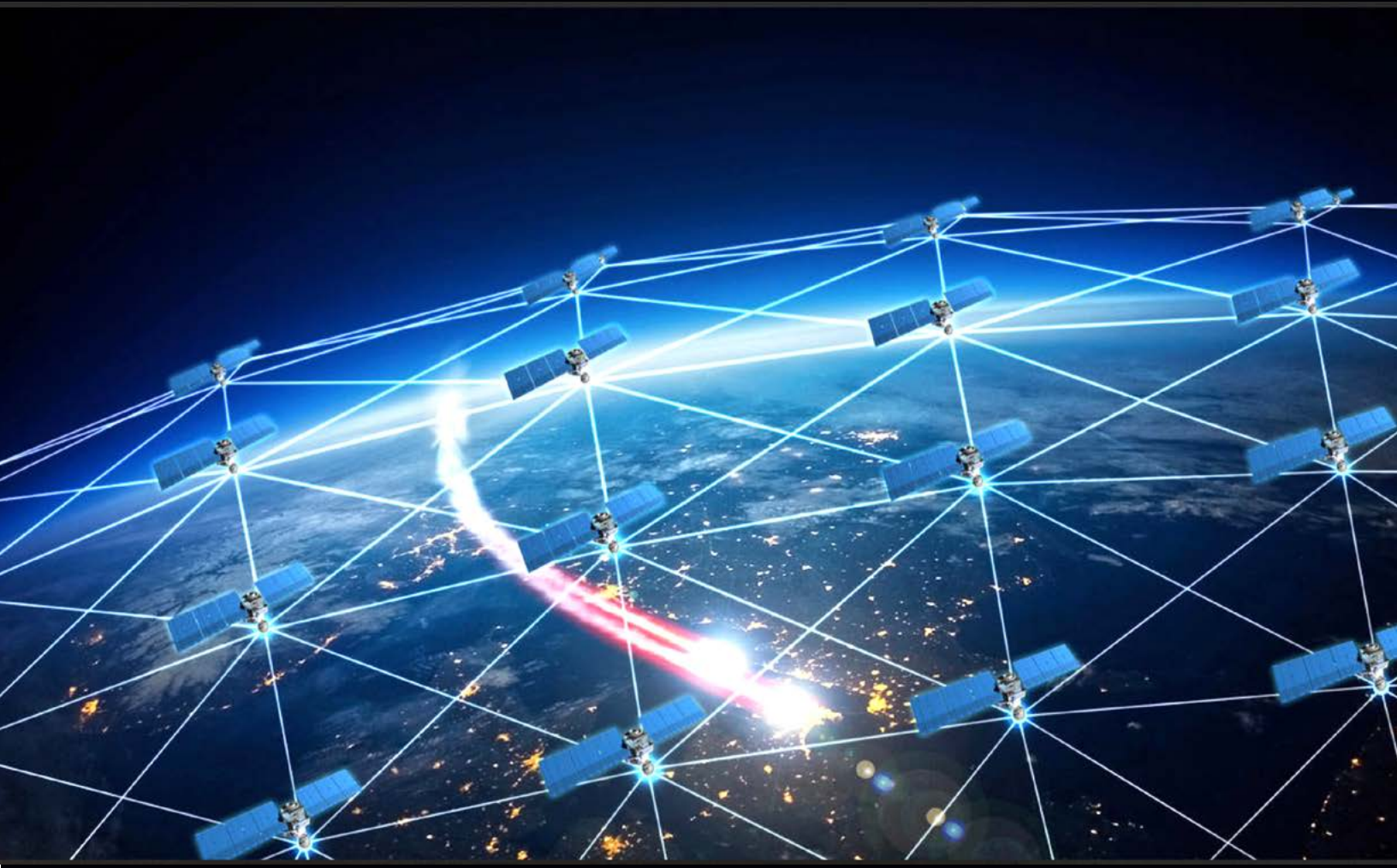
SES GS, Network Innovations, and GovSat, a public-private joint venture between the Government of Luxembourg and SES, recently announced that the organizations would be partnering to introduce tactiXs, a new X-band and military Ka-band volume-based managed service that will make mission-specific, military-band satellite capabilities available to the U.S. Government and its Alliance partners.

This article first on GovSat and is reprinted with permission from ***SES GS and Government Satellite Report****.*

Ryan Schradin is the Executive Editor of GovSat Report. A communications expert and journalist with more than a decade of experience, Ryan has edited and contributed to multiple popular online trade publications focused on government technology, satellite, unified communications and network infrastructure. His work includes editing and writing for the GovSat Report, The Modern Network, Public Sector View, and Cloud Sprawl. His work for the GovSat Report includes editing content, establishing editorial direction, contributing articles about satellite news and trends, and conducting both written and podcast interviews. Ryan also contributes to the publication's industry event and conference coverage, providing in-depth reporting from leading satellite shows.

ADDRESSING AN ACCELERATING THREAT ENVIRONMENT: MISSILE WARNING + DEFENSE

Author: L3Harris Editorial



As quickly as technologies advance worldwide, global threats continue to rapidly increase. Missile capabilities have expanded, with continued and accelerated development of long-range and ballistic missiles. Of increasing concern, however, is the development of a new generation of missile technology.

Within this new generation of missile technology exists the potential for ***hypersonic glide vehicles***, which are highly maneuverable and travel at speeds exceeding Mach 5, making them extremely difficult to detect.

"*Hypersonic glide vehicles do not follow the same deterministic trajectory as preceding ballistic technology*," said ***John Holder***, ***Missile Warning and Defense*** (**MWD**) Chief Systems Engineer, L3Harris.

Previous defense architectures, which counted on being able to predict where the missile would land based upon initial launch trajectory information, are no longer viable options.

"*Beyond their high maneuverability, low heat signatures during various phases of flight make the missiles very hard to detect through the atmosphere from space*," ***Holder*** continued.

Developing an architecture and technology that address these threat capabilities (*both current and projected*) has been the primary focus of the L3Harris MWD team.

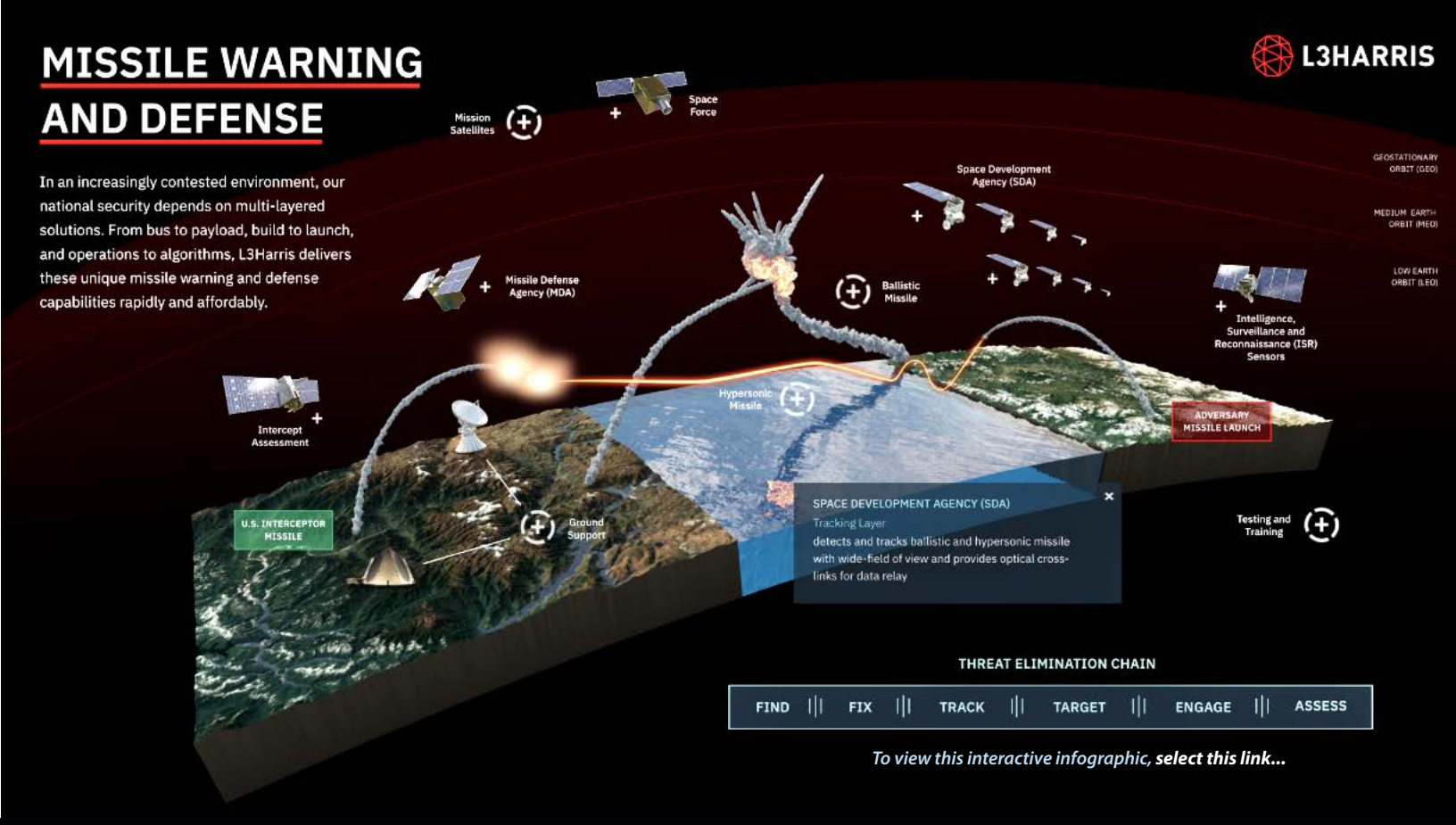
MISSILE WARNING AND DEFENSE

L3Harris has an extensive, 60-year history in the design, build and test of both geosynchronous and LEO weather and climate instruments. Among these are the ***Advanced Baseline Imager*** (**ABI**) instruments, which are the most sophisticated meteorological imaging instruments ever built for operational weather forecasting. In fact, they are the only weather instruments that provide flexible, custom scanning that is configurable on-orbit.

"*We observed that these instruments had the sensitivity and performance capability of detecting launches from orbit*," ***Holder*** said. "*This led to significant company investment to develop accompanying on-orbit algorithms that supported detection and tracking of these missiles through the multiple stages of flight and potential atmospheric conditions.*"

The MWD system architecture contains many overlapping layers and phases that support different functionality throughout the various stages of missile flight. The system begins with initial detection (*launch*), extends through tracking, and finally concludes with targeting/engagement (*fire control*) prior to the missile reaching its intended target during its terminal phase.

"*L3Harris' recent focus has been on the detection and tracking phases of the MWD system architecture, identifying key technology required to support these critical functions*," ***Holder*** said.



To view this interactive infographic, ***select this link...***

Overall, L3Harris has identified four key requirements that are guiding the technology being developed to effectively support these targeted phases of the MWD system:

- ***Continuous global coverage, as a threat could be from anywhere at any time***
- ***High sensory sensitivity and dynamic range, as targets can be dim to very bright throughout flight***
- ***Real-time, on-board processing that is capable of immediately detecting and tracking threats under a multitude of different geometries and atmospheric conditions***
- ***Open design architecture that supports rapid evolving performance in a schedule-driven, cost-constrained environment***

"*Mitigating emerging threats is our number one priority,*" ***Holder*** said. "*We need to respond quickly and ensure that our solution is cost-effective and easily proliferated, while in an open architecture that will allow the design to evolve easily as lessons are learned and threats evolve.*"

MISSION TECHNOLOGY

L3Harris continues to dedicate and prioritize investments to address MWD architecture and technology needs. Upon completion of the on-orbit algorithm performance demonstration, further investments were initiated for the development of a ***proliferated low earth orbit*** (**PLEO**) technology centered around the MWD algorithm.

"*The focus of this effort is to develop a common architecture that supports two different L3Harris capabilities that directly address the needs of the targeted MWD system phases, detection and tracking,*" ***Holder*** said. "*These capabilities can provide a strong performance against both current and emerging threats.*"

In December of 2021, the ***SDA*** approved L3Harris' missile-tracking satellite design at the ***Tranche 0 Critical Design Review*** (**CDR**), affirming L3Harris' satellite build plans and technology.

The CDR was successfully held less than a year from the original contract award and resulted in ***Authorization to Proceed*** (**ATP**), which is unprecedented for an ***electro optical*** (**EO**) ***infrared*** (**IR**) sensor of this complexity. L3Harris was commended for its commitment to supporting the critical needs of the MWD system and sustaining such a rapid development pace to address these present and evolving threats.

"*Common architectures are the cornerstone of multiple payload designs to combat this threat on current and future programs,*" ***Holder*** said. "*The success experienced by the SDA Tranche 0 Tracking team is a testament to this approach.*

"*From the use of heritage L3Harris technologies and real-time detection algorithms to incorporation of common interfaces, the commitment to IR&D in these areas will continue to deliver common payload technologies that meet the evolving needs of our customers within the rapid development timelines required to keep pace with this emerging threat.*"

EXPANDING THREAT

L3Harris understands that in this age of new generation missile technology, precision tracking is key and can only be made possible through advanced satellite technology. As threats grow daily, MWD technologies are ever-more important in addressing shifting needs in the space domain.

L3Harris is invested in amplifying MWD capabilities through dedicated development efforts and the expansion of a dedicated workforce at its recently opened Fort Wayne facility and expanded satellite production site in Central Florida. These investments build upon a legacy of success to address the rapid evolving threats of today.

www.l3harris.com/

L3HARRIS™
FAST. FORWARD.

FOCUS: VIASAT GOVERNMENT SYSTEMS

A Briefing With Joel Babbitt, Army Business Development

Authors: Viasat newsroom team

The U.S. military is in the midst of a dramatic transformation.

As the Joint Chiefs of Staff noted in the *2018 National Defense Strategy*, the speed and breadth of technological transformation "*risks eroding the conventional overmatch to which our nation has grown accustomed.*"

U.S. military advantage, and the technological superiority upon which it has rested, the strategy stated, is now contested by great-power adversaries in every domain — land, sea, air, space, and cyberspace.

U.S. military dominance is no longer a certainty in any domain, in many regions, and at most times. This is increasing the chances that an adversary's actions may force the U.S. military and its allies into a war — be it a regional war or global, a limited war, or total.

To retain its battlefield dominance and maintain global stability, the strategy stated, the U.S. military needs to "*gain and maintain information superiority*" — the ability to gather, analyze, and present to commanders anywhere in the world the data they need to make better decisions — and do it faster than the enemy. That means identifying targets, confirming no friendlies or civilians are in the target area and delivering munitions — quickly.

That's where ***Viasat*** comes in: providing interoperable technologies, services, and expertise that facilitate stitching together that global decision chain in a resilient and secure fashion, boosting information superiority for the U.S. military — even in the intensity of battle that a great-power war would bring.

Traditionally, U.S. forces have cobbled together that capability between stove-piped service technologies, explained retired U.S. Army Colonel ***Joel Babbitt***, who recently joined ***Viasat Government Systems*** as vice president for Army business development and strategy.

"*You have a guy with a map and a pencil, managing two radios, a computer, and multiple targeting devices. It's like playing a cello in a marching band or dragging your office into the middle of a battle*," Babbitt said. "*He's primarily using voice communications, both with higher headquarters and with the forward observer on the ground who's got eyes on the target. The forward observer then has to help the pilot to identify a target.*"

Joel Babbitt

This, he says, makes targeting a process ripe for improvement.

Forward observers use a "*nine-liner*" standardized communications format to transmit — via voice communications — the location of the target and nearby friendly forces, once it's been manually gathered and collated.

This process, however, can present risks to warfighters requesting ***close air support*** (**CAS**).

PULLING THE THREADS TOGETHER

Fortunately, advanced U.S capabilities, enabled by Viasat's game-changing technology, are automating and making the process much less prone to error. Capabilities now include tools such as the ***Tactical Assault Kit*** (**TAK**), an open-source, geolocation software package built to enable situational awareness and tracking of friendly forces.

Then there's ***Tactical Radio Application eXtension*** (**TRAX**), a software package that creates a common data layer that enables stove-piped data sources and applications to communicate and share data across networks via multiple communications pathways.

Viasat's network and tactical data link expertise is the thread that pulls these capabilities together to improve safety for U.S. warfighters on the tactical edge.

"*Using Viasat's Link-16 capabilities, Special Operations Forces reduced that 15-30 minute process (to call in CAS) down to 15-30 seconds,*" Babbitt said. "*It has become seamless, it all works together to produce this common operational picture that allows immediate, accurate responses to battlefield threats.*"

Link 16 is the foundational network that delivers this critical, real-time situational awareness — a secure, resilient, and interoperable communications protocol that joins these capabilities together, enabling that encrypted global decision-chain for identifying and engaging threats to be used across services and among allies.

Link 16 terminals are now deployed on Air Force, Navy, USMC, and Army attack aircraft and widely available for other services.

"*Almost all of our allies use it,*" said Babbitt, "*In coalition operations (like in Iraq or Afghanistan) we are fighting wars on Link 16.*"

Viasat's development of the first handheld Link 16 radio for ground soldiers, known as ***Battlefield Awareness and Targeting System – Dismounted*** (**BATS-D**), improved situational awareness and CAS capabilities (*photo to the right*).

Viasat is still driving innovation in Link 16 working with the ***Air Force Research Laboratory*** (**AFRL**) to build the first ***XVI*** satellite, a Link 16 enabled LEO satellite that will, for the first time, turn Link 16 connectivity into ***Beyond Line of Sight***, or **BLOS**. This kind of innovation offers an immediate impact for warfighters.

EXPANDING LINK 16 ADOPTION

Currently, the Army only routinely deploys Link 16 capabilities to **Patriot** missile batteries and **Apache** helicopter squadrons, Babbitt said. "*We need to get Link 16 capability into the hands of forward observers,*" Babbitt stated. "*We need to get the Air Defense Artillery community fully integrated, and we need every aircraft to have these capabilities. Anywhere there's a TAK server, like at a brigade-level command post, they need it so that they can see what assets are coming and going across the battlespace. The ability to see that complete picture — all the assets, in real time and to coordinate fires — is a key enabler of modern battle.*"

Evangelizing for Link 16 is part of Babbitt's new job, which he says boils down to a simple mission statement: "*I help Viasat meet the Army's needs.*"

The company has a long history with the U.S. Army and continues to partner in developing cutting-edge capabilities to support mission operations. For instance, last year, Viasat demonstrated through-rotor, broadband satellite connectivity on an Army National Guard **UH-60** helicopter.

Babbitt is the ideal person to make those connections between the Army and Viasat. After 32 years in the service, he jokes, "*I speak fluent Army,*" adding that he's only slowly learning to "*speak civilian*" again.

"*I understand the context in which our Army customers are operating, the processes that they have to go through,*" he said. "*I understand what enables them, and my job is to help us at Viasat understand that too. Working together with the patriots that we are serving, we can thus enable America's next generation of battlefield dominance.*"

THE JADC2 VISION

To achieve that dominance, the National Defense Strategy lays out a futuristic vision of a totally networked force enabling a digitally managed battlefield.

This vision, ***Joint All-Domain Command and Control,*** or **JADC2**, proposes a U.S. military able to connect sensors with shooters so that frontline troops and commanders in the rear echelon can share the same "*God's Eye*" view — comprehensive situational awareness to improve effectiveness and reduce errors.

"*JADC2 is a construct, a vision of the Joint Chiefs,*" Babbitt said, "*to get those two C's in JADC2, command and control, you need the infrastructure, and you need the networks, which are built by each of the services.*"

The Army's exercise to unite that infrastructure is called ***Project Convergence.***

"*It's going to take collaboration across services and industry to bring the vision of seamless integration to life,*" Babbitt noted. "*And we here in industry are best positioned to help the various branches of the military work together, because they're all our customers.*"

JADC2 is about the development and integration of technologies to enable the data sharing to deliver information across domains. However, this integration requires agreement on standards to ensure the technologies are interoperable.

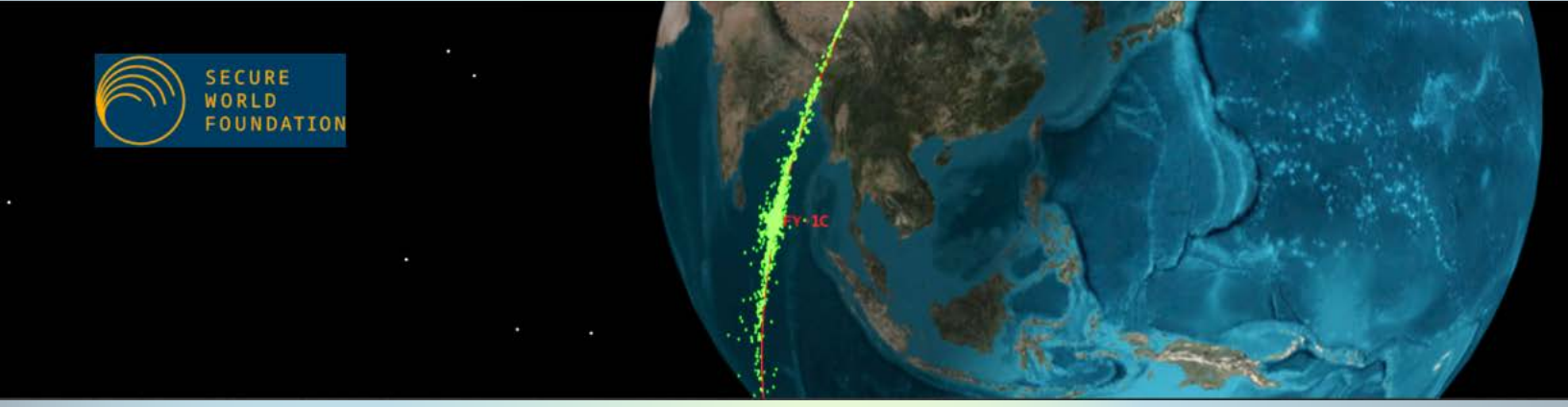
Facilitating interoperability is going to be the key to JADC2. For the Army, creating this data fabric — a transport layer through which information can be seamlessly moved from network to network — is critical to delivering the resilient capability needed to support missions and overcome adversaries.

For his part, Babbitt is looking forward to the challenge.

"*We believe we can provide the infrastructure, as well as the networking expertise and partnership to create interoperability among Army, joint, and coalition services,*" he said. "*And we're working toward that goal every day for our Viasat customers all over the world.*"

www.viasat.com

This article was first published on the Viasat Newsroom
www.viasat.com/about/newsroom/blog/



A SECURE WORLD FOUNDATION EXECUTIVE SUMMARY GLOBAL COUNTERSPACE CAPABILITIES REPORT

Space security has become an increasingly salient, policy issue

Authors: Dr. Brian Weeden, Director of Program Planning, and, Victoria Samson, Washington Office Director

The space domain is undergoing a significant set of changes. A growing number of countries and commercial actors are getting involved in space, resulting in more innovation and benefits on Earth, but also more congestion and competition in space.

From a security perspective, an increasing number of countries are looking to use space to enhance their military capabilities and national security. The growing use of, and reliance on, space for national security has also led more countries to look at developing their own counterspace capabilities that can be used to deceive, disrupt, deny, degrade, or destroy space systems.

The existence of counterspace capabilities is not new; however, the circumstances surrounding them are — today there are increased incentives for development, and potential use, of offensive counterspace capabilities. There are also greater potential consequences from their widespread use that could have global repercussions well beyond the military, as huge parts of the global economy and society are increasingly reliant on space applications.

Te complete report compiles and assesses publicly available information on the counterspace capabilities being developed by multiple countries across five categories: ***direct-ascent***, ***co-orbital, electronic warfare*** (**EW**), ***directed energy***, and ***cyber***. The report assesses the current and near-term future capabilities for each country, along with their potential military utility.

The evidence shows significant research and development of a broad range of destructive and non-destructive counterspace capabilities in multiple countries. However, only non-destructive capabilities are actively being used in current military operations. The following provides a more detailed summary of each country's capabilities.

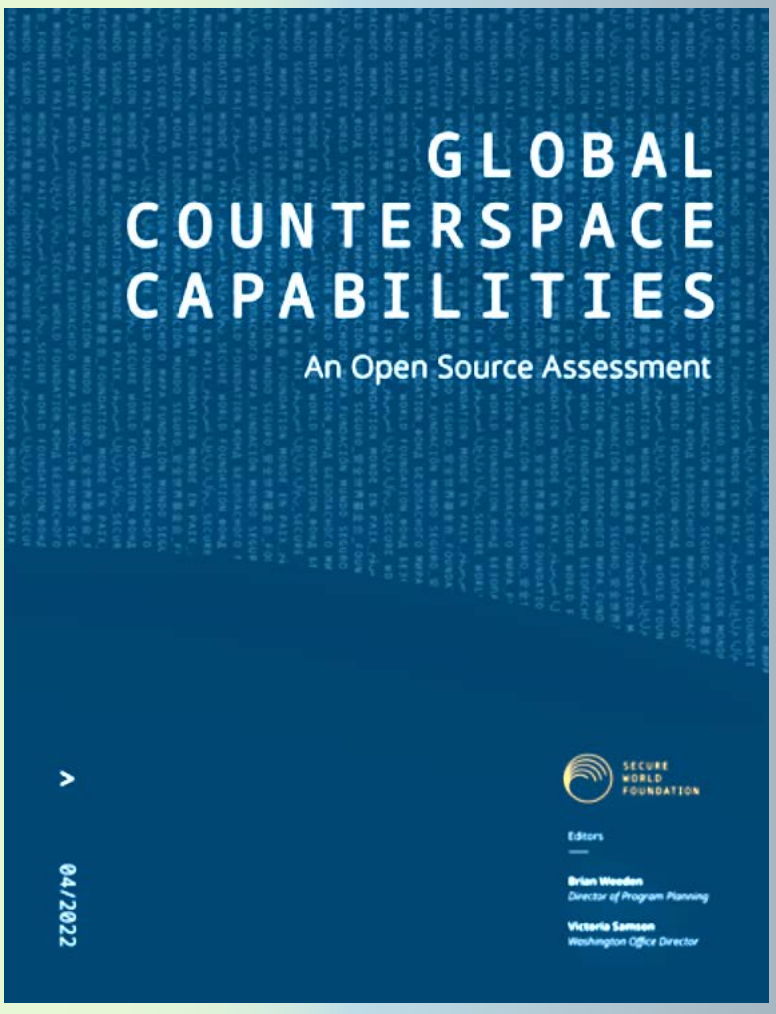
THE UNITED STATES

The United States has conducted multiple tests of technologies for r***endezvous and proximity operations*** (**RPO**) in both ***Low Earth Orbit*** (**LEO**) and ***Geostationary Earth Orbit*** (**GEO**), along with tracking, targeting, and intercept technologies that could lead to a co-orbital ASAT capability. These tests and demonstrations were conducted for other non-offensive missions, such as missile defense, on-orbit inspections, and satellite servicing, and the United States does not have an acknowledged program to develop co-orbital ASAT capabilities.

However, the United States possesses the technological capability to develop a co-orbital ASAT capability in a short period of time. While the United States does not have an operational, acknowledged ***direct ascent anti-satellite*** (**DA-ASAT**) capability, it does have operational, midcourse, missile defense interceptors that have been demonstrated in an ASAT role against a low LEO satellite.

The United States has developed dedicated DA-ASATs in the past, both conventional and nuclear-tipped, and possesses the ability to do so, should it decide to do so, in the near future. The United States has an operational EW offensive counterspace system, the ***Counter Communications System*** (**CCS**), which is deployed globally to provide uplink jamming capability against geostationary communications satellites.

The United States has also initiated a program called ***Meadowlands*** to upgrade the CCS capabilities. Through its ***Navigation Warfare*** program, the United States has the capability to jam the civil signals of ***global navigation satellite services*** (***GNSS***) within a local area of operation to prevent their effective use by



adversaries and has demonstrated such in several, military exercises. The United States likely could jam military GNSS signals as well, although the effectiveness is difficult to assess, based on publicly available information. The effectiveness of U.S. measures to counter adversarial jamming and spoofing operations against military GPS signals is not known.

Over the past several decades, the United States has conducted significant research and development on the use of ground-based, high-energy lasers for counterspace and other purposes. We assess that there are no technological roadblocks to the United States operationalizing them for counterspace applications. With its ***Satellite Laser Ranging*** (**SLR**) sites and defense research facilities, the United States possesses low-power laser systems with the capability to dazzle, and possibly blind, ***Earth Observation*** (**EO**) imaging satellites. However, there is no indication that these potential high or low power capabilities have been operationalized.

There is no public evidence that the United States has space-based, ***directed energy weapons*** (**DEW**) capabilities. However, the ***Missile Defense Agency*** (**MDA**) is planning to conduct research into the feasibility of space-based DEW for defending against ballistic missiles. If developed, these systems may have a capability against other orbiting satellites and, depending on their target acquisition and tracking capabilities, may be considered de facto anti-satellite systems.

The United States currently possesses the most robust ***space situational awareness*** (***SSA***) capabilities in the world, particularly for military applications. U.S. SSA capabilities date to the beginning of the Cold War and leverage significant infrastructure that was developed for missile warning and missile defense. The core of its SSA capabilities is a robust, geographically dispersed network of ground-based radars and telescopes and space-based telescopes.

The United States is investing heavily in upgrading its SSA capabilities by deploying new radars and telescopes in the Southern Hemisphere, upgrading existing sensors and signing SSA data sharing agreements with other countries and satellite operators. The United States still faces challenges in modernizing the software and computer systems used to conduct SSA analysis and is increasingly looking to leverage commercial capabilities.

The United States has had established doctrine and policy on counterspace capabilities for several decades, although not always publicly expressed. Most U.S. presidential administrations since the 1960s have directed or authorized research and development of counterspace capabilities, and in some cases greenlit testing or operational deployment of counterspace systems. These capabilities have typically been limited in scope and designed to counter a specific military threat, rather than be used as a broad coercive or deterrent threat.

The U.S. military doctrine for space control includes ***defensive space control*** (**DSC**), ***offensive space control*** (**OSC**), and is supported by SSA. The United States recently underwent a major reorganization of its military space activities as part of a renewed focus on space as a warfighting domain.

Since 2014, U.S. policymakers have placed increased focus on space security, and have increasingly talked publicly about preparing for a potential "*war in space*." This rhetoric has been accompanied by a renewed focus on reorganizing national security space structures and increasing the resilience of space systems. This has culminated in the reestablishment of ***U.S. Space Command*** (**USSPACECOM**) and the creation of the ***U.S. Space Force*** (**USSF**), which assumed the responsibilities of U.S. Strategic Command for space warfighting, and ***Air Force Space Command*** (**AFSPC**) for operating, training, and equipping of space forces, respectively.

To date, the mission of these new organizations is a continuation of previous military space missions, although some have advocated for expanding their focus to include cislunar activities and space-to- ground weapons. It is possible that the United States has also begun developing new offensive, counterspace capabilities, although there is no publicly available policy or budget direction to do so.

There are recent budget proposals to conduct research and development of space-based missile defense interceptors and DEW that could have latent counterspace capabilities. The United States also continues to hold annual space wargames and exercises that increasingly involve close allies and commercial partners.

This Secure World Foundation report also includes analysis of Russian, Chinese, Indian, Australian, French, Iranian, Japanese, North Korean, South Korean, and United Kingdom capabilities as well as reports on cyber capabilities of several nations.

Read the entire Secure World Foundation report ***by accessing this direct link...***

swfound.org

Secure World Foundation (SWF) is a private operating foundation that promotes cooperative solutions for space sustainability and the peaceful uses of outer space. The Foundation acts as a research body, convener, and facilitator to promote key space security and other space-related topics and to examine their influence on governance and international development.

Dr. Brian Weeden

Author Dr. Brian Weeden is the Director of Program Planning for Secure World Foundation and has more than two decades of professional experience in space operations and policy. Dr. Weeden directs strategic planning for future-year projects to meet the Foundation's goals and objectives, and conducts research on space debris, global space situational awareness, space traffic management, protection of space assets, and space governance. Dr. Weeden also organizes national and international workshops to increase awareness of and facilitate dialogue on space security, stability, and sustainability topics. He is a member and former Chair of the World Economic Forum's Global Future Council on Space Technologies, a former member of the Advisory Committee on Commercial Remote Sensing (ACCRES) to the National Oceanic and Atmospheric Administration (NOAA), and the Executive Director of the Consortium for Execution of Rendezvous and Servicing Operations (CONFERS). Prior to joining SWF, Dr. Weeden served nine years on active duty as an officer in the United States Air Force working in space and intercontinental ballistic missile (ICBM) operations. As part of U.S. Strategic Command's Joint Space Operations Center (JSpOC), Dr. Weeden directed the orbital analyst training program and developed tactics, techniques and procedures for improving space situational awareness.

Victoria Samson

Author Ms. Victoria Samson is the Washington Office Director for Secure World Foundation and has nearly 25 years of experience in military space and security issues. Before joining SWF, Ms. Samson served as a Senior Analyst for the Center for Defense Information (CDI), where she leveraged her expertise in missile defense, nuclear reductions, and space security issues to conduct in-depth analysis and media commentary. Prior to her time at CDI, Ms. Samson was the Senior Policy Associate at the Coalition to Reduce Nuclear Dangers, a consortium of arms control groups in the Washington, D.C. area, where she worked with Congressional staffers, members of the media, embassy officials, citizens, and think-tanks on issues surrounding dealing with national missile defense and nuclear weapons reductions. Before that, she was a researcher at Riverside Research Institute, where she worked on war-gaming scenarios for the Missile Defense Agency's Directorate of Intelligence.

2022 MILSAT SYMPOSIUM

NEXT-GENERATION SPACE DEFENSE

Join the Community Protecting and Expanding Critical Space Assets

OCTOBER 13 – 14, 2022

MILSATSHOW.COM