Next Generation Space Defense

MilsatMagazine

March 2022

Cover image is courtesy of PathFinder Digital and AvL Technologies

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

Advantech Wireless Technologies

Military & Government Solutions

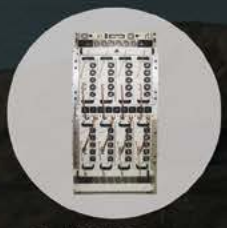
X-Band SSPAs/BUcs
GaN & GaAs configurations

Engage Class Integrated
SATCOM Terminals

X-Band / Ka-Band
Frequency Converters

Troposcatter Products

LNAs / LNBs



Solid State
Pulsed Amplifiers

Faster & More Secure Communications for Military and Government Agencies

At Advantech Wireless Technologies, we have over 25 years of experience delivering cutting-edge innovations in communications that solve mission critical communications challenges.
We understand the challenges that government & military leaders face and our technologies empower them with the freedom to communicate quickly, reliably and securely.

ADVANTECH
Wireless Technologies

advantechwireless.com

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
Ken Peterman, Viasat
Giles Peters, Track24 Defense
Koen Willems, ST Engineering
Mike Young, Envistacom

Authors

Dr. Juan Deaton
Juan Manuel Martinez
Dominic Perez
Charles Pope
David Presgraves
Ryan Schradin
Melanie Stricklan
A special thanks to Krystal Dredge of AvL Technologies

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

Experience Matters

Ask us about
Q- and V-band!

Catch the Ka-band wave with CPI

- More than 5,000 Ka-band HPAs and Solid State BUCs fielded
- Largest selection of Ka-band amplifiers available
- Field proven, outstanding reliability
- Worldwide Ka-ready regional service centers

WATTS	BANDWIDTH	TECHNOLOGY
80-160 Ka	Up to 2 GHz*	GaN BUC or SSPA
50-650 Ka	Up to 4 GHz	TWTA
800 Ka	Up to 300 MHz	Klystron PA
180 Q	Up to 2 GHz	TWTA
250 Pk V	Up to 4.2 GHz	TWTA

*Two 1 GHz selectable bands

Download our app! Search: CPI Satcom

Download on the App Store | GET IT ON Google Play

KNOW WHAT MATTERS

CPI
Communications & Power Industries

CPI SMP Satcom Products | www.cpii.com | satcommarketing@cpii.com | +1 (669) 275-2744

NOAA'S GOES-T SATELLITE LAUNCHED TO ORBIT BY UNITED LAUNCH ALLIANCE

A United Launch Alliance (ULA) Atlas V rocket carrying the GOES-T spacecraft for the National Oceanic and Atmospheric Administration (NOAA) and NASA lifted off on March 1 at 4:38 p.m. EST from Space Launch Complex-41 at Cape Canaveral Space Force Station. To date, ULA has launched 149 times with 100 percent mission success.

Artistic rendition of NOAA's GOES-T satellite.

The mission launched on an Atlas V 541 configuration rocket, which first flew in November 2011 with NASA's Mars Curiosity rover. This configuration has launched missions for the National Reconnaissance Office, carried the GOES-R and -S satellites into space, and most recently launched the Mars 2020 mission with the Perseverance rover and Ingenuity helicopter.

The Atlas V 541 included a 17-ft (5-m) diameter short payload fairing. The Atlas booster for this mission was powered by the RD AMROSS RD-180 engine. Aerojet Rocketdyne provided the RL10C-1 engine for the Centaur upper stage and Northrop Grumman provided the Graphite Epoxy Motor (GEM) 63 solid rocket boosters.

This was the 92nd launch of an Atlas V rocket and 22nd mission launched on an Atlas V in partnership with NASA's Launch Services Program (LSP). ULA's next launch is USSF-12 for the U.S. Space Force from Cape Canaveral Space Force Station, Florida.

"*Thank you to NASA, NOAA and our mission partners for your teamwork to launch this important mission. This successful launch adds to the GOES-R series, the Western Hemisphere's most sophisticated weather observation and environmental monitoring system*," said ***Gary Wentz***, ULA vice president of Government and Commercial Programs. "*The Atlas V delivered GOES-T directly to a geosynchronous transfer orbit. The orbital delivery accurately placed the spacecraft closer to its final destination which conserves the satellite's fuel supply and enables a longer mission life.*"

Lockheed Martin, the manufacturer of this satellite, added…

Space and Earth weather forecasting across the Western Hemisphere just got a little boost thanks to the Geostationary Operational Environmental Satellite (GOES-T), an advanced weather satellite built by Lockheed Martin [NYSE: LMT] for the National Oceanic and Atmospheric Administration (NOAA). The satellite successfully launched from Florida's Space Coast at 4:38 p.m. ET.

GOES-T will be renamed GOES-18 when it reaches geostationary orbit. Once operational, GOES-18 will take GOES-17's place tracking atmospheric rivers, floods, wildfires, drought, and other severe weather and climate phenomena over the West Coast of the United States.

"*GOES-T's launch is the culmination of innovative engineering, science and strong teamwork between NASA, NOAA and Lockheed Martin*," said ***Jagdeep Shergill,*** Lockheed Martin's GOES-R chief engineer and program manager. "*With the impact climate change has on weather patterns around the world, the work of satellites like GOES-T is more crucial than ever before, to help keep people safe now and in the future.*"

Advanced Monitoring of Weather, Oceans and Climate
As climate change continues to drive more frequent and severe environmental impacts, the GOES-R satellite series — of which GOES-T is the third — uses sophisticated technology to put information in the hands of those who need it most, when they need it.

Before it starts collecting and sharing critical weather data, the satellite's journey to space began in Littleton, Colorado, where it was designed and built by Lockheed Martin engineers.

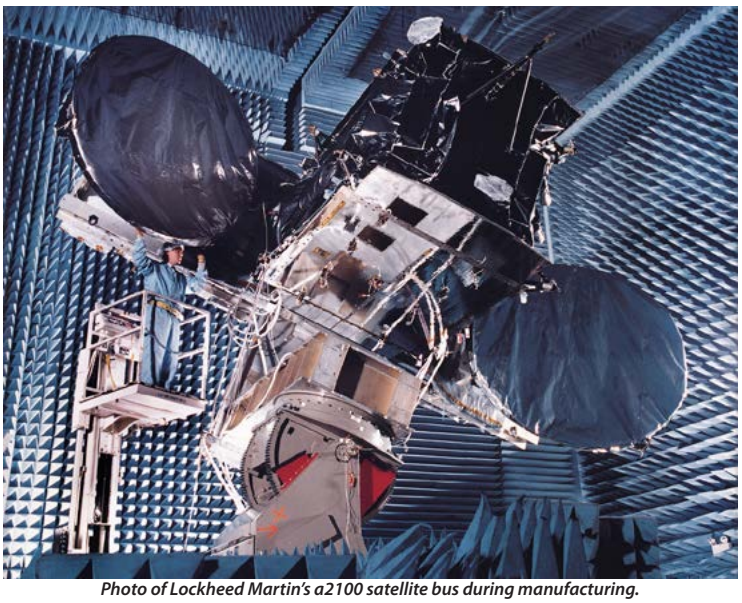


Photo of Lockheed Martin's a2100 satellite bus during manufacturing.

Based on Lockheed Martin's A2100 satellite bus design, the spacecraft features two high-tech instruments built by the company's Advanced Technology Center in Palo Alto, California…

- *Geostationary Lightning Mapper (GLM), which is a first-of-its-kind operational lightning mapper flown into its orbit, tracking lightning across the U.S. in real-time. By collecting data on the frequency, location and extent of lightning discharges, GLM allows meteorologists to quickly identify intensifying storms and take appropriate action. In 2020, GLM captured a lightning megaflash nearly 500 miles long that broke the world record for longest lightning flash.*

- *Solar Ultraviolet Imager (SUVI), focuses on space weather and measures the sun in extreme ultraviolet wavelength range and provides solar images. SUVI is essential to understanding active areas on the sun and predicting solar events that may disrupt power utilities, communication or navigation systems here on Earth.*

Over its 10-year operational lifetime, GOES-T can produce over a terabyte of data per day and monitors severe weather continuously, supporting NOAA's mission to provide weather data to save lives.

What's After Lift Off?
Now that it's in space, GOES-T will undergo an on-orbit checkout of its instruments and systems before beginning official operations in January 2023.

In addition to severe weather monitoring, it will do things like:

- *Identify volcanic eruptions, even ones under the ocean, like the recent event near Tonga*

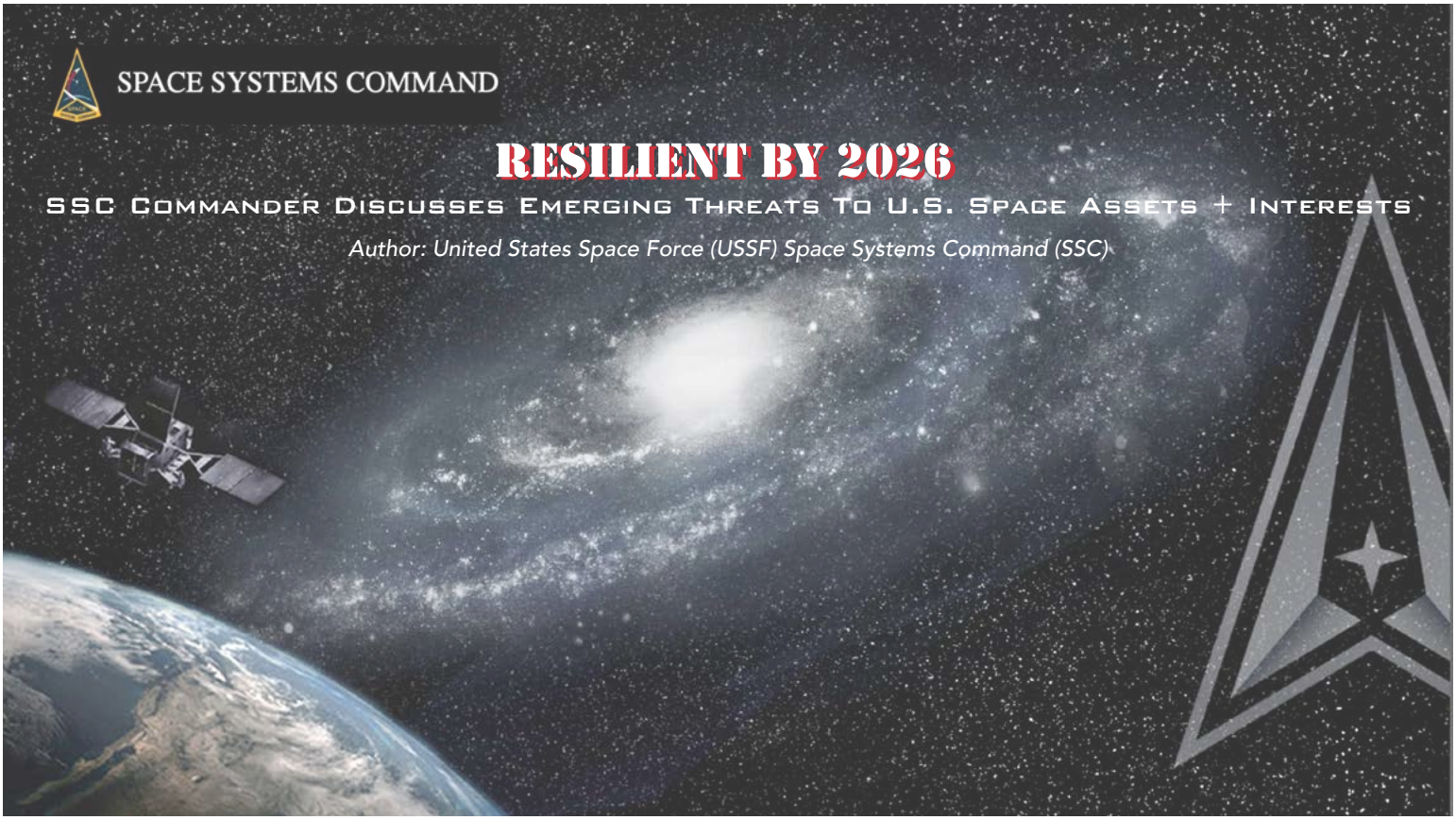
- *Measure land and sea surface temperatures to track drought conditions and warming oceans*

- *Provide early alerts to emergency responders for wildfires, including those caused by lightning strikes*

- *Observe solar flares that could impact telecommunication on and around Earth*

With three of the four GOES-R weather satellites now launched, GOES-U, the last satellite in the series, is in production and planned for a 2024 launch.

Beyond the GOES-R series, Lockheed Martin looks forward to continued partnership with NASA and NOAA as they look ahead to future weather and climate missions.



RESILIENT BY 2026

SSC Commander Discusses Emerging Threats To U.S. Space Assets + Interests

Author: United States Space Force (USSF) Space Systems Command (SSC)

Space Systems Command is focused on threats to U.S. assets in space and working to make them more resilient, even as adversary nations race to catch up.

Lt. Gen. Michael A. Guetlein, commander, ***Space Systems Command*** (**SSC**), recently sat down with ***Jason Davidson***, a member of the organization's *Public Affairs* team, to talk about some of the emerging threats to U.S. space assets, competition with China and Russia and some of the ways SSC is working to stay ahead of the threat and forging partnerships with space industry and allies.

Guetlein has said before that the U.S. military is the best in the world, but won't remain so for long if we don't place more effort on resilient capabilities, because our adversaries — particularly China and Russia — are working to catch up.

"*For the past 50-plus years, we have led the space race,*" Guetlein said. "*It started with our ascent to the moon and has continued on since then. It is clear to us that our way of fighting is in and through space.*"

While the United States continues to lead in the space domain and has the ability to protect and defend all of our assets on orbit and our capabilities here on Earth, Guetlein says that we have been watched throughout the years and our adversaries are quickly catching up.

"*Today, the Chinese are actually launching more rockets than we're launching on a day-to-day basis,*" Guetlein said. "*We still have more capability in orbit and we still have more satellites in orbit than they do, but they're rapidly attempting to catch up. And at the pace that they're growing, they will outpace us within the next decade.*"

Russia is more than just a disruptor for the United States; it's also a contender and a very determined peer in space, Guetlein said. They were part of the initial race to the moon, and they currently have a close partnership with China, working on potential things such as a base on the moon and the next generation of GPS.

"*The space environment has changed and that's why SSC is making resiliency a priority,*" Guetlein said. "*If you look at our traditional systems, they were built for an uncontested and uncongested environment. They never had to worry about how they were going to protect and defend themselves. They never had to worry about potential collisions with other satellites because it just wasn't that congested up there.*"

Guetlein said that as we go forward, our satellites must become more resilient, something that will require proliferation and disaggregation.

"*I can't just harden the satellite and expect the satellite to stay up there and defend itself. I have to proliferate the capability, which means get more satellites up there. I also have to disaggregate the capabilities, which means instead of trying to cram all of our capabilities on one satellite like we used to do because they were so expensive, we actually start disaggregating those capabilities to other satellites. That allows us to get some level of resiliency through proliferation and through disaggregation.*"

Guetlein also mentioned that resiliency is gained by having a redundancy of systems with integrated data levels and multiple data sources, a redundancy that can be achieved through partnerships with other government agencies, academia, industry and allies.

"*If you look at the history of our satellites and why they were taking so long to develop and why they were so expensive, it was because the cost of launch was expensive,*" Guetlein said. "*It could cost in excess of $350 million just to launch one satellite.*"

"*Because it cost so much to launch, we started to aggregate our capabilities on board one satellite,*" Guetlein explained. *The more you put on one satellite, the more expensive that satellite becomes and that the more expensive that satellite becomes, the less of them you can buy and the more dependent you become on that one asset going forward.*"

"*In that scenario, we end up paying a lot of money for mission assurance to guarantee that on one, very expensive satellite was guaranteed to get on orbit*," he added. "*What has happened over time is commercial innovation have driven the cost of launch way down. That has allowed us to put more satellites on orbit. In addition to that, technology has progressed to a point where I don't necessarily have to put as much technology on every single satellite so it doesn't cost as much, which has driven the cost of the satellites down.*"

This means SSC can start proliferating more satellites in different orbits and start connecting them in unique and opportune ways.

"*From a Space Systems Command perspective, what we have done is really started to embrace disaggregation and started looking at our capabilities from a system-to-systems capability and understanding what the warfighter really needs, and how can I best provide that capability without having to put all my eggs in one basket — if you will — on one satellite that's very, very expensive*," Guetlein continued.

For SSC, system-to-systems integration means doing that horizontal integration across multiple platforms. In the past, with very expensive satellites, a lot of time was spent integrating vertically through the satellite: making sure the COMM system worked, the propulsion system worked, the payload mated to the spacecraft. Much time was spent on mission assurance and on those interfaces in that vertical integration to deliver a very exquisite capability on orbit with one platform.

"*Stepping back, as we start to increase proliferation, disaggregation and our partnerships, it becomes very important that we start to integrate across different platforms*," Guetlein said. "*Just think of integrating GPS into MILSATCOM and integrating GPS into missile warning. Not only do we need to do that, but now we need to integrate with our industry partners who are providing a lot of space services, and our allied partners who are providing other capabilities. So the system-of-systems integration concept is really integrating across those disparate platforms and with different partnerships to make sure that the capability that we deliver is going to be survivable and it's going to be something that the warfighter needs.*"

SSC recently rolled out a new alignment, featuring five ***Program Executive Officers*** (**PEOs**):

1) Assured Access to Space

2) Battle Management Command, Control, and Communications (BMC3)

3) Space Domain Awareness & Combat Power

4) Communications & Positioning, Navigation, and Timing (PNT)

5) Space Sensing

The PEOs report directly to the ***Service Acquisition Executive*** (**SAE**) within that reporting chain under the ***Secretary of the Air Force***. Also under the realignment, the SSC commander, as the ***Space System-of-Systems Integrator***, serves as an advisor to space *Milestone Decision Authorities* regarding integration of space capabilities into the broader space enterprise prior to all milestone decisions.

The SSC commander will be responsible for staffing, personnel management, contracting, and budget execution across SSC space programs. The SSC ***Portfolio Architect Office*** (**SSC/ZA**) realigns as the ***Space Systems Integration Office*** and is responsible for managing the integration and sequencing of the space enterprise.

"*So it is my job, working for the SAE, to integrate across those five PEOs to ensure that the systems that we are delivering are going to be integrated into an enterprise approach*," the general explained. "*Not only that, but SSC is also the secretariat for an organization that actually brings in all the other program offices like the Space Development Agency, the Missile Defense Agency, the Rapid Capabilities Offices, and the National Reconnaissance Office, to also integrate them into the enterprise to make sure we're getting after a system of systems integration approach.*"

"*This new office that we stood up for system-to-systems integration, is under Dr. Claire Leon,*" Guetlein said. "*She is an amazing leader that we are going to be relying on heavily to make sure that as we deliver all of our capabilities, they're going to be effective, they're going to be time relevant, and they're going to be well integrated.*"

"*Our number one objective at standing up Space Systems Command last August, was to get a warfighter focus*," he said. "*Everything we do has a purpose and has a need on the battlefield. With that warfighter focus, we are going to guarantee those services will be available in a contested environment, and that the operators can absolutely depend on every capability that we're going to deliver.*"

The next objective was to get unity of effort.

"*I bring up unity of effort because it's kind of a foreign term for us in the military*," he said. "*We understand really well what unity of command is. That means I can look up above me and I can immediately understand who's in charge. Unity of effort is a little tougher because nobody's in charge. The reason we need unity of effort is there are multiple organizations developing space capabilities that go across organizational boundaries. Space Development Agency reports to the OSD R&E. Missile Defense Agency reports to the director of the Missile Defense Agency. Space RCO reports to the CSO as an example. No single individual has oversight over all of those different acquisition organizations. So we needed to achieve unity of effort in order to get after the system-to-systems integration concept.*"

The Space Force has been working with its partners and allies to develop a set of standards for acceptable behavior in space — including what to do with satellites when they are no longer operational.

"*We have norms of behavior in every other domain, but we don't have norms of behavior today in space*," Guetlein shared. "*To give you an example, how close can I operate next to an adversary satellite or to a partner satellite or to a commercial satellite? What is that standard*?"

"*The Space Force is currently working through with our international partners trying to understand what that standard is*," he said. "*One of the standards is how much debris can we leave on orbit? It's very dangerous. Some of that debris is traveling at 17,000 miles an hour, and you can just imagine debris the size of a BB slamming into a satellite, it would be catastrophic. Think about that same BB slamming into the International Space Station — that would also be catastrophic and probably cause loss of life. So it is to all of our benefit, to the world, to limit the amount of debris that we leave in orbit, but also try to do debris removal.*"

Guetlein mentioned that if it ever gets to a point where it is profitable for a commercial company to do debris removal, then it wouldn't need to be a government function. However, until that happens, industry would likely not want to spend its own money to do debris removal from space and would require the governments of the world to incentivize them to do that, possibly through a fee-for-service kind of approach.

With the tremendous amount of innovation coming from the space industry and perhaps the greatest interest in space since the push for the moon, the demand for STEM talent continues to grow and is another area in which SSC needs to compete.

"*In order for us to remain competitive in the space environment and competitive as a technological nation, we're going to have to continue to grow our STEM population*," Guetlein said. "*We do that at SSC in many different ways. We have outreach starting in elementary school to try to get kids energized into STEM. We try to mentor them in STEM, and we do the same thing at the university level.*"

Guetlein said, the U.S. Space Force needs are greater than just STEM graduates.

"*We also have many non-technical career fields, so anybody that's interested in space that wants to participate, we would love to take them regardless of their career or their degree*," he said. "*It doesn't have to be a STEM degree. We have public affairs, we have contracting officers, financial officers and intelligence analysts. All are part of our team for the Space Force.*"

Scan for Space Force career opportunities.

Following the signing of U.S. Space Force's University Partnership Program Memorandum of Understanding with University of Southern California, Lt. Gen. Michael A. Guetlein toured USC's Institute for Creative Technologies, Vision & Graphics Laboratory, where students and faculty are developing new techniques for creating and displaying photorealistic computer graphics of people, objects, and environments. Photo by Michiko Riley, SSC

Guetlein said he doesn't believe the general public understands just how integrated space is into their day-to-day life.

"*If you look at just GPS, the Global Positioning System…everybody knows that it gets us from point A to point B and it's on the dash of our cars and it's on our cell phones*", he said. "*But what they probably don't understand is that it also drives our banking networks, it drives our electric grid, and it drives distribution logistics. So without having GPS... we would not be able to get the milk delivered in the grocery stores, nor the food on the shelves and we would not be able to unload the ships out at sea. A bad day in space, a day without space... the entire economy would come to a halt because we couldn't move data, we couldn't move people and couldn't move goods.*"

Guetlein said that the public needs to understand that space has changed fundamentally and is now a contested environment.

"*The adversary has not only proven determined to prevent our use of space for peace and defense, but they've also proven extremely capable of doing that*," he said. "*[Late last year], the Russians launched a direct ascent, ASAT (a rocket)…into space and destroyed one of their own satellites. When they did that, they created 1,500 pieces of debris in a very unprofessional move. Those 1,500 pieces of debris are still up there, but worse yet, they caused the International Space Station to go into their escape capsules because they were afraid they were going to get hit with debris. And there were two (Russian) cosmonauts in that International Space Station as well.*

"*So not only has the adversary proven capable, they've proven the intent, and they've proven that they're willing to do it in a very unprofessional and unsafe way as well! However, the Nation should be proud that they have the greatest Space Force on the planet that was created by the greatest Air Force on the planet, and we are getting after business!*" Guetlein said.

Scan to view the video interview.

Space Systems Command is the U.S. Space Force field command responsible for rapidly identifying, prototyping and fielding resilient space capabilities for joint warfighters. SSC delivers sustainable joint space warfighting capabilities to defend the nation and its allies while disrupting adversaries in the contested space domain. SSC mission areas include launch acquisition and operations; space domain awareness; positioning, navigation and timing; missile warning; satellite communication; and cross-mission ground, command and control and data.

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

MISSILE TRACK CUSTODY DEMONSTRATION PROJECT TAKES DIGITAL ENGINEERING TO THE NEXT LEVEL

Computers have been used to help design high-tech satellites for many years, but one Space Systems Command (SSC) project in particular is working to take digital engineering to the next level, officials said.

The ***Missile Track Custody Demonstration*** (**MTCD**) is a prototyping effort to determine possible future satellite constellations supporting SSC's ***Missile Warning and Missile Tracking*** mission.

Lt. Col. Gary Goff

"*The digital engineering sprint of the project, which was formally launched in May of 2021, is using digital engineering, modeling and simulation to validate requirements for missile raid containment while building flight demonstration units that will validate performance and feed data back into the digital models*," said Lt. Col. ***Gary Goff,*** materiel leader for rapid prototyping at SSC. "*We look at the current missile threats that are out there – what they look like, how they fly, how they emit heat – and do a war-game simulation with them. Then we simulate what our sensors would see, how well we can track the position and velocity and contain them at a certain accuracy, and how we tell the radars on the ground where to search for an inbound missile so they can use that information to launch an intercept.*

"*The contractors are going to look at how they build that sensor, the optics it would take, the electronics it would take, the full satellite design and they're going to represent that digitally and tie it back to the government requirements*," Goff explained. "*This gives us the ability to do a full digital design. We call it 'try before you buy' — we're going to show we can meet all these performance requirements before we go and start building it.*"

Goff said there will be some smaller demonstrations of some of the electronics — which will serve to validate the performance of the digital models – but most of the project in the initial design phases will be digital.

"*Let's say that in your model, you thought that you could detect a certain missile, based on the way you simulated it*," Goff explained. "*We're going to put some of those electronics to the test on the ground in a live environment and be able to show if the performance matches the model prediction. This way, we tie the model to some real data.*"

Joel Gussy

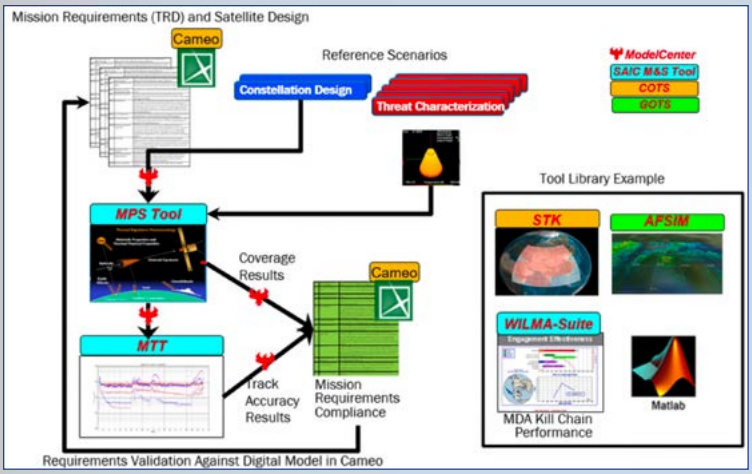
Joel Gussy, system director for demonstrations and technology programs for ***The Aerospace Corporation***, the lead **FFRDC** (***Federally Funded Research and Development Centers***) organization on the project, said MTCD has two key aspects: development of a new space-based capability to track emerging missile threats, and a digital engineering approach that will capture the technical details in the model space to help design the system and analyze its performance.

"*I see three key elements to digital engineering that all need to be tightly integrated. There's the model-based systems engineering models, then the detailed modeling, simulation and analysis tools and then there's things like digital twins, where you have a representation of something that's real built in a software model*," Gussy said.

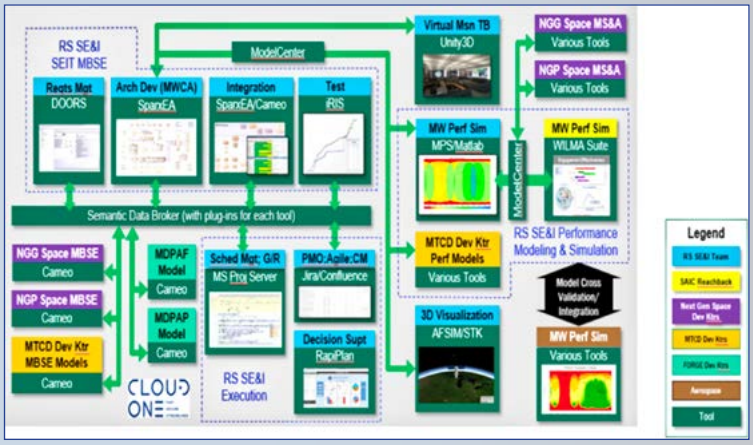
The MTCD project is primarily focused on the first two elements now but is also pursuing targeted, digital, twin representations that will have a large payoff during later phases of the program, Gussy said.

MTCD has two prime development contractors: ***Millennium Space Systems*** (**MSS**) and ***Raytheon Intelligence and Space***.

The effort includes integration of the model-based systems engineering data from the two payload contractors and other SSC ***Overhead Persistent Infrared*** (**OPIR**) programs in a ***Government Reference MBSE Model*** (**GRMM**). The MTCD GRMM will provide the government requirements, high-level architecture, internal/external interfaces and enterprise behavior.



End-to-End digital thread example. Image is courtesy of SSC.



Missile Warning Future Digital Engineering Ecosystem. Image is courtesy of SSC.

The methodology for both contractors to connect their models to the MTCD GRMM is through a ***Cameo Project Usage*** — a software package that handles system markup language, separate from the performance model — to ensure evaluation of each contractor's solution against the same problem domain.

For most modern military programs, performance models and simulation tools are used to validate a contractor's designs. However, MTCD is taking this practice one step further by connecting the performance and simulation capabilities to the model based system engineering models.

The Aerospace Corporation and ***Science Applications International Corporation*** (**SAIC**) models will be used to independently verify contractor performance results using the contractor's system characteristics as defined in their model based system engineering models.

"A lot of folks associate digital engineering with model-based systems engineering, but I see that as just one piece," Gussy said. *"On this program, not only did we request model based systems engineering products from our industry partners, but a dozen specific analytical models that break down how their system and subsystems operate or interact with each other.*

"These analytical models will allow us to execute the integrated modeling, simulation and analysis effort but also help pave the way towards those digital twins," Gussy said. *"This gives us a methodology to represent the physical, functional and the performance aspects at a high level of fidelity. We're not just doing the independent validation, but also helping to integrate the components of contractor development with the broader missile warning, tracking and defense enterprise, including the Missile Defense Agency and the Space Development Agency. How all those weapon systems will work together is something we can do efficiently with these digital models and performance simulations."*

"There's a lot of talk about "digital twins" but the first step is a digital thread," said ***Franco Macchia***, systems engineer with SAIC, which also is working with SSC on a prototype missile warning sensor system for the project.

"If I have a system described in a model-based system engineering model and I want to run a trade-off analysis — maybe I want to add more satellites — those are threads you can test digitally and do a trade analysis very quickly," Macchia said.

Frank Macchia

"Digital engineering is an enabler," he added. *"It can immediately help you manage and understand that system. Think about all the different connections and behaviors to everything else: you're trying to model different communication links, satellite to ground, cross-links with other satellites – there's a ton of information flowing. Using a model based systems engineering model helps to understand and capture a lot of information that's very difficult to do with PowerPoint charts – and you can see where something is impacted as soon as you make a change."*

Currently, Goff said, the project is undergoing its *Preliminary Design Review*. The team understands the requirements and is working on the preliminary design of the sensor itself. In November, the project will undergo an all-digital ***Critical Design Review*** (***CDR***) *"in the model."*

"The whole purpose of that CDR means that we are ready to start building that sensor," Goff said. *"If we come out of that meeting and we agree that it can do everything we need it to do, we've shown it all works together, the next step is to start ordering parts and assembling the sensor and building satellites, targeting a launch as early as 2026."*

"Having a CDR with only digital deliverables is very unusual," Macchia said. *"Normally, you would do some R&D testing of hardware prior to the CDR. We're evaluating these prototype systems entirely digitally, which is also, in a way, a prototype of the methodology for passing CDR without building system hardware. Our program is a major pathfinder for future SSC efforts."*

"At some point as part of this project, we'll be able to take the models to a classified environment and we'll be able to tie the performance models to a requirements-based model," Goff said. *"We'll be able to do quick iterations and design trades, almost automatically. Say you want to launch another satellite; how much will that improve your performance? What if there's a new missile? How can your system perform against that? Well, we will be able to do that very quickly and tie that right back to the war-fighter requirements."*

"As you move forward in a program, it becomes more complicated to integrate more systems as you fill it out and add more satellites, both from the ground perspective and the space perspective," Goff said. *"One of the biggest benefits of using a digital model is being able to define all the appropriate interfaces and do all the integration work necessary. A lot of these sensors will be built by one contractor, maybe the bus will be built by another, and the ground system by a different contractor. You have the models tying together these different areas of expertise, across all these different contractors, and it gives you an ability to do that integration much more rapidly."*

The biggest barrier challenging the MTCD's full implementation of the digital engineering approach is the lack of a collaborative digital environment. Currently, SSC government/contractor networks are mostly isolated from each other and do not have the capability to use these tools and integrated threads in a common space.

"We're spending time on and investing in the infrastructure to allow us to have a secure environment to share and integrate these various products," Gussy explained. *"There's different models and tools that come from the developers and products from the integrated government team that we want to tie and link together for the full system of systems assessment. We need a common shared environment we can do that in."*

MTCD is pursuing a ***Cloud-Based Digital Environment*** to provide broad access to all of the digital engineering and ***Modeling & Simulation*** (**M&S**) tools. The project is currently evaluating usage of the ***U.S. Department of Defense's Cloud One's Digital Engineering as a Service*** (**DEaaS**). MTCD also is looking into ***Direct Connect and Commercial Solutions*** for classified options to increase the speed at which connections to the Cloud can be made.

If the project is successful, it will be a game-changer for SSC,

Goff said. *"How it works now is, we have a government model, and sometimes we send that model over to the contractors on CDs, because it's classified. If we're able to interact in the Cloud, when I come to work every day, I'm logging in to a set of software in a classified, Cloud-based environment and the contractor is logging on to the same Cloud-based environment.*

"They're doing their development, and the government is reviewing that development, different contractors are interacting together in the Cloud at a classified level," Goff said. *"There's no awkward stage of delivering a model, figuring out the software, what patches you have, what you don't have, what modules you need."*

It would also make it easier in the future for new, emerging and smaller commercial space companies to work with the USSF, Goff added. Currently, larger defense "*primes*" have an advantage because they have established relationships with the government, have personnel with security clearances and access to secure facilities. A secure Cloud environment could help smaller companies interact with the government at the right classification levels in a matter of months, not years.

Macchia said one misconception he often hears about model-based systems engineering modeling is that there are a lot of non-recoverable costs. However, a MBSE model can be generated fairly quickly with initial information, but then subject matter experts and engineering leads have to help refine that data, which can sometimes take weeks.

"The resource-intensive piece in understanding a system is still the Systems Engineering required to ensure that the model is accurate, not the actual modeling effort," Macchia said. *"The model is a tool to help organize the systems engineering and helps to catch any areas that were missed or do not make sense. In the long run, the model saves time and money by identifying optimal solutions that wouldn't have been possible to, or would have been difficult to identify by traditional means.*

"Additionally, once we build a model of the system(s), engineers can use the models for future programs — update them and build off of them," Macchia said. *"It's a dynamic description, rather than a static one."*

Even with the advances in modeling and technology, human experts are still a critical component for success, Gussy said. *"One thing that doesn't get said enough about digital engineering is that there is still a need for the subject matter experts and the real engineering teams," Gussy said. "Some people envision that you have all these models and you change a parameter and push a button and an optimized design gets spit out. We can do that for simple trades but we still have some work to go to automate for assessment of the complex and dynamic mission systems and warfighting scenarios that we are dealing with here.*

"We need the skilled engineering personnel and technical experts to help build the models, drive smart trades and evaluate and interpret the data and results," Gussy said.

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

DISPATCHES

GEN. JAMES DICKINSON, USSPACECOM COMMANDER, GIVES HIS INSIGHTS TO THE U.S. HOUSE + SENATE

U.S. Army Gen. *James Dickinson*, *U.S. Space Command* commander, appeared before the *U.S. House and Senate Armed Services Committees* to provide his Fiscal Year 2023 Priorities and Posture in Washington, D.C., on March 1st and 8th.

The USSPACECOM commander testified alongside U.S. Navy Adm. ***Charles Richard***, U.S. Strategic Command commander, U.S. Air Force General ***Glen Van Herck***, U.S. Northern Command commander and Honorable ***Sasha Baker***, Deputy Undersecretary of Defense, on March 1st. Dickinson and Richards also appeared before the Senate Armed Services Committee in Washington, D.C., March 8th.

The hearings give committee lawmakers insight into the priorities of senior defense leaders and also give lawmakers an opportunity to ask questions.

During his testimony, Dickinson offered insight on where the command stands currently and its posture for the future aligned with National Defense Strategy.

"*Today, we remain hard at work building the Command toward Full Operational Capability*," said Dickinson. "*We are prepared to execute our Unified Command Plan missions and responsibilities, yet acknowledge that the challenges from our competitors in the domain are substantial and growing.*"

Dickinson provided an overview of challenges presented by Russian and Chinese counterspy testing, such as Russia testing a destructive ***Direct Ascent Anti-Satellite*** (**DA-ASAT**) missile on November15, 2021, and China conducting the first launch of a fractional orbital platform with a hypersonic glide vehicle.

"*In 2021, the PRC increased on-orbit assets by 27%*," Dickinson said. "*Their recent counter-space capability demonstrations include the DN-1 and DN-2 Direct Ascent Anti-Satellite tests and the Hypersonic Glide Vehicle test. In January, the recently launched SJ-21 "space debris mitigation" satellite docked with a defunct PRC satellite and moved it to an entirely different orbit. This activity demonstrated potential dual-use capability in SJ-21 interaction with other satellites.*"

Dickinson explained USSPACECOM is committed to deterring the use of competitor counterspace capabilities within the framework of the D***epartment of Defense's Integrated Deterrence*** initiative. And, if called upon, the command is capable of providing options to protect and defend against such threats.

Due to the growing need and demand to provide decision-quality information to combatant commanders and the ***National Command Authorities***, Dickinson requested the Committees to authorize and fund ***SDA*** programs that enable USSPACECOM to monitor, characterize and attribute behavior as well as provide combat-relevant indications and warning of potential threats to U.S. government, allied, and partner space systems.

"*SDA helps us analyze, not just identify what is occurring in space, which, when combined with information from our intelligence agencies, helps develop an understanding of why things are happening,*" said Dickinson. "*SDA remains my top mission priority for USSPACECOM. SDA provides the backbone of USSPACECOM's strategy for accomplishing our mission. That strategy sets the conditions to deter first, and when called upon, to defend space capabilities and deliver combat power to the United States and its allies.*"

Dickinson thanked the members of the committees for their unwavering support of the men and women of USSPACECOM and for the opportunity to tell their stories of mission challenges, and their successes in meeting those challenges.

"*I am honored to represent the approximate 18,000 military, civilian, and contractor personnel supporting USSPACECOM's mission. Our success is fundamentally a reflection of their superb capabilities, their unrelenting dedication, and their steadfast perseverance*," said Dickinson. "*Space is vital to our modern way of life and our people remain our most critical asset.*"

News authored by U.S. Space Command Public Affairs

DISPATCHES

NORTHROP GRUMMAN SELECTED BY USMC FOR NEXTGEN HANDHELD TARGETING SYSTEM

Northrop Grumman Corporation (NYSE: NOC) has been selected to provide the U.S. Marine Corps with the Next Generation Handheld Targeting System (NGHTS).

This compact targeting device provides unparalleled precision targeting and is capable of operation in GPS-denied environments

NGHTS is a laser-based device that will give Marines an enhanced capability to identify and designate targets from extended ranges.

"*NGHTS will significantly enhance the ability of Marines to identify ground targets under a wide range of conditions*," said Bob Gough, vice president, navigation, targeting and survivability, Northrop Grumman.

Gough continued, "*Connected to military networks, NGHTS can provide superior situational awareness and accurate coordinates for the delivery of effects from beyond the line of sight*."

Northrop Grumman's NGHTS is capable of performing rapid target acquisition, laser terminal guidance operation and laser spot imaging functions.

Its high-definition infrared sensors provide accuracy and grid capability over extended ranges. Additional features include a high-definition color display and day/night celestial compasses.

DISPATCHES

ADVANCED TECHNIQUES = RECORD BREAKING BUILD SPEED FOR BOEING'S WGS-11+ SATELLITE

Artistic rendition of the Boeing manufactured WGS-11+ satellite, courtesy of the company.

Boeing has begun building the latest version of the *Wideband Global SATCOM* satellite system, *WGS-11+*, using advanced techniques to effectively integrate the latest commercial technology while enabling a high-paced five-year schedule that will deliver years faster than similar, clean-sheet designs.

Boeing and the ***U.S. Space Force*** completed the system's critical design review in late 2021, officially launching the program's production phase. Leveraging additive manufacturing, rapid prototyping, agile development and other advanced techniques, Boeing has created cost and schedule benefits, while boosting system performance.

WGS-11+ showcases an evolution in phased array technology. Based on Boeing's advances on its commercial 702X software-defined satellite payload, it is capable of generating hundreds of electronically-steered beams simultaneously, providing users with more than twice the mission capability compared to satellites within the existing WGS fleet.

Like 702X, each individual beam is shapeable and can be uniquely tailored to any operation, enabling increased mission flexibility and responsiveness. Narrower beam widths with dual polarization unique to WGS-11+ help protect against jamming and interference while allowing greater frequency reuse.

When it joins the constellation of ten WGS satellites, WGS-11+ will substantially increase throughput capacity of essential communication services for the U.S. government and its allies. It is scheduled for delivery in 2024.

"*We're moving at record-breaking speed to deliver the unmatched resilience, efficiency, and throughput WGS-11+ offers our warfighters*," said Col. ***Matt Spencer***, Space Systems Command Geosynchronous Earth Orbit and Polar Division Senior Materiel Leader. "*Boeing's ability to rapidly integrate the latest commercial technology into our infrastructure gives us a competitive edge on the battlefield.*"

"*We're printing more than a thousand parts for WGS-11+, giving us the capability to introduce customization in a way that improves system performance, without requiring extensive integration times or customized tooling*," said ***Troy Dawson***, Boeing Government Satellite Systems vice president. "*We understand how important speed is to the mission. That production speed translates to effectiveness against threats. As we continue to invest our technology and processes, we know that a similarly capable satellite could be delivered even faster.*"

INTELSAT NAMES THE COMPANY'S NEW CEO

Intelsat **has named *David Wajsgras* as the company's next chief executive officer (CEO). Effective April 4, Wajsgras succeeds *Stephen Spengler*, who announced his planned retirement in October of 2021.**

Wajsgras has two decades of experience at the senior executive management level, providing operational, strategic and financial leadership in both the commercial and defense industries.

David Wajsgras

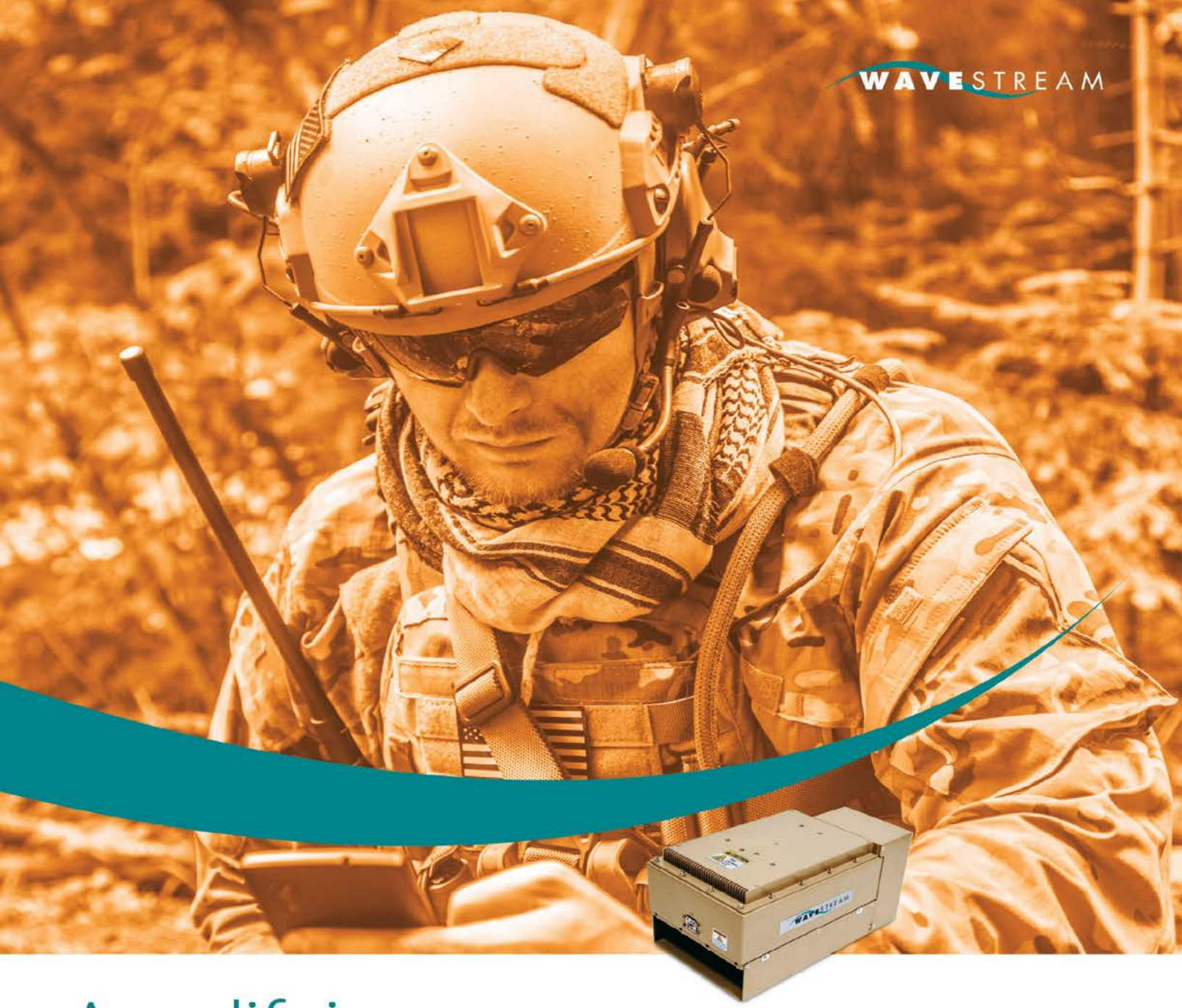
He most recently served as president of the global, $7.5-billion, advanced-technology Intelligence, Information and Services (IIS) business at the former Raytheon Company, now part of Raytheon Technologies (NYSE: RTX).

Before joining Raytheon as chief financial officer, Wajsgras was executive vice president and chief financial officer at Lear Corporation (NYSE: LEA) and held other key operations and leadership roles.

"*Dave Wajsgras is a results-oriented leader with a great track record of performance throughout his career*," said ***Lisa Hammitt***, chairperson of the Intelsat Board of Directors. "*He develops talent and builds teams, thinks and acts strategically, and engages positively with customers and other stakeholders to the benefit of the business. Dave is just the right person to lead Intelsat at this important time. As we welcome Dave, we also will be saying goodbye to Steve Spengler. The members of the Board – and indeed the whole Intelsat team – owe great thanks to Steve for his tremendous contributions to the company for 18 years and his steady and accomplished leadership over the past seven. His retirement is well earned.*"

"*Intelsat has a leading position in the market and a strong, global team of professionals*," said ***Wajsgras***. "*While the company has made history over nearly 60 years, it's Intelsat's future that excites me most. With a focus on customers and a commitment to delivering on our promises, we're ready to write the next chapter in the story of communications and connectivity.*"

WAVESTREAM



Amplifying Mission-Critical Satellite Communication

50W Ka-Band GaN Wideband BUC

Operates in all commercial and military Ka-Band frequencies

Supporting ARSTRAT-certified Ka-Band units 14 years after initial deployment.

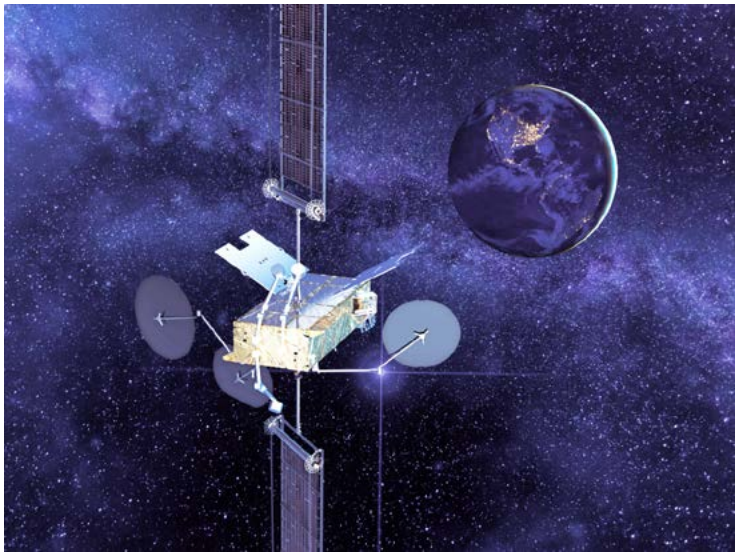
We're ready to support the most critical networks on the planet.

WAVESTREAM. READY FOR YOUR BUSINESS.

www.wavestream.com

DISPATCHES

NEW PROJECT TO PLACE DENMARK ON THE MILITARY SPACE TECHNOLOGY MAP



Space technology and satellites are not only important for monitoring climate change, for navigating ships and airplanes, and for communicating over long distances — they are also essential to the security of Denmark and the EU.

A new project develops a technology that makes it possible to monitor and identify military threats in space and on Earth. The AI-driven technology will contribute to process the vast data streams stemming from satellites and land-based sensors and thereby create the basis for using the space data and intelligence for military purposes.

The project, which goes under the name ***INTEGRAL*** and is a part of EU's SSAEW SC2, ***Space Situational Awareness – Space Command and Control,*** is supported with funds from the European Defence Fund and is a cooperation between DTU (***Technical University of Denmark***), the Danish company ***Space Inventor*** and the French defence and technology company ***Thales*** in Denmark.

The Danish company Space Inventor is going to play a key role in the project by contributing to the development of the prototype for INTEGRAL and finding an algorithm that can trace the orbit of satellites. With the awarded funds follow a significantly increased visibility on the international stage as well as access to knowledge and powerful networks.

A unique cooperation with massive potential

The project is one of only 26 projects which have been approved by the EU Commission under the test program ***European Defence Industrial Development Program*** (EDIDP) in 2020. Thales sees great potential in the Danish Defence industry looking towards Europe.

"*It is a unique project because we unite science and industry on multiple levels. We are, in Thales, a part of the Danish ecosystem within defence and also an international company with deep knowledge about the European defence market. We would like to contribute with this knowledge so that Danish companies can unlock the great potential which the Danish defence industry holds*," said ***Tommy Ayouty***, CEO, Thales Danmark, VP Thales Group in the Nordics.

Several Danish companies are participating in EU projects such as project SAURON for SSA Sensors and the space & defence project ***SSA Early Warning*** which both have received funds from EDIDP 2020. Along with INTEGRAL, these projects can improve Denmark's visibility within the defence and space sector and are expected to lay the foundation for further cooperation and to gather knowledge in connection with the surveillance of the Arctic in the future.

The INTEGRAL project runs until 2023, at which point the parties involved can seek funds to continue the work.

CUSTOM ELECTRONICS' NEW PORTABLE POWER SYSTEM FOR MILITARY + DEFENSE INDUSTRY

Custom Electronics, Inc. **(CEI) has introduced their CMP2500 portable battery system.**

At the heart of the ***CMP2500*** battery system are ***LiFePO4*** lithium-iron phosphate cells. Each battery has a 2.5kWh capacity while the system provides up to 10 kWh capacity at 24 VDC or up to 5 kWh at 12 VDC.

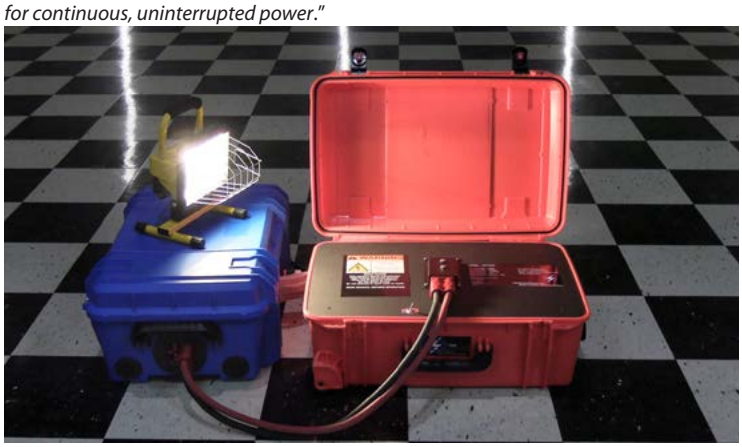
The batteries are housed in a rugged military-spec case that can be moved by one person, making it ideal for military and defense field and training applications including charging of drones, running simulations, targetry and silent watch. Users can set up in a field or training space without having to run a cable to a generator or back to the military installation. In addition, the quietness of the system when running is a main benefit for these types of applications.

One of the unique features of the CMP2500 solution that distinguishes itself from many of its competitors is its proprietary battery management system (BMS). With a focus on taking a modular integrated systems design approach to generate, store, distribute and utilize electric energy in order to power devices and equipment, the BMS delivers a safe, effective and cost-efficient energy storage solution.

The BMS is custom designed to protect cells, equipment and the user. In addition, the system is fully scalable in voltage and capacity, and can replace or supplement generator operations by reducing operating time, fuel consumption and related noise.

The systems charger and inverter capabilities are sourced from high-quality manufacturers and included as system components. In addition, the inverters feature up to 4000W output and chargers up to 40 ADC.

"*From start to finish, the CMP2500 battery solution is designed to provide power when and where you need it,*" said ***Carol Brower***, Vice President of Operations, Custom Electronics, Inc. "*Simplicity of design, ease of use and safety are top priorities we focused on when designing all system components. The design allows for continuous, uninterrupted power.*"



DISPATCHES

DOD AND PARTNERS RELEASE COMBINED SPACE OPERATIONS VISION 2031

U.S. Department of Defense

The United States joins Australia, Canada, France, Germany, New Zealand, and the United Kingdom in the joint release of the "*Combined Space Operations (CSpO) Vision 2031*."

CSpO is an initiative to address the overarching need to encourage responsible use of space, recognizing challenges to space sustainability, threats presented by technological advances, and the increasingly comprehensive and aggressive counterspace programs of other nation states.

The "*CSpO Vision 2031*" outlines the initiative's overarching purpose and highlights its guiding principles, including: freedom of use of space, responsible and sustainable use of space, partnering while recognizing sovereignty, and upholding international law.

These guiding principles steer the initiative's objectives and are supported by several lines of effort, from developing and operating resilient, interoperable architectures to fostering responsible military behaviors in space and sharing intelligence and information, all leading to the pursuit of a safe, secure, and sustainable space domain.

CSpO Principals last met in December of 2021, reaffirming their nations' support to the *Vision*, including the intent to prevent conflicts extending to or originating in space and to hold accountable those who threaten the safety of the space environment and the space assets of others.

Representatives from the ***Department of Defense*** specifically addressed the importance of information sharing, leading to greater cooperation and interoperability, all key CSpO components.

Combined Space Operations Vision 2031

Vision

Partners in national security space operations leading as responsible actors and seeking and prepared to protect and defend against hostile space activities in accordance with applicable international law.

Mission

Generate and improve cooperation, coordination, and interoperability opportunities to sustain freedom of action in space, optimize resources, enhance mission assurance and resilience, and prevent conflict.

The Importance of Space

Space is integral to modern multi-domain military operations and provides strategic advantage. Space-based capabilities deliver a wide range of effects that underpin daily life, including communications, navigation, remote sensing, Earth observation, weather services, and financial transactions. Maintaining and supporting the availability of these capabilities are in the interest of each nation. Continued delivery of these capabilities requires complete access to and freedom to operate in space.

Space has evolved into a contested and congested operational domain. As space becomes more crowded, the security and stability of this critical domain are endangered. Some nations have developed capabilities designed to deny, degrade, and disrupt access to and utilization of space-based capabilities. These nations have demonstrated the ability to hold space-based capabilities at risk and to target critical assets in an effort to reduce our military effectiveness in a crisis or conflict. Further, the lack of widely accepted norms of responsible behavior and historical practice

The convergence of these factors creates compelling strategic and operational urgency that serves as a call to action. We share a desire to accelerate and improve our ability to conduct combined military space operations, as responsible space actors, in order to maintain security and prevent escalation in space and on Earth. We seek to be prepared to protect our national interests and the peaceful use of space.

Shared Guiding Principles

The following guiding principles are shared broadly among the Participants in the Combined Space Operations (CSpO) Initiative Memorandum of Understanding (MoU):

- **Freedom of Use of Space**: *Militaries have an important role in contributing to international efforts to ensure freedom of access to and use of space. CSpO Participants work to ensure our national security space operations promote a secure, stable, safe, peaceful, and operationally sustainable space domain.*

- **Responsible and Sustainable Use of Space**: *The world is reliant on space- based systems —- activities in space have consequences across the spectrum of human activity. CSpO Participants pursue activities that endeavor to minimize the creation of long-lived space debris and contribute to the enduring sustainability of the outer space environment.*

- **Partnering While Upholding Sovereignty**: *CSpO Participants recognize and uphold the rights of each Participant to act and communicate independently and in a manner commensurate with their own national policies and interests. National efforts are synchronized, where appropriate, through clear and open dialogue.*

- **Upholding International Law**: *Each Participant conducts activities in accordance with applicable international law, including the Outer Space Treaty, the UN Charter, and, in case of armed conflict, with the law of armed conflict.*

Objectives

To realize our vision and mission, CSpO Participants affirm the following objectives to guide our national and collective actions:

- **Prevent conflicts** – *CSpO Participants seek to prevent conflict, including conflict extending to or originating in space. By strengthening coordination, building resiliency, promoting responsible behavior in space, enhancing partnership, and communicating transparently, we improve our national and collective abilities to prevent conflict and to promote security and stability in all domains*

- **Unity of Effort** – *CSpO Participants seek to enable combined space operations by sharing information across multiple classification levels – from the strategic to the operational and tactical levels, and at a pace that is operationally relevant – through real-time synchronized networked operations centers operated by a workforce with common training.*

- **Space Mission Assurance** - *CSpO Participants seek to establish and maintain a robust, responsive, and interoperable space infrastructure enabling continued space effects in the face of adverse action or changes to the space domain. Ensuring the continued function and resilience of equipment, facilities, networks, information and information systems, personnel, infrastructure, and supply chains, we seek to deny the benefit of interference and to ensure the availability of CSpO Participants' national security mission-essential functions throughout the spectrum of military operations.*

- **Defense and Protection** - *CSpO Participants are committed to the defense and protection of our national interests and the space domain. This may include collaboration across a range of measures, such as: developing requirements for current and future systems to counter hostile space activities and to deter, deny, or defeat attacks or interference with the space enterprise; delivering the ability for combined, agile, and adaptive command and control through resilient, secure, interoperable, and sustainable communications; sharing appropriate intelligence and information; and timely and inclusive leadership dialogues and decision-making.*

Lines of Effort

The CSpO Participants seek to achieve the shared objectives outlined above through several lines of effort (LOE). The following LOEs provide a framework to guide the national and collective efforts of CSpO Participants:

- **Develop and operate resilient, interoperable architectures** *to enable space mission assurance and unity of effort, through identification of gaps and collaborative opportunities.*

- **Enhance command, control, and communications capabilities and other operational linkages among CSpO Participants** *to support unity of effort and the ability to conduct combined and synchronized operations throughout the spectrum of military operations.*

- **Foster responsible military behaviors in space** *to promote conditions to maintain freedom of use, access to, and sustainability of the space domain, and to discourage irresponsible behavior and avoid escalation.*

- **Collaborate on strategic communications efforts** *to set the desired conditions in the information environment.*

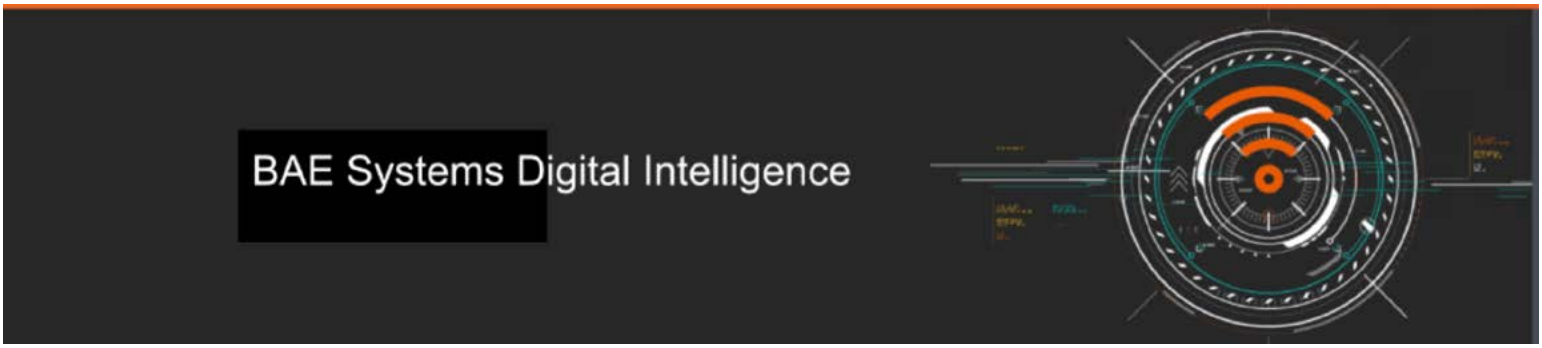
- **Share intelligence and information** *to create a common understanding and support unity of effort.*

- **Professionalize space cadres and training** *to energize shared, common understanding of the space domain, share best practices, and increase our collective expertise.*

Conclusion

The CSpO Participants are committed to pursuing the above objectives and lines of effort in alignment with our shared guiding principles to achieve our national and collective interests. The expansive opportunities and challenges presented by the rapidly changing space domain require collaboration to enhance responsible behavior and promote a secure, stable, and sustainable domain. Through our discussions and working group activities, we intend to implement national and collective efforts toward those ends.

NEW DIGITAL INTELLIGENCE BUSINESS FORMED BY BAE SYSTEMS



***BAE Systems* recently formed a new *Digital Intelligence* business, bringing together many world-class digital, data and cyber capabilities from across the Company to deliver a greater digital advantage to its customers and partners.**

The creation of the new business, comprising almost 5,000 people in 16 countries around the world, reflects a growing requirement from customers to gather, process and manage complex data.

Digital Intelligence will deliver a greater range of digital capabilities alongside leading cyber, intelligence and security expertise to an extensive portfolio of government, defence and commercial customers around the globe. The business will focus on helping customers from across the Company to operate successfully, securely and efficiently in the digital world.

Digital Intelligence incorporates recent strategic acquisitions by BAE Systems, which further enhance the Company's capabilities in digital, data analytics and space, positioning it to accelerate growth in an evolving market.

Acquisitions include: ***In-Space Missions,*** a UK company which designs, builds and operates satellites and satellite systems; ***PPM***, a developer and manufacturer of high-end electronics; and data consultancy and digital services company, ***Techmodal***.

David Armstrong

David Armstrong, Group Managing Director, BAE Systems' Digital Intelligence business, said, "*We have some of the very best digital capabilities in the market. By bringing them together into one business, we will bring a greater range of capabilities to our customers and capitalize on market opportunities. We will also be able to offer exciting career development opportunities to the most talented people operating in this sector.*"

Existing projects under the new business

The business will specialize in securely collecting, connecting and understanding complex data, so that customers can make can make near-real time decisions in the most demanding multi domain environments. Existing projects include:

- *Developing communication systems which enable military land, air and maritime platforms to communicate with each other to share real-time mission imagery while on operations*
- *Transforming national Automatic Number Plate Recognition (ANPR) technology to prevent crime – the resulting data set involves over 50m ANPR reads per day, with feeds from 11,000 cameras*
- *Delivering satellite and communications technology, which is embedded within the operational infrastructure of major broadcasters globally*
- *Helping the Royal Navy predict failures on warships before they happen and providing detailed analysis of how to diagnose issues;*
- *The 2020 In-Space Missions launch of the world's first commercial satellite 'rideshare' service, Faraday;*
- *Veritas, the product which helps the British Army accurately plan and forecast requirements for equipment and material – significantly improving inventory and fleet management and delivering multi-million-pound savings;*
- *Working with more than 200 financial institutions worldwide to help protect them against financial crime, fraud and cyber crime;*
- *Developing a simulation modelling toolkit for passenger and vehicle security screening, which is used to provide the UK's Department for Transport with a detailed understanding of the impact of different security screening operations at major air and sea ports;*
- *Helping the Royal Navy transform how it gains insight from vast amounts of disparate data, enabling better decision making; and*
- *Creating a mixed vendor 'rainbow team' in Australia to address integrated cloud and data capabilities in a way that will enable global collaboration within multiple geographies for our customers.*

www.baesystems.com

WHAT DOES SHARED SPACE SUSTAINABILITY LOOK LIKE?

Author: Melanie Stricklan, Co-Founder and Chief Executive Officer, Slingshot Aerospace

A revolution is happening above our heads as companies race to take advantage of what is quickly becoming a precious resource — Earth's orbit.

A few years ago, satellites were the size of garbage trucks and cost $400 million. Today, cubesats the size of a loaf of bread are an economical $1 million or less.

This thriving ecosystem has additionally lowered cost and technology barriers of entry with launch and on-orbit services bringing entrants to market faster than ever before experienced. Of the ***$250 billion*** in investment over the last decade, more than half has been secured since 2018.

Alongside this unprecedented growth, society continues to place its future and safety in the hands of the space community. Everyday, we rely on satellite technology.

Satellites help us find our way home, let us binge watch our favorite shows and protect us from domestic and foreign attack. Plus, the use cases for space continue to expand. The space economy is now home to mega-constellations that aim to provide global internet connectivity, ambitious space tourism programs and fleets of Earth Observation (EO) satellites that can help us understand and protect our world.

Earth's orbit offers huge opportunities for innovation and profound advances that could shape the future of humanity. However, the situation is growing increasingly complex for satellite operators to protect these precious assets.

Not only are the number of satellites on-orbit planned to increase exponentially during the next decade, space is also cluttered with 10,000 metric tons of fast-moving debris. The chance of a collision has never been higher.

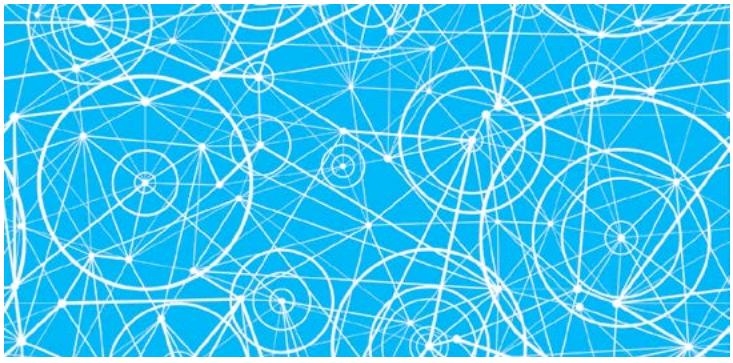
As satellite operators face more risk and less time to take action, they desperately need access to better data and a faster way to coordinate and share information to avoid collisions that put the entire space community in harm's way.

AN EXPONENTIAL RISE IN CONJUNCTIONS

Operating in ***Low Earth Orbit*** (**LEO**) is a high stakes endeavor. It is the most congested orbit with thousands of satellites and millions of pieces of debris flying at speeds of 17,000 miles per hour. At this speed, these objects are making their way around the globe every 90 minutes — additionally, new objects are added into the equation all the time.

Since 2018, there have been 11 major debris generating events. The most recent was a ***Russian ASAT*** test, which sent thousands of ***Kosmos 1408*** fragments of debris into LEO, forcing the ***International Space Station*** crew to take ***evasive action***.

There's far more to come: ***Federal Communications Commission*** (**FCC**) and ***International Telegraph Union*** (**ITU**) filings suggest the number of satellites on-orbit will increase ***by a factor of 25 during the next decade***.



SpaceX's ***Starlink*** constellation will have 12,000 satellites on-orbit by the time that company has completed launching their constellation members. Other companies appear even more ambitious, with some shooting to launch mega-constellations with satellites that number in the tens of thousands.

All of this activity is driving an exponential rise in the number of potential collisions between objects on-orbit.

Today, the ***U.S. Government*** (**USG**) serves a vital role in monitoring the space environment and determining whether two objects have a likelihood of conjuncting. The ***18th Space Control Squadron*** (**18 SPCS**), located on the central coast of California at ***Vandenberg Air Force Base***, leverages a global network of radar telescopes to track space objects on a daily basis and provide the domestic and international operator community information about the risks posed to their assets.

The 18 SPCS scans the skies multiple times a day. They take these radar observations and then forecast which objects are likely to have a conjunction that may warrant a maneuver over the next few days.

Once a potential conjunction passes a certain probability threshold, they generate warnings called ***Conjunction Data Messages*** (**CDMs**) that are sent to operators who sign up for these free alerts.

The 18 SPCS currently generates more than 500,000 of these warnings every single day. For the 800 or so satellite operators with equipment on-orbit, it's no exaggeration to say the status quo is unsustainable.

With every satellite launch, Earth's orbit becomes more dynamic and precarious. In 2019, a defunct Soviet satellite and an eight-ton Soviet rocket body avoided colliding by ***just 95 yards***.

The resulting debris would have doubled the amount of tracked debris in LEO; meaning this single event would have been on par with 60 years' worth of space-debris growth.

For the space-based economy to safely continue on this path, operators have to find a better way to assess risk and coordinate with each other.

Here is one way to think about the situation and how to reduce the risk. On the x-axis we move across the community spectrum, from a single, siloed player to one that is more interconnected with the broader community. On the y-axis, we move from poor and incomplete data, to more accurate, more timely and more complete data. The ideal, and lowest risk quadrant is in the upper right, what we call Shared Sustainability. Here, rich and accurate data is combined from multiple sources. Sophisticated solutions help operators filter the signal from the noise and everyone in this bucket is part of Slingshot's connected community, allowing for simple and timely coordination.

COLLISION AVOIDANCE IN THE AGE OF MEGA CONSTELLATIONS

Much of this assessment and coordination is currently conducted in a manner that undermines the ingenuity of the industry and its operators.

Depending on the number of assets under your control, thousands of CDMs can arrive each day via email or through an in-house API. Judgments then have to be made on which are enough of a high risk to warrant expensive and disruptive maneuvers to avoid damage.

These decisions are often based on limited, low-fidelity data. The result can be an uninformed course of action with potentially ruinous consequences. A case in point is the ***February 2009 collision*** between an active ***Iridium*** satellite and a defunct Russian military satellite — despite calculations predicting the two would miss each other by almost 2,000 feet.

For CDMs involving two stakeholders, the lines of communication are also antiquated. A high-risk conjunction report can lead to a chain of emails while operators resolve the issue and decide who will do what, and when — and that's assuming the operator is able to get in touch with the relevant counterpart.

With more infrastructure being sent into orbit, limited space awareness across the board represents a significant risk to every operator.

There are too many manual processes, barriers to effective communication between stakeholders,and vital operational decisions being made with low fidelity data.

Fortunately, there's a better way. It starts with higher quality data, improved CDM processing and seamless communication between stakeholders. These are the foundations operators need to increase certainty around conjunction outcomes and reduce the number of maneuvers required.

SLINGSHOT BEACON: SHARED SPACE SUSTAINABILITY IN ACTION

Slingshot Beacon is the industry's first, two-sided, communication and collaboration platform. (***See the chart on the previous page***.)

Slingshot ingests and filters the daily avalanche of CDMs and facilitate direct collaboration between space stakeholders. Conjunctions that meet predefined criteria are highlighted, while mission plans, timelines and constraints are shared with all the relevant parties.

The result is a platform that de-risks conjunctions, fosters a more ***sustainable approach*** to operations, and saves satellite owners valuable time.

As commercial, scientific, and military capabilities in orbit scale up, it's useful to think of space awareness across two spectrums: *data depth* and *data sharing*.

Incomplete or low fidelity data is one of the single biggest challenges operators must contend with on a regular basis. Slingshot Beacon enhances the CDM analysis process through the addition of the company's advanced ***Machine Learning*** (**ML**) technology, third-party data sources, intuitive visualizations, and automated filtering.

Even when the data can be trusted, the current level of information sharing between satellite operators is far from ideal. Information silos and standalone processing methods are remnants of the industry's early years. Both reduce interconnection within the space community and add friction where there should, instead, be a shared approach.

Slingshot Beacon includes several collaborative features that push the industry toward a status quo of ***Shared Sustainability***. These include the option of one-to-one contact, community broadcast channels and a step-by-step CDM resolution process built on the transparent exchange of data.

IT PAYS TO WORK SMARTER

The bottom line for operators is that every maneuver comes at a cost. The lifespan of a satellite depends on the efficient use of fuel, while service disruption caused by evasive action can be, well, disruptive.

With rich and accurate data from multiple sources, Slingshot Beacon allows operators to filter the signal from the noise, easily coordinate with each other and only maneuver when such becomes an absolute necessity.

Slingshot Beacon was developed to mitigate risks on-orbit and to enable safer satellite operations for all.

Learn more about Slingshot Beacon at this direct link....

SLINGSHOT AEROSPACE

Author Melanie Stricklan is the Co-Founder and Chief Executive Officer of Slingshot Aerospace.

A worldwide leader in ground station antennas and radomes

CPI has built an industry-leading portfolio of satcom products, featuring integrated offerings from its acquisitions of the former GD SATCOM Technologies, Orbital Systems and Malibu Research antenna businesses and the Radant and ESSCO radome businesses.

Today, CPI offers one of the world's broadest satcom and LOS antenna portfolios, serving GEO, MEO and LEO applications from L-band to Q/V-band. CPI's radome offering is a global leader in breadth and depth.

CPI Satcom & Antenna Technologies Inc.

T: +1 (770) 689-2040 - M-F - 8am-5pm US ET
E: CustomerCareSAT@cpii.com

CPI
Communications & Power Industries

cpii.com/antennas

DISPATCHES

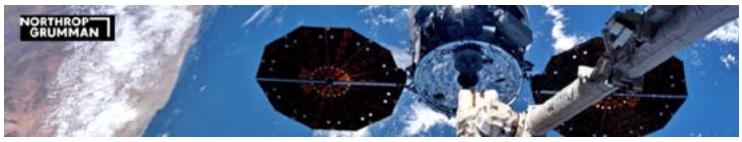
SDA AWARDS CONTRACTS FOR 126 SATELLITES

The *Space Development Agency* (SDA) has awarded three prototype agreements that are worth approximately $1.8 billion to establish the foundation for Tranche 1 Transport Layer (T1TL), a mesh network of 126 optically-interconnected space vehicles (SV) that will provide a resilient, low-latency, high-volume data transport communication system and be ready for launch starting in September 2024.

These agreements are awarded to ***Lockheed Martin Space***, ***Northrop Grumman Space Systems*** and ***York Space Systems*** to each build and demonstrate effectiveness for two, near-polar, Low Earth Orbital (LEO) planes of the six-plane T1TL, which forms the initial warfighting capability tranche of the National Defense Space Architecture (NDSA).

Tranche 1 Transport Layer will leverage and proliferate the capabilities being demonstrated in Tranche 0 Transport Layer with targeted technology enhancements, mission-focused payload configurations, increased integration, and greater production efficiencies. The T1TL will provide global communications access and deliver persistent regional encrypted connectivity in support of warfighter missions around the globe by serving as the backbone for Joint All Domain Command and Control (JADC2) built on low-latency data transport, sensor-to-shooter connectivity, and direct-to-weapon platforms connectivity.

Lockheed Martin Corporation, Littleton, Colorado, is awarded a prototype agreement with a potential value of approximately $700 million to execute a research and development program for the development of a T1TL prototype constellation consisting of 42 satellites in two near-polar low Earth orbital planes (21 SVs for each orbital plane). The proposal was received and evaluated under an Other Transaction Authorities solicitation SDA-PS-22-01. "*Our team at Lockheed Martin is thrilled to be awarded a T1TL contract*," said ***Erik Daehler***, Protected Communications Mission Area leader at Lockheed Martin Space. "*We're looking forward to building upon our team's success on Tranche 0 by approaching Tranche 1 with modernized and streamlined processes that do more, cost less and achieve mission goals faster. Producing these innovative spacecraft will be a collaborative effort, with Lockheed Martin using its longstanding partnerships to deliver high-quality products that will provide the right capabilities to the warfighter.*"



Northrop Grumman Strategic Space Systems, Redondo Beach, California, is awarded a prototype agreement with potential value of approximately $692 million to execute a research and development program for the development of a T1TL prototype constellation consisting of 42 satellites in two near-polar low Earth orbital planes (21 SVs for each orbital plane). The proposal was received and evaluated under an Other Transaction Authorities solicitation SDA-PS-22-01. "*Northrop Grumman recognizes information on the modern battlefield must be delivered to our warfighters at the speed of relevance*," said ***Robert Fleming***, vice president and general manager, Strategic Space Systems. "*Our T1TL solution combines proven end-to-end satellite system integration and heritage communication mission expertise accumulated over decades, across multiple orbital regimes to rapidly field these critical capabilities to warfighters in the field.*"

York Space Systems, Denver, Colorado, is awarded a prototype agreement with a potential value of approximately $382 million to execute a research and development program for the development of a T1TL prototype constellation consisting of 42 satellites in two near-polar low Earth orbital planes (21 SVs for each orbital plane). The proposal was received and evaluated under an Other Transaction Authorities solicitation SDA-PS-22-01. "*We are honored to again have SDA's confidence in executing the agency's vision*," said ***Dirk Wallinger,*** chief executive officer, York Space Systems. "*Their competitive, fixed-price procurements leverage York's private capital investments to deliver low-risk, industry-leading constellations today and well into the future.*"

DISPATCHES

GENERAL ATOMICS SUCCESSFULLY COMPLETES FINAL DESIGN REVIEW FOR USSF WEATHER SYSTEM

General Atomics Electromagnetic Systems (GA-EMS) has successfully completed the *Final Design Review* (FDR) of its spacecraft design for the U.S. Space Force (USSF) Space Systems Command (SSC) *Electro-Optical Infrared* (EO/IR) *Weather System* (EWS) satellite program.

GA-EMS has developed a prototype EWS spacecraft using a reliable, redundant bus with a high performance EO/IR weather sensor payload to support the USSF as it looks to transition from aging on-orbit systems to next generation weather satellites.

As the prime contractor, GA-EMS has assembled a highly experienced, best-in-class team to successfully deliver the EWS satellite design. The team includes **EO Vista, LLC.** to provide the EO/IR weather sensor payload, ***Atmospheric and Environmental Research*** (AER) Inc. for weather product generation, and **Parsons Corporation** (NYSE:PSN) to provide Enterprise Ground Station command and control and operations support.

"*Successfully completing the EWS program FDR is a vital milestone for us*," said ***Scott Forney***, president of GA-EMS. "*We are extremely proud of the team's results to date. Our goal is to be a weather mission partner with USSF by providing the USSF with new, more advanced technologies that ensure essential weather data is delivered to the warfighter and by supporting novel USSF initiatives such as weather data as a service.*"

"*In November 2021, we announced an up-scope of our EWS program efforts to deliver an on-orbit three-to-five-year prototype spacecraft with residual operational capabilities, rather than a one-year sensor demonstrator*," said ***Gregg Burgess,*** vice president of Space Systems at GA-EMS. "*The Defense Meteorological Satellite Program satellites are rapidly reaching end of life. By pivoting to provide operational capability, we enable the Space Force to continue to support the warfighter by filling EO/IR cloud data gaps created as legacy satellites are retired. Our world-class manufacturing, test and integration facilities are ready to meet the critical build and launch timelines for EWS.*"

DISPATCHES

NORTHROP GRUMMAN AWARDED USSF CONTRACT FOR DEEP-SPACE ADVANCED RADAR CAPABILITY

Northrop Grumman Corporation (NYSE: NOC) has been awarded a $341 million contract by the U.S. Space Force (USSF) Space Systems Command (SSC) to develop, test and deliver a Deep-Space Advanced Radar Capability (DARC) in support of its Space Domain Awareness (SDA) mission.

DARC will augment the military's space surveillance network as an additional sensor with increased capacity and capability to monitor deep space objects and eventually provide full global coverage.

The initial DARC contract includes the design, development and delivery of a Site 1 system located in the Indo-Pacific region, expected to be completed in 2025. There will be a follow-on of two additional sites strategically placed around the world.

"*The DARC program will field a resilient ground-based radar providing our nation with significantly enhanced space domain awareness for geostationary orbit,*" said ***Pablo Pezzimenti***, vice president, integrated national systems, Northrop Grumman. "*While current ground-based systems operate at night and can be impacted by weather conditions, DARC will provide an all-weather, 24/7 capability to monitor the highly dynamic and rapidly evolving geosynchronous orbital environment critical to national and global security.*"

SOYUZ LAUNCHES SUSPENDED

Arianespace **is strictly abiding by the sanctions decided by the international community (European Union, United States of America and United Kingdom) following the invasion of Ukraine by Russia.**

As part of the mandate given by the ESA Member States to Arianespace, the operation of the Soyuz launcher from Europe's Spaceport (CSG, French Guiana) and from Baikonur (Kazakhstan) through Starsem are governed by France/Russia inter-governmental agreement and ESA – Roscosmos space agencies agreement.

This operation began after the end of the Soviet Union and has been very successful— up to now. However, it is now challenged by Roscosmos' unilateral decision to withdraw from CSG and suspend all Soyuz launches from Europe's Spaceport. Readied Soyuz launchers and Galileo satellites are in stable configuration and in security.

Regarding ST38 for OneWeb from Baikonur, that launch has been postponed indefinitely, following the conditions posed by Roscosmos to proceed. Arianespace will work with its partners to ensure the well-being of the goods and means currently in Baikonur.

Arianespace is in close contact with its customers and French and European authorities to best assess all the consequences of this situation and develop alternative solutions.

In the meantime, preparation of upcoming Ariane 5 and Vega C campaigns of 2022 are progressing according to plan and schedule.

Taking over from Ariane 5 and Vega, Ariane 6 and Vega C will provide Europe with a sustainable and autonomous access to space. Arianespace is confident in the success of these two launchers, to which it has been strongly committed since ESA's 2014 Ministerial Conference in Luxembourg, on European institutional and global commercial markets.


hisdeSAT
20 ANNIVERSARY
2001 - 2021: Fulfilling goals, building the future up.
Space Communications at the Service of Society
Satellite Communications Services for Government
Hisdesat Servicios Estratégicos.
Paseo de la Castellana, 149, 5th floor - 28046 Madrid - SPAIN
Tel.: +34 914 490 149
www.hisdesat.es

THE KEY COMPONENTS OF MILSATCOM TRANSFORMATION:

Digitization + Virtualization

Author: Dr. Juan Deaton, Senior Research Scientist, Envistacom

Satellite ground networks are in the midst of evolutionary challenges that promise a transformative impact to industry business models and network architectures. Satellite network operators are faced with the demand to create networks capable of operating on a myriad of different waveforms, orbits and constellations — while simultaneously maintaining profitability.

With as many as 50,000 active satellites predicted to be in orbit over the next 10 years, new satellites include ***Low Earth Orbit*** (**LEO**) constellations, such as ***Starlink*** (among others), as well as new ***Medium Earth Orbit*** (**MEO**) and ***Geosynchronous Earth Orbit*** (**GEO**) satellites.

This evolution in the space segment drives the need for SATCOM ground and terminal segments to advance, as well. Specifically, the forward momentum demands resilient and agile networks capable of operating on a myriad of waveforms, orbits and constellations, all the while simultaneously maintaining service quality and operational sustainability.

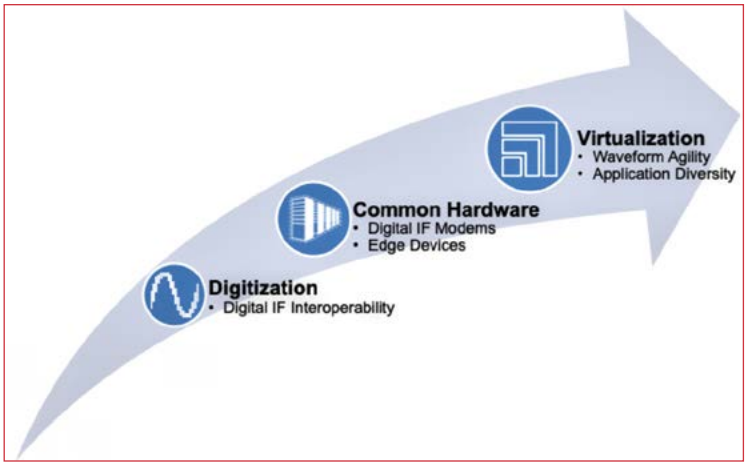
In the past, a restrictive market of purpose-built proprietary modems thrived. These rigid solutions dominated SATCOM ecosystems for decades, but they're now unfit for a rapidly changing space layer. As ***Northern Sky Research*** (**NSR**) recently reported, legacy "*satellite ground networks ... lack the scale and agility necessary to avoid the palpable risk of becoming bottlenecks.*"

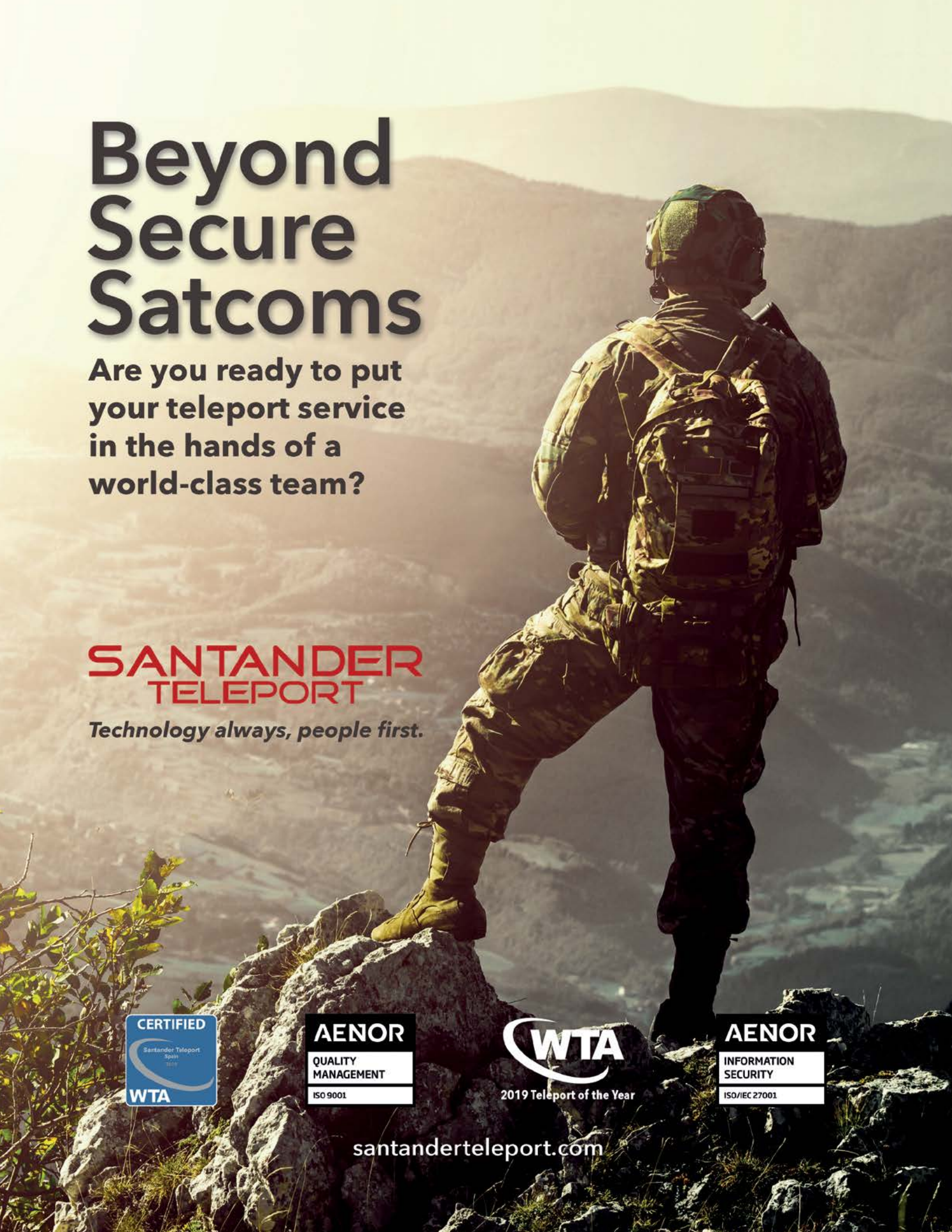
Furthermore, the ***U.S. Space Force*** (**USSF**) in a recent vision document expressed the requirement for agile SATCOM networks and modem terminals — including the ability to seamlessly transition between different SATCOM waveforms, orbits and constellations. The future of satellite communications resides in its ability to become agile and resilient.

THE FIRST STEP: DIGITAL IF

In a world that's largely migrated from analog technologies to digital versions, SATCOM vendors and operators are positioning to digitize SATCOM networks. Specifically, replacing L-band ***Intermediate Frequency*** (**IF**) transmission systems with ***Internet Protocol*** (**IP**)-based interfaces — creating digital IF.

Replacing L-band transmission systems with digital IF stands to improve system RF performance, network agility and resilience. More importantly, digitized SATCOM modems and network architectures can better take advantage of common hardware, which provides the foundation for virtualization.




Beyond Secure Satcoms
Are you ready to put your teleport service in the hands of a world-class team?
SANTANDER TELEPORT
Technology always, people first.
CERTIFIED
Santander Teleport
Spain
WTA
AENOR
QUALITY MANAGEMENT
ISO 9001
WTA
2019 Teleport of the Year
AENOR
INFORMATION SECURITY
ISO/IEC 27001
santanderteleport.com

With the promise of these many benefits, the movement into digital IF is fast underway as an interoperable standard. In September, industry and agencies within the ***Department of Defense*** (**DoD**) came together to form the ***Digital Intermediate Frequency Interoperability*** (**DIFI**) ***Consortium***.

DIFI's mission is to enable the digital transformation of space, satellite and related industries by providing a "*simple, open interoperable Digital IF/RF standard that replaces the natural interoperability of analog IF signals and helps prevent vendor lock-in*."

With the inclusion of 25 satellite industry and major DoD agencies — including the USSF — DIFI continues to attract members and work toward evolving SATCOM network architectures. Through a reliable digital IF transport, communications can extend across greater distances and leverage cloud capabilities.

"*Achieving interoperability across the many networks in the U.S. government that supply, use or consume satellite-related data is a mission critical imperative, especially within the Department of Defense*," ***William Joo***, PEO C4I PMW/A 170 Special Projects Engineer and DIFI's Navy representative, said in a DIFI release. "*This need becomes even more important when looking across systems used by allies around the world*."

FROM DIGITIZATION INTO VIRTUALIZATION

Digitization is a key step that eliminates the need for purpose-built hardware that adds complexity and cost to SATCOM networks.

Some of the biggest sunk costs in SATCOM operations are in buying managing hardware and networks and ensuring their longevity. After all, with every new purchase of purpose-built hardware comes new cost (to purchase, install and operate), new workforce operational needs, additional rack space, and another system to manage and monitor. Using virtualization, several applications and functions can be consolidated into common hardware enabled by digitization.

Instead of buying purpose-built modems for every mission — which costs more over longer design-integrate-deploy lifecycles and stifles innovation — virtualization leverages software migrations instead of hardware migrations.

Virtualization can support numerous functions, eliminating evolutionary bottlenecks that impede faster, less-expensive network migration and reconfiguration—not to mention the development and deployment of continuously emerging technologies.

Performance, agility and resilience are key factors, including for the military efforts under way in ***JADC2*** and in other efforts relying on SATCOM to help provide the competitive edge in the evolving space domain. This can't be done effectively without the rapid scalability, reduced maturation cycles, and reduced barriers to prototyping, testing and deploying new capabilities enabled by virtualized architectures.

Additionally, virtualization accelerates the speed of innovation by fostering a larger pool of competitors where superior functionality can be selected and deployed independent of vendors.

It's clear that digitization and virtualization both promote resilient and agile networks and terminals, which will shape the future of satellite communications. Both concepts provide significant cost savings and increase SATCOM network performance. These principles work well together — a digital IF architecture provides a smooth transition to virtualization, since digital modem processes can now run on common server hardware.

As digitization enables network agility, virtualization enables modem and terminal agility—providing the flexibility and adaptability that will be essential to the continued success and growth of the SATCOM industry.

www.envistacom.com

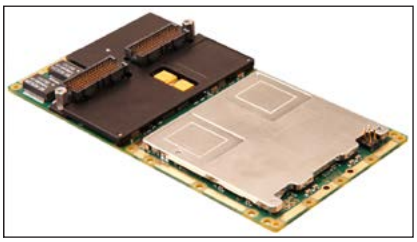
ENVISTACOM

Dr. Juan Deaton

Dr. Juan Deaton is currently a research scientist at Envistacom, where he is using his 20 years of telecom experience to build virtualized transport satellite systems. In his previous employment with Comtech EF Data, he was engaged in a variety of different types of research like anti-jam waveforms, satellite channel models, and developing LDPC codes for Versa FEC 2. Before working at Comtech EF Data, he worked for the Idaho National Lab, where he researched spectrum optimization, spectrum modeling, and emergency communications. Before the INL, Juan worked for Motorola's CDMA network division where he was the recipient of the 2005 CDMA quality award for developing hands-on training for CDMA cellular equipment deployments. His patented and published work includes spectrum sharing in cellular networks, wireless airborne emergency communications, and mobile advertising. His M.S. and Ph.D. degrees were earned from Virginia Tech and BSEE from the University of Idaho.

DISPATCHES

CURTISS-WRIGHT SELECTED TO PROVIDE COST-EFFECTIVE DEFENSE-GRADE SECURITY IP MODULE FOR COTS MODULAR OPEN SYSTEMS



Curtiss-Wright's Defense Solutions **has been selected by a leading defense system integrator to provide its embedded Security IP module technology.**

Under the contract, Curtiss-Wright will supply its ***XMC-528 Mezzanine Card*** for use in multiple sensor system programs. The enhanced ***TrustedCOTS*** (**eTCOTS**™) module speeds the integration of advanced security IP, such as ***Raytheon***'s ***Night Cover***™ product suite and ***Idaho Scientific***'s ***Immunity*** cryptographic products, into new and legacy systems wherever ***XMC*** (**VITA 42/61**) mezzanine cards can be used, including modules designed to align with ***The Open Group Sensor Open Systems Architecture***™ (**SOSA**) and ***U.S. Army's C5ISR/EW Modular Open Suite of Standards*** (**CMOSS**) technical standards.

This makes the XMC-528 a compelling security IP solution for a wide range of system architectures including **ATCA**, rackmount servers with **PCIe** slots, as well as **VME** and **OpenVPX** modules. The value of the contract is $4 million. The lifetime value of the contract is estimated at $25 million.

"*We are very proud that our recently introduced XMC-528 module, in a first major win for this innovative new security IP solution, has been selected to protect critical data and technology on deployed sensor systems*," said ***Chris Wiltsey***, Senior Vice President and General Manager, Curtiss-Wright Defense Solutions.

"*Previously, most security IP solutions have required costly and time-consuming customization of the target military hardware. Now, with the XMC-528 XMC module, system designers can quickly add security to any Curtiss-Wright or third-party module that supports an XMC site, which significantly lowers the cost and time required to bring advanced security IP to embedded electronics.*"

The XMC-528 enables system integrators to add embedded security to fielded systems without a complete redesign.

Using industry standard interfaces, the XMC-528 mezzanine card can be hosted on existing system modules — such as Curtiss-Wright's VME-1910, VPX6-1961, and SOSA-aligned VPX3-1260 single board computers — to implement advanced data protection.

The same security IP suite provided by the XMC-528 mezzanine module can also be integrated directly into the on-board security FPGA resident on Curtiss-Wright's family of security-ready OpenVPX modules — such as the **CHAMP-XD1S 3U** digital signal processor card and soon to be announced next-generation processor modules.

Systems such as high-performance rack-mount servers can be supported with an appropriate **XMC** carrier.

GOVERNMENT SATELLITE REPORT

Prioritizing Space Architecture Resiliency

Author: David Presgraves

A Falcon 9 rocket carrying a GPS III-5 satellite into orbit launches from LC-40 at Cape Canaveral Space Force Station, Fla., June 17, 2021. (Photo by: Airman 1st Class Samuel Becker)

It's almost hard to believe that last month marked the U.S. Space Force's (USSF) second year in operation—especially considering how much the newest military branch has accomplished in such a brief period of time.

So far, USSF has stood up its headquarters, become the 18th member of the Intelligence Community, established three field commands, and has brought on more than 13,000 personnel. These achievements are only a few of the bullet points on the long list of Space Force wins since the organization's inception in late-2019.

One person who has witnessed to all of the branch's successes, setbacks, and growing pains —– since the very beginning — is U.S. Space Force's Chief of Space Operations, ***Gen. John W. "Jay" Raymon***d. Earlier this month, Gen. Raymond joined the ***Mitchell Institute***'s ***Spacepower Advantage Center of Excellence*** for a special ***Schriever Spacepower Forum*** moderated by ***Gen. (Ret.) Kevin P. Chilton***. During their discussion, Gen. Raymond reflected on the Space Force's journey thus far and discussed the service's year-three priorities, which will include a heavy focus on building and implementing a resilient space architecture.

TWO YEARS DOWN

Gen. Raymond opened the forum by expressing that — to him — the first two years of Space Force operations have flown by. From major organizational milestones to force design deployments, he is extremely proud of all the branch has accomplished in just two years.

"*If you look at the body of work that has been done, it's pretty incredible,*" said Gen. Raymond. "*I would have flunked the test if you had told me at the two-year mark we'd have gotten all of this done.*"

Notable achievements that he highlighted included the design and operation of Space Force headquarters, as well as standing up the branch's field commands — ***Space Operations Command***, ***Space Systems Command*** and the ***Space Training and Readiness Command*** (**STARCOM**).

Developing a new capability program was also a priority during Space Force's first two years. "*One of the big discussion points, when we were looking to establish a separate service, was how do you build capability at speed*," said Gen. Raymond. "*How do you get warfighting capabilities in the hands of our operators at tactically relevant timelines?*"

Satellite Managed Services Take Off

Author: Ryan Schradin

Arianespace preparing to lift the SES-17 satellite to orbit via an Ariane 5 launch vehicle.

For decades, the United States government and military have leased commercial satellite capacity on what is often referred to as the "spot market." This leased capacity was often purchased as needed from the leftover capacity in a region, and at a premium to the user.

However, there is a new approach to acquiring commercial satellite services that is rapidly gaining traction across the government — a movement toward satellite managed services — that promises to bring more innovative, more affordable satellite solutions to government users. As the government begins to shift from leased capacity to this new "***Satellite as a Service***" approach to satellite acquisition, commercial satellite providers are working to introduce exciting new technologies that can deliver the added resiliency, scalability, and flexibility needed to meet the demands of government users.

One of these providers — ***SES Government Solutions*** (**SES GS**)— has invested heavily into new systems and satellites that will enable the company to deliver high-throughput satellite connectivity to government users from multiple orbits, ensuring that its satellite service offering will be capable of meeting even the most bandwidth-hungry missions that absolutely demand assurance and resiliency.

A cornerstone in the company's plan to offer multi-orbit connectivity to government users as a service is the ***recently-launched SES-17 satellite***, a revolutionary ***High-Throughput Satellite*** (**HTS**) that was sent into orbit in October of last year.

To learn more about the SES-17 satellite, why the company refers to it as a satellite that was "*built for managed services*," and what makes satellite managed services so attractive to the United States government and military, ***Amit Katti*** and ***Rashid Neighbors*** offered their insights.

> ***SES-17 was launched in late October, but that doesn't necessarily mean that it's in use already, correct? What is the current status of the SES-17 satellite, and when is it expected to go into service?***

Amit Katti: SES-17 was successfully launched onboard an Ariane 5 launcher operated by Arianespace from a spaceport in Kourou, French Guiana on October 23, 2021.

Carolyn Cuppernull: SES-17 is going through on-orbit testing for optimal performance, with the goal to commence services on June 15, 2022 — anticipate that SES-17 will commence service in about four months.

"One thing is for certain, if the resilient satellite architecture that Gen. Raymond envisions is to be a reality, the Space Force…is going to need to embrace a network that combines both MILSATCOM and COMSATCOM resources."

During the past two years, Gen. Raymond learned that the acquisition component of providing warfighting capabilities is just a part of a much bigger process. He explained that in order to effectively and efficiently provide capabilities at speed, the approach must include force design, requirements, acquisition, and testing.

On the force design, requirements and acquisition fronts, Gen. Raymond expressed that he feels very comfortable with where the Space Force currently stands. He did admit that Space Force's testing program was not robust — initially — but he happily shared that the service now has a testing program that will fully mature in 2022. *"So, on the capability development front, I couldn't be more thrilled with where we are,"* said Gen. Raymond.

Gen. Raymond also gave an update on the growth of Space Force's international partnerships. He shared that he is extremely pleased with how the branch has largely transformed its partnerships from being one-way data sharing to being two-way, operationally-focused data sharing.

He went on to say that USSF and U.S. allies are now exercising and wargaming together, as well as collaborating to develop tactics, techniques and procedures that link their operational centers together. Through these partnerships, the service is now in a position to develop new capabilities that will be provided to the warfighter. *"I really believe we have an opportunity to bring our international partners and commercial industry more into the fold…going forward,"* he said.

One of the more intriguing updates that Gen. Raymond shared concerned the first budget that the Space Force drafted and submitted on its own. *"I think once that budget is released, you'll see a very bold budget as it relates to space and being able to shift to a more resilient architecture."*

A TOP PRIORITY: RESILIENCE

As for what's in store for Space Force's third year of operation, Gen. Raymond believes that, *"year three is going to be even more consequential than year two."* One reason why he thinks 2022 will be pivotal is due to the fact that Space Force plans to fully migrate to a resilient space architecture this year.

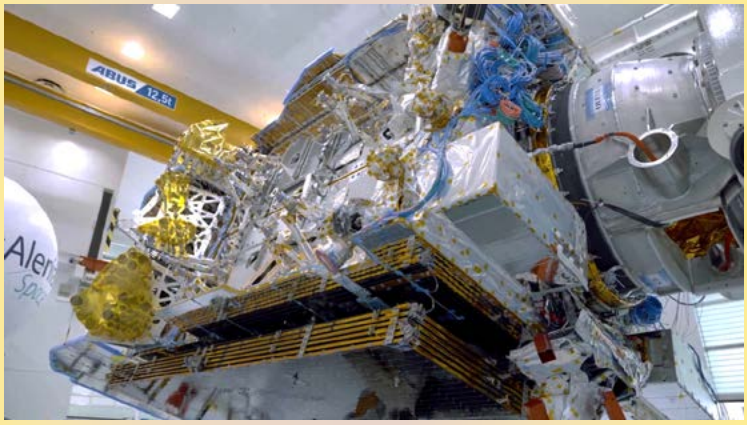
"We have got to shift the space architecture from a handful of exquisite capabilities that are very hard to defend to a more robust, more resilient architecture by design," said Gen. Raymond. And, according to the General, resiliency is the key factor to deterring U.S. adversaries from denying Space Force capabilities and benefits.

"People ask me all the time about deterrence," said Gen. Raymond. *"We very firmly believe that space can amplify those deterrence messages." He explained that ensuring the resiliency and readiness of U.S. assets in space would make it extremely difficult for an adversary to deny Space Force's access to its capabilities and advantages. But it's not just about innovation. Integrating COMSATCOM services into an integrated MILSATCOM and COMSATCOM satellite architecture will have the added bonus of baking resiliency into the military's networks. We will begin our pivot significantly to a resilient architecture this next year. I will tell you, our first priority is a resilient priority. That's been the majority of our focus for this year."*

One thing is for certain — if the resilient satellite architecture that Gen. Raymond envisions is to be a reality, the USSF — and broader ***Department of Defense*** (**DoD**) — is going to need to embrace a network that combines both MILSATCOM and COMSATCOM resources.

THE KEY TO RESILIENCY — INTEGRATED ARCHITECTURE

It's understandable why the military is so laser-focused on resiliency for their networks and satellite communications. Satellite has long been a tactical advantage that our military has over our adversaries, and that tactical advantage only grows as satellite — and the technology it enables — becomes increasingly mission-critical at the tip of the spear.



Recently, when SES has talked about the exciting new technologies that it's implementing in its spacecraft and ground segment, the company is touting its upcoming O3b mPOWER MEO satellite solution. Is SES-17 a part of that? If not, what is the difference?

Rashid Neighbors: SES' O3b mPOWER service is a low-latency, high throughput satellite service offering that is anticipated to launch in Q1 of 2022. That service uses ***HTS*** at an orbit closer to Earth — at MEO — to deliver incredibly high throughputs at extremely low latency. While SES-17 is an HTS, much like the satellites that power the O3b mPOWER service, it will operate in GEO.

There are many reasons why a government agency or military organization would want to use a commercial satellite service delivered from GEO. Depending on the mission and the use case, a GEO satellite solution with a larger coverage area may be ideal. Or the data being transferred via the satellite may not suffer from slightly higher latency — such as voice data.

Ultimately, our intent is to provide the U.S. Government with highly resilient, multi-orbit hybrid satellite solutions. While the spacecraft technology in SES-17 and the O3b mPOWER satellites is fundamentally different, the ground system will be integrated through a centralized system called ***ARC***. This allows our government customers to focus on their mission and applications and let SES GS worry about how the transport works.

You mentioned a system called ARC. What is that specifically, and what does it do?

Amit Katti: ARC functions like the motherboard for a computer. It basically creates a common interface for different processing units.

With ARC, we can coordinate mission assurance across different technologies and orbits. We can also manage the space and ground segment resources, together, for our U.S. government and military customers.

In past conversations, you referred to SES-17 as a satellite built for managed services. How is a satellite managed service different from how the government and military have traditionally acquired satellite capacity? Why would the government and military want to make a move towards managed services?

Carolyn Cuppernull: Typically, the government has worked with multiple commercial satellite service providers to lease or purchase wholesale bandwidth that it then distributes to its users, as needed. Ultimately, this system of purchasing capacity on the spot market was expensive for the government and limited its ability to leverage new technologies being leveraged by the commercial satellite industry.

A recent trend that we're seeing in the government and military is a movement toward a managed service model. In this model, everything that is necessary for an end-to-end satellite network is delivered as a service. The satellite capacity, the ground hardware — including terminals and antennas — are all included in the service.

Rashid Neighbors: With a managed service model for satellite services, the government would always have the latest commercial technologies and solutions available to them. With systems like ARC in place, they'll also have the added resiliency and capability of being able to leverage a multi-orbit constellation. This means they would have access to low-latency,

For years, the DoD's trusted industry partners in the space and satellite sector have been pushing for the military to move away from purchasing, launching, and managing purpose-built military communications satellites. They've been, instead, encouraging the military to leverage commercial capacity to meet its communications requirements – and with good reason.

The commercial space and satellite industries are the innovation leaders in that domain. By embracing commercial satellite capacity for its mission-critical communications requirements, the military is gaining access to the innovative and cutting-edge technologies in which the commercial satellite industry has been investing heavily over the past few decades.

"*We will begin our pivot significantly to a resilient architecture this next year. I will tell you, our first priority is a resilient priority. That's been the majority of our focus for this year,*" said Gen. Raymond

However, it's not just about innovation. Integrating COMSATCOM services into an integrated MILSATCOM and COMSATCOM satellite architecture will have the added bonus of baking resiliency into the military's networks.

There are more than 150 commercial satellites orbiting the Earth in MEO and GEO. By using commercial partners to meet communications requirements, the military can both bake redundancy into their satellite networks, and make it more difficult for adversaries to target satellites for jamming and kinetic attacks.

In a recent interview with the ***Government Satellite Report***, ***Hughes Defense***'s ***Rick Lober*** emphasized how commercial satellite capabilities can be game-changers for ensuring resilient military communications and mission assurance.

"*Only by being able to switch seamlessly from satellite to satellite can the user be assured of uninterrupted communications,*" said Lober. "*Being able to switch between satellites in different orbit planes provides greater network resiliency and gives commanders more options to enhance their APACE communications. Having a diversity of satellites allows for optimizing the best solution set while making the network more robust.*"

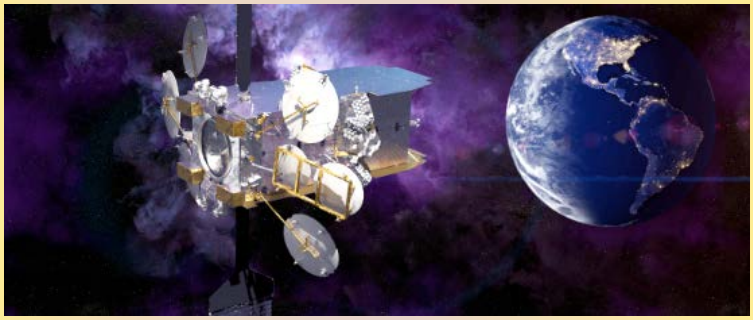
Amit Katti, Principal Engineer at SES GS, echoed Lober's sentiment in a recent interview about ***SES GS' new Common Operational Picture platform***, ***Hydra***. *"If an adversary denies a satellite — either disables it with a kinetic attack or jams its signal — having the ability to manage and control the network to send traffic around that satellite — either to other available military satellites or commercial satellites – could be the difference between having comms and not having comms."*

Select this direct link to watch the Schriever Spacepower Forum video in its entirety.

*Author David Presgraves is the Executive Editor of **GovDesignHub**, and Staff Writer for **GovCyberHub**, **GovDevSecOpsHub**, The Last Mile, and the **Government Satellite Report;** Senior Associate at **Strategic Communications Group***

*This article was first published on **GovSat** and is republished in MilsatMagazine with the publication's and **SES GS**' permission.*

David Presgraves



Artistic rendition of the SES-17 satellite on-orbit.

high-throughput connectivity from MEO, as well as wideband high-throughput connectivity from GEO, and they would be able to seamlessly switch between those resources based on their mission requirements.

The government and military rarely operate in static conditions. The environment changes, the mission shifts and evolves. Having a satellite managed service that gives them access to the latest and greatest technologies, as well as a multi-orbit satellite constellation ensures that they'll always have the communications and connectivity they need to accomplish their mission – even if mission parameters or requirements change.

The technologies in SES-17, and the development of the ARC system, make this satellite a natural fit for the "*Satellite as a Service*" model, as it enables us to listen to the government's and military's requirements, and tailor a multi-orbit satellite solution that meets their needs and helps them accomplish their mission.

What is the coverage area of SES-17? Where will the government and military be able to leverage the services of this satellite, in particular?

Amit Katti: SES-17 will service the majority of North and South America. The satellite will also provide coverage to an area that is of incredible importance to the U.S. Department of Defense (DoD), delivering services to parts of the Arctic Circle. Coverage will extend east into Africa, and cover a large part of Europe, as well.

SES-17 also offers coverage over much of the Atlantic Ocean, delivering seamless connectivity for maritime and air travel between the Americas and Europe.

To learn more about SES-17 and its potential to enable multi-orbit satellite managed services to the government and military, select this direct link...

*Author Ryan Schradin is the Executive Editor of **Government Satellite Report.***

*This article was first published on **GovSat** and is republished in MilsatMagazine with the publication's and **SES GS**' permission.*

Ryan Schradin

the **TECHNOLOGY LEADER** in **WIRELESS LINK OPTIMIZATION**

- Recognized leader for satellite-based acceleration and wireless link optimization
- Best quality of experience to the end user
- XipOS provides the highest link utilization and bandwidth capacity to the network operator
- Both small and extremely high capacities up to tens of Gigabits per second
- Hybrid Networks - Interconnect GEO, NGEO, cellular data, terrestrial wireless and wireline links into one optimized network with ultimate bandwidth flexibility!

MARITIME

CELLULAR BACKHAUL

MILITARY & GOVERNMENT

VSAT NETWORKS

HYBRID NETWORKS

XipLink™
Better. Wireless.

@SATELLITE2022 VISIT US AT BOOTH 202

xiplink.com | **855-408-2483**

SECURE WIRELESS SOLUTIONS FOR TACTICAL, EXPEDITIONARY + DEPLOYABLE COMMS

Author: Dominic Perez, Curtiss-Wright Defense Solutions

U.S. Department of Defense (DoD) tactical/expeditionary networking and command post programs have a widely-acknowledged the critical need to improve mobility. The current state of the art for tent-based command posts requires hours or days of setup, which includes thousands of feet of copper wiring that delays network availability.

To enable mobility for warfighting, the ***National Security Agency*** (**NSA**) established a program (*with a set of guidelines*) called "***Commercial Solutions for Classified***" (**CSfC**). CSfC-based mobility solutions are currently being fielded by the U.S. Marine Corps and by U.S. Army programs of record to provide command post mobility and soldier dismounted situational awareness, including using ground vehicles as network nodes and mobile command posts. However, the extensive requirements and processes involved are complex and not well-understood. This article compares various CSfC network architectures and proposes several approaches for CSfC solutions optimized for mobility use cases.

CSfC enables access to classified information using inexpensive, commercial technologies. This enables entirely new classes of wireless access to classified networks for warfighting and lets U.S. coalition partners access classified information without taking possession of ***controlled cryptographic items*** (**CCI**). The use of CSfC significantly reduces equipment costs and simplifies key management, equipment handling and security procedures.

CSfC guidelines provide configuration options that allow classified data to be transmitted using two layers of ***Commercial-Off-The-Shelf*** (**COTS**) encryption products. Previously, the only way to transmit classified data was by using expensive, controlled, military grade encryption devices, such as **TACLANEs** *(Tactical FASTLANE, or, Tactical Local Area Network Encryption and protects networks against threats as well as defends assets across all domains)* and **KG-250s** *(Type 1 network encryptor)*.

CSfC mobility and wireless solutions provide enormous potential to enable command post mobility and soldier- dismounted situational awareness, including the use of ground vehicles as radio nodes. Research and design for such use cases are currently underway. In order to satisfy CSfC and DoD guidelines for classified networking, systems integrators and technology developers must meet an extensive set of requirements and processes that are both complex and not well-understood.

This article describes, compares, and contrasts various CSfC network architectures and proposes several approaches for CSfC solutions optimized for tactical networks and mobility use cases.

CSFC ARCHITECTURE + PROCESS

Using CSfC, classified information can be transmitted over untrusted wireless networks such as **Wi-Fi**, **LTE**, and **SATCOM**, including public, government, and partner networks. This is achieved by using two sets of encryption technologies, one layered inside the other.

Approved configurations include encryption using **VPN inside VPN**, **VPN inside Wi-Fi WPA2**, **MACsec inside VPN**, and **TLS inside VPN**.

Though layered encryption is straightforward in concept, full CSfC implementations must include a breadth of technologies, including ***public key infrastructure*** (**PKI**), encryption gateways and clients, authentication systems, cybersecurity technologies, and secure network infrastructure. Additionally, to successfully field systems, the CSfC program requires organizations to follow a well-defined process.

CSFC PROGRAM OVERVIEW

Organizations can select from the following CSfC-related technology and process components to create integrated solutions that enable classified networking over radio infrastructure such as SATCOM, Wi-Fi, LTE, or LMR, enabling vehicles to communicate with upper echelons/HQ, or enabling soldiers to use mobile devices such as laptops, tablets or smartphones, in transit, at-the-halt, and in dismounted use cases.

- ***Cryptographic Primitives: the approved algorithms and mathematics that the CSfC specifies for transmission of classified information***
- ***Encryption Protocols: are approved to conduct communications between devices that transmit encrypted data. Most used today are VPN solutions providing data-in-transit encryption***
- ***DAR (Data-at-Rest): encryption technology used to encrypt data stored on media such as hard drives, flash drives, etc.***
- ***Public Key Infrastructure (PKI): the approved technologies and protocols required to manage trust, encryption key generation, and sharing***
- ***Key Validation and Testing Processes: required by the CSfC program in order to comply with CSfC rules***

DETAILED CSFC ARCHITECTURES (CAPABILITIES PACKAGES)

There are several main CSfC architectures for transmitting classified information over ***Wide Area Networks*** (**WAN**) and ***Wireless Local Area Network*** (**WLAN**) infrastructure, depending on the desired use cases. These architectures are specified in "*Capability Packages*" that outline — in great detail — the components, configurations, processes, and testing required by the government before they will approve the use of a system. The following architectures are most suited for use in tactical/expeditionary use cases, for both WAN communications with upper echelons/HQ or teleport sites, and WLAN communications for short-range communications with end-user devices.

A. Multi-Site Connectivity Capability Package

This configuration provides the ability to use any type of wireless transport for network WAN access, including SATCOM, Wi-Fi, LTE, or other radio types, so that deployed, remote CSfC gateways may include a minimum of deployed equipment. This architecture depicts the ***Multi-Site Connectivity Package Access Capability Package***[1], with a ***Central Management Site*** (**NOSC**) and a remotely-managed site using two layers of IPsec VPN encryption

This architecture also allows for multiple network classifications sharing a gray network and transport infrastructure. In the case of ground vehicles, the remote system could be vehicle-mounted. Depending on the number and type of networks being accessed, as well as bandwidth requirements, the remote system could comprise just two small vehicle-mounted or soldier-carried VPN gateways.

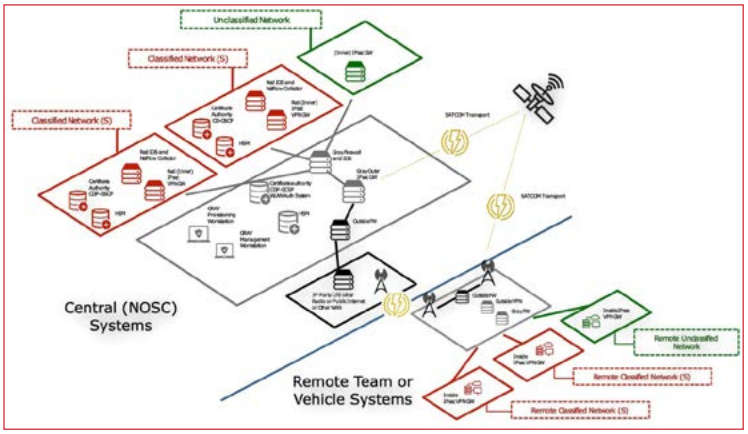


Figure 1. WAN encryption using dual VPN MSC CP.

B. Campus WLAN Capability Package

For organizations looking to develop fly-away or vehicle-mounted classified WLAN systems that can enable at-the-halt or on-the-move and dismounted ***situational awareness*** (**SA**) over short distances, the Campus WLAN Capability Package[2] architecture is an option. The architecture above assumes a pre-existing WAN encryption solution and adds the deployment of Wi-Fi so that ***end-user devices*** (**EUDs**) can be used on a wireless LAN with access to classified information.

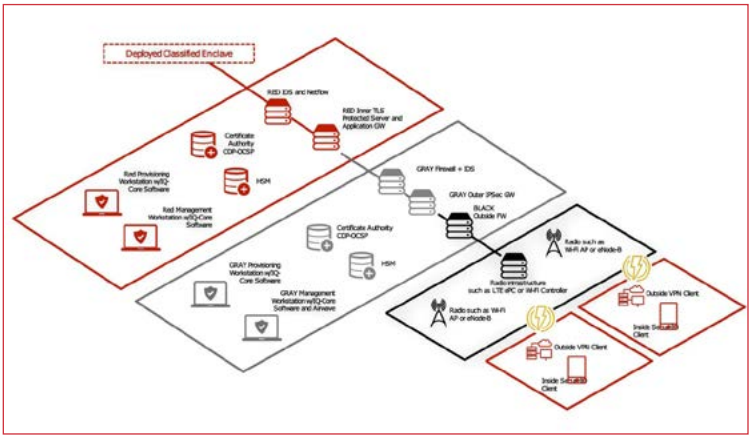


Figure 2. WLAN encryption using Wi-Fi WLAN CP.

This architecture uses the Campus WLAN Capability Package, using built-in, commercial, Wi-Fi stack (*supplicant*) and OS security on the EUD to provide one layer of the required two-layer package. The architecture uses a single IPsec VPN client on the EUD to provide the second, inner encryption layer. This architecture provides for a straightforward EUD configuration using well-tested approaches.

C. Mobile Access Capability Package with VPN EUD

For organizations looking to deploy classified wireless systems supporting longer distances, the Mobile Access Capability Package (**MA CP**)[3] is an option. MA CP can enable on-the-move and dismounted SA over distances longer than Wi-Fi radios can support.

The architecture pictured in ***Figure 2*** assumes a pre-existing WAN encryption solution and adds the deployment of fly-away or vehicle-mounted radios (of any type) so EUDs can be deployed using wireless with access to classified information at longer distances. Rather than depending on the Wi-Fi supplicant on EUDs, this architecture requires two layers of VPN encryption, and is radio/transport-independent.

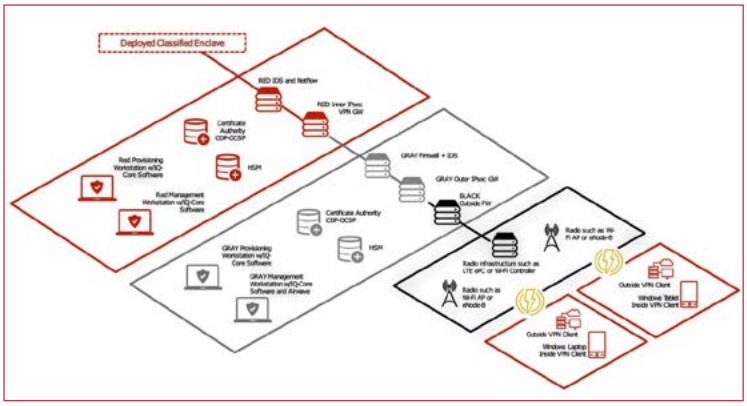


Figure 3. WLAN encryption using any radio via MA CP VPN EUD.

D. Mobile Access Capability Package with TLS EUD

For organizations looking to deploy classified networking for use cases similar to the Mobile Access Capability Package (MA CP) [3] VPN EUD above, but wishing to overcome hypervisor separation requirements, using the TLS- EUD architecture is an option. This architecture depicts the Mobile Access Capability Package v2.1 using one layer of VPN encryption (outside) and a second layer of TLS and/or **SRTP** (***Secure Real-time Transport Protocol***) (*inside*) to provide select voice and data access to mobile devices over wireless infrastructure. This architecture is referred to as **MA CP TLS-EUD** for TLS encrypted EUD access. This architecture is similar to the MA CP VPN EUD described above, but replaces the inner layer of encryption with a TLS-encrypted server for the inner encryption component and a TLS-encrypted application on the client EUD.

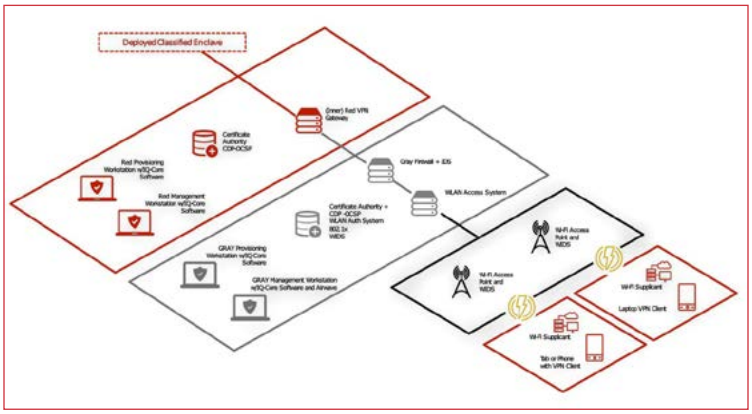


Figure 4. WLAN Encryption Using Any Radio via MA CP TLS.

TECHNOLOGY SELECTION + DEPLOYMENT CONSIDERATIONS

While CSfC solutions can transform communications for the soldier by enabling classified networking over wireless infrastructure, they have two significant issues: size and complexity. The CSfC program requires that solutions include comprehensive suites of security technologies at the command post or datacenter, and that the technologies be provided by different vendors. With the number of required components in CSfC systems, vehicle integration can be a challenge due to the size, weight, and power (SWaP) limitations imposed by vehicles. The diversity of equipment also creates a system configuration, management, and training burden that many organizations are under-equipped to manage. The following sections address methods to mitigate these challenges.

Size, Weight, and Power

All else being equal, communications equipment can never be too small, too light, or too power-efficient. In contrast to legacy, data-center style 19" rack mount equipment, new generations of equipment designed for tactical/expeditionary use are becoming available for use with enterprise-grade networking and security technologies. Additionally, with network function virtualization, many required technologies may be co-located on a single server platform, such as the one shown below.

For example, new tactical equipment, as compared to legacy 19" rack mount equipment, on average:

» *+ Is 10.4 times lighter than a typical 1ru server*

» *+ Is 12.4 times smaller than a typical 1ru server*

» *+ Consumes up to 18 times less power*

These types of low SWaP solutions enable maximum program flexibility, enabling vehicle-mounted, roll-on/roll- off, fly-away, and stationary use cases, all using the same hardware platform.

Figure 5. Depiction of SWaP savings made possible with PacStar Small Form Factor Devices

SWAP SAVINGS MADE POSSIBLE

To ensure reliable uptime of CSfC solutions in vehicle mount applications, components should be selected that have completed and passed **MIL-STD** testing appropriate for vehicle-mounted use cases, including for environment, EMI, and power (**MIL-STD-810G/H** and **MIL-STD-461F/G**). These tests should have been conducted by independent, outside laboratories, and, where applicable, with the equipment powered on and operating.

Some manufacturers may cut corners on tests, test to a subset of these standards, or simply claim products are "*designed for MIL-STD 810*," leaving considerable schedule and project cost risk, since a complete set of independently validated test reports will be required before fielding solutions by government agencies.

Organizations should consider solutions that have undergone at least:

+ (18) types of MIL-STD-810G/H environmental tests, including vibration in a variety of vehicles (ground, helicopter, etc.), shock, crash safety, high/ low temperature, humidity, altitude, acceleration, blowing sand/dust, and explosive atmosphere – at the component and chassis level.

+ (7) types of MIL-STD-461F/G EMI tests, including radiated emissions, radiated susceptibility, conducted emissions, conducted susceptibility — at the entire solution level.

Figure 6. Rugged PacStar communications equipment mounted on a U.S. Marine Corps. JLTV

PACKAGING

The government continues to evolve CSfC guidelines, frequently adding requirements as threats evolve and technology improves. Organizations looking to deploy CSfC solutions should consider modular systems that are flexible and easily upgradeable, avoiding costly fork-lift replacements, supply chain, and logistical rework.

Currently, there are options available that address these needs through modular design, including vehicular rack mount solutions. Some solutions include the ability to replace modules without requiring tools. Some systems include completely dismountable solutions with a built-in UPS.

CONFIGURATION MANAGEMENT AND MONITORING

To address the added complexity and training burden imposed by the two layers of encryption and extensive security requirements, organizations should consider CSfC-focused configuration management tools, such as ***PacStar IQ-Core® Crypto Manager***. IQ-Core Crypto Manager simplifies the setup, configuration, and management of the underlying equipment and devices used in CSfC solutions.

IQ-Core Crypto Manager can provide a base level of capabilities, including:

+ Simplifying the deployment of CSfC solutions, with attendant benefits, while reducing the amount of added complexity and training

+ Providing a unified interface ("a single pane of glass") to underlying equipment from multiple vendors

+ Providing a means to monitor multiple sets of equipment, in fixed/branch offices and tactical settings, enabling lightly trained operators to manage the equipment

IQ-Core Crypto Manager

Organizations should consider functionality specifically designed to make CSfC manageable, including:

VPN Setup Wizards

VPN setup and certificate generation wizards reduce the complexity of providing the correct information to the devices involved in CSfC encryption by providing step-by-step wizards, insulating lightly-trained users from dealing with the command line interfaces and multiple UIs across the underlying devices.

VPN Monitoring/Troubleshooting

VPN monitoring capabilities include the ability to display, in real time, the connection and configuration status of one or more VPN devices. Status indicators should include status of the active authentication and bulk encryption settings in use, ensuring the connection follows CSfC guidelines.

CERTIFICATE MANAGEMENT

Management capabilities include automating the process of managing device certificates, a process that is error-prone, and requires extensive training. Reducing the opportunity for errors in this process helps ensure uptime and allows security administrators to focus on more important tasks.

Capabilities related to certificates should include:

+ Generation of certificate signing requests

+ Display of certificate details and expiration dates, including expiration alerts

+ Encrypted transmission of certificate signing requests

+ Management of the signing process at either the deployed systems or at the NOSC

+ Management/monitoring of certificate authorities

+ Certificate revocation checking via built-in OCSP and CDP functions

By using IQ-Core Crypto Manager as described, the U.S. Army is deploying CSfC solutions and gaining the benefits of Wi-Fi in tactical settings, reducing command post setup time and enabling new classes of wireless applications, while limiting management complexity and training burdens.

Dominic Perez

Dominic Perez, CISSP is the CTO at Curtiss-Wright Defense Solutions and a Curtiss-Wright Technical Fellow, with PacStar since 2008 he joined Curtiss-Wright through their acquisition of PacStar in 2020. In the past 13 years, he has supported development of PacStar's rugged, tactical hardware and IQ-Core Software serving as the subject matter expert for compute, virtualization and virtualized network functions. Dominic is part of the team that won tactical networking equipment and software awards for numerous DoD tactical programs including the US Army T2C2, US Army SFAB, US Army ESB-E, PM TN Secure Wireless Small Form Factor, PEO-C3T TCNO, and US Marine Corps NOTM vehicle-mount and deployable communications programs.

Dominic currently leads the teams developing Curtiss-Wright's PacStar Commercial Solutions for Classified, Modular Data Center, and Tactical Fusion System product lines deploying cutting edge secure communications, edge data processing, and rapid sensor to shooter situational awareness to the warfighter at the tactical edge systems in the face of disconnected, limited, and intermittent (DIL) comms environments.

Prior to PacStar, Dominic worked for Biamp where he created automated testing infrastructure for the hardware, firmware and software powering their network distributed audio, teleconferencing and paging systems. Dominic studied mechanical engineering and computer science at Oregon State University. He currently holds multiple professional certifications from VMware in Data Center Administration; Cisco in Design, Security, and Routing/Switching; and EC Council and ISC2 in Security.

www.curtisswrightds.com

INTERFERENCE: THE CRITICAL THREAT TO DEFENSE NETWORKS

Author: Juan Manuel Martinez, Technical Director, INTEGRASYS

The MILSATCOM industry is experiencing a formidable challenge, that being the crucial resiliency of networks for mission assurance. According to Euroconsult, in 2021, $6.6 billion were spent on government telecommunications programs, $3.6 billion of this amount was spent on secured satellite communications (SATCOM).

The need to guarantee the security of the network has led to an opportunity for new technologies, which are the key enabler and offer militaries a reliable environment for their communications. Due to the frenzied activity in hostile environments that are carried out by brigades, efficient communications has become essential.

The problems derived from ***RF interference*** (**RFI**), whether generated intentionally or not, are one of the main MILSATCOM. RFI hinders the reception of message to and from command and can cause irreparable miscommunication and that can lead to mission disasters. If RFI affects TT&C links needed for proper satellite control, as well as the disruption associated with payload links, this becomes even more of a potential concern for the military sector.

As the interference cancellation problems are affecting so much of what militaries need to accomplish, the need for new, anti-interference and anti-jamming techniques is high on the development list. The resulting technolgies must be fully effective, in real-time and in any situation, and fully comply with the militaries' demands for service optimization.

RF Interferences are treated as a threat; however, the problem is that, due to the congested comms environment, there are intentional interferences that are extremely dangerous due to the disruption they cause, as well as unintentional interferences that have become a critical issue when military activity is located in a conflict area with coexisting, different networks.

Over the years, new solutions have been created that are able to protect waveforms by incurring extra bandwidth resources to offset potential interoperability problems. Some solutions offer physical, layer fingerprinting of emissions that are complete with operational information. Ad-hoc coordination of databases, or the development of sophisticated and expensive interference geolocation systems, continue to be developed.

Existing tool sets can resolve some interference types, but at the expense of technical resources and incurring possible performance degradation. The main problem with these interference techniques is the poor use of resources, not only at the monetary level, but also at the operational level.

When referring to defence critical missions, the battlespace stands out, rarely are warfighter resources dedicated to dealing with RF interferences and the maintenance of ground terminals.

To enhance the network for "*protected communications*" whose users manage critical infrastructures, government assets, communications for security forces and so on, as well as all satellites/payload control operators, the technologies that are required to protect the links effectively against unintentional or intentional (jamming) interference to achieve maximum service availability and robustness must take into account both types of previously mentioned interferences, be able to handle equipment issues as well as offset operator errors.

Integrasys has now developed a new tool that is able to cancel interferences, such as 5G, congested networks, or jamming. The solution is ***CLEANRF*** — this is an elegant solution that negates costly interference conflicts, avoids cumbersome frequency coordination as well as elusive interference localization procedures, thereby maximizing the amount of usable, clean spectrum.

CLEANRF allows for the detection, identification, separation, and cancellation of RFI sources that affect the service signal being processed by receivers or transceivers that are operating with the satellite links. This offering enables satellite terminals to coexist with satellite and terrestrial interferences.

CLEANRF can effectively cancel a significant number of harmful interference sources on satellite-to-ground links for GEO, MEO and LEO satellites. Moreover, CLEANRF is the only technology capable of canceling 5G over C-band interferences, a problem that is on the rise in many developed countries and severely affecting the satellite industry. The CLEANRF solution enables secure and robust communications and protects network terminals from the most common, interference sources.

The MILSATCOM industry needs to count on reliable, real-time and efficient communications to achieve high performance when operating in conflicted and congested areas. Technology companies, such as INTEGRASYS, continue to innovate in cancellation technology for satellite signals, with the main aim being to contribute to ensuring high-quality communication that is secure, accurate and providing quick response.

www.integrasys-space.com

INTEGRASYS


37TH SPACE SYMPOSIUM
SPACE FOUNDATION
April 4-7, 2022
Colorado Springs, Colorado | USA
New Business Opportunities
World Class Networking
Space Industry Experts
Be Connected. Anywhere.
Reserve Your Space!
www.spacesymposium.org
+1.800.691.4000 | #37Space #SpaceSymposium

SOFTWARE DEFINED RADIO FOR DATA STREAMING

Raw RF data (IQ Pairs) Vs. Processed Digital RF Data in SDR Applications

Software defined radios (SDRs) are radio communication systems that carry out certain processes in RF communication typically performed by hardware, such as modulation, demodulation, and signal processing, using software instead. An SDR comprises a flexible radio front end (RFE) and a digital back end.

The RFE, which is responsible for all receive (Rx) and transmit (Tx) functions, typically contains amplifiers, filters, mixers, and analog-digital/digital-analog converters (ADC/DAC). The digital backend comprises an FPGA with DSP capabilities and is responsible for digital modulation/demodulation, upconverting/downconverting, signal processing, and data packetization/transfer.

After a signal is received, prepared, and converted by the RFE, the next step before signal processing is demodulation. Similarly, digital signals to be transmitted have to be modulated before conversion, preparation, and transmission by the radio front end. There are various schemes used in telecommunications for digital modulation/demodulation, with the most commonly used in SDRs being Quadrature modulation/demodulation.

These schemes involve quadrature signals, known as IQ signals, and are carried out by IQ modulators and demodulators. IQ signals are a pair of signals that differ in phase by 90° (2π). In this state, they are said to be in quadrature. The reference signal is the "in-phase" signal referred to as "I" while the differing signal is the Q signal, i.e. the quadrature signal, as seen in ***Figure 1***.

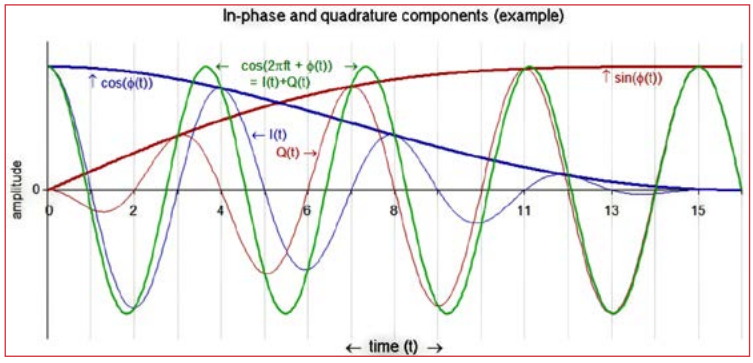


Figure 1: I and Q components of a signal are shown. cos(2πft + Φ(t)) = cos(2πft)cos (Φ(t)) + cos (2πft + π/2) sin (Φ(t)). The phase modulation (φ(t) is a non-linearly increasing function from 0 to π/2 over the interval 0 < t < 16. The two amplitude-modulated components are known as the in-phase component (I, thin blue, decreasing) and the quadrature component (Q, thin red, increasing)

(image source: https://commons.wikimedia.org/wiki/File:In-phase_and_quadrature_components_of_angle_modulation.gif)

In the receive chain, an IQ demodulator converts the received signal into its I and Q components while the reverse is carried out in the transmit chain by an IQ modulator. When the received signal has been demodulated, i.e. converted into its IQ pair, it is often referred to as raw RF data. Usually, this data is further processed in the FPGA + DSP to provide processed RF data. This processed data is then available as spectrograms, power vs. time plots, magnitude phase plots, FFTs, etc. However, in certain cases, raw RF IQ data that hasn't undergone any form of processing is required.

Raw data is often needed when the precise data of interest is not known, for example, when the modulated wave carrier is unknown. Another common example is when interfering signals are suspected within a band of interest but the signals' exact sources/frequencies and the actual source of the interference are unknown. In such cases, the raw RF data has to be preserved for further analysis.

SDRs make it possible to carry out data streaming operations seamlessly. High-performance SDRs can capture and preserve large amounts of data. This operation involves a series of procedures. The first step is capturing the RF signals. This step involves receiving, downconverting, and digitizing the signals by conversion to IQ data. IQ conversion, carried out with high fidelity, is followed by recording. In the recording stage, the raw IQ data is streamed to storage solutions where it is stored for playback and analysis. Playback and analysis are carried out on dedicated systems and involve upconversion, waveform regeneration, etc. for further analysis. In certain SDR platforms that require minimal storage, it's possible to have onboard storage capabilities. As well, in certain systems, the data is streamed for real-time analysis on a host system, eliminating the need for storage.

Whether for real-time analysis or storage for future analysis, SDRs stream data between RF systems and related equipment, often by using VITA 49 radio interface. Per Vices's highly advanced SDRs, Crimson TNG and Cyan, support standard signal data packets as stipulated by VITA 49, a packet-based protocol for conveying digitized signal data. Per Vices employs a data encapsulation format that implements stack layers — VITA 49 (application) within UDP (transport) within IP (internet) within Ethernet (link layer). Within the link layer, an Ethernet stack is available for transferring data between SDR and the host computer. Figure 2 shows the data stack.

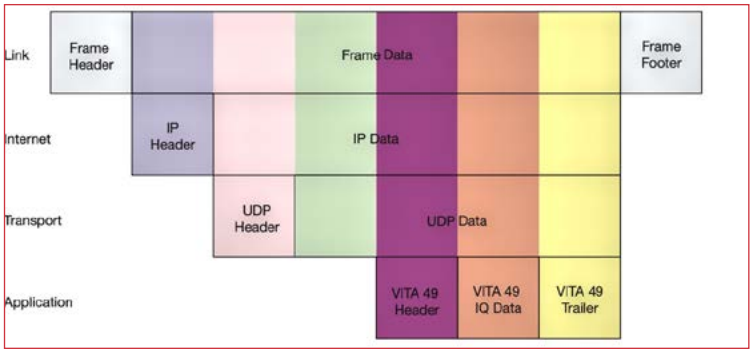


Figure 2: The stack for Per Vices's Crimson TNG and Cyan is shown. The data stream is divided into frames. All data and headers are within each Ethernet frame as shown. The internet layer features an IP packet that comprises a header and a data section. The data section bears the payload protocol lodged within the link layer. Located within the transport layer is the UDP while the application layer is where the VITA 49 layers are implemented.

There are various reasons why sometimes processed data and other times raw RF data are used. This can be due to the application itself, or limiting factors in terms of storage solution, and/or computational power. Both types of data offer unique advantages in different scenarios. One scenario requiring raw IQ data is environment simulation, in which everything within the spectrum is needed to ensure that algorithms or other processing developments are taking place as they should. On the other hand, processed data is utilized in numerous SDR applications to ensure data can be transferred correctly, including broadcast, GNSS, scientific data collection, and satellite communication. In these situations, the exact information-carrying signal is known and digital processing is required to uncover the signal and obtain the data through noise/interference, downconverting, demodulation, and processing.

Furthermore, processed data requires much less storage space than its raw data counterpart, as digital signal processing significantly reduces the amount of data that needs storing. In addition, processing data on an SDR's FPGA is much faster than sending it to a host system. Processing data also allows you to use IQ modulators to perform different forms of modulation, such as 16QAM.

IMPORTANT PARAMETERS FOR DATA STREAMING

There are certain requirements that the SDR, storage solution, and host system used for raw RF IQ data capturing and recording must meet in order to ensure an efficient and seamless process. These requirements are defined under parameters such as RF bandwidth, data throughput, storage space, and memory.

Data capturing for raw data applications involves monitoring various signals. It is therefore imperative for SDRs used in these applications to have substantial bandwidth. Regarding storage, the bandwidth being captured and the bit rate/ resolution of the ADC determine how much data will be streamed to and stored on the storage device.

For example, at 500MHz of IQ data being captured at 16 bits per sample, 500 MSPS*16 bits*2(IQ) = 16Gbps of data will need to be stored. This means that capturing only 5 minutes of data would result in 600GB of data needing to be stored per radio chain.

Considering the large amounts of data being transferred, high throughput is a crucial requirement for both the host system and SDR. Per Vices utilizes 10/40/100GBASE-R network interface cards capable of 10, 40, and 100 gigabits per second data transfer, ensuring that no packets are dropped or lost. An ultrafast host system with high-speed PCI express serial buses capable of up to 32 Gbps is also required.

As well, RAM is a vital consideration in the host system as it determines how much data can be written due to buffering. Moreover, we recommend using RAID (Redundant Array of Inexpensive Disks) configuration as, using this mass storage technique, data can be transferred from SDR to hard disk at rates beyond the rate of acquisition: thus making maximum waveform size independent of on-board memory and more dependent on hard disk size.

APPLICATIONS REQUIRING RAW RF DATA

There are a number of applications that require raw RF data before processing. One of these applications is spectrum monitoring and recording. In this application wideband spectra are monitored and the obtained RF data recorded for future analysis to identify unlicensed or illegal interference. This application allows raw RF data to be utilized and involves monitoring a particular part of the spectrum over a period and recording the data for further analysis.

In this application, the carrier wave signals are known (and likely able to be changed), and so all signals within the bandwidth of the spectrum which could pose a problem, have to be monitored. This is also the case in radar applications which involve continuous monitoring with the aim of detection of jamming signals, etc.

Raw RF data is also used in signal intelligence. Signal intelligence involves gathering intelligence from communication systems through the interception of signals. This application is now a vital aspect of public safety, security initiatives, and situational awareness. As wireless protocols become increasingly complex, there is a corresponding increase in spectrum congestion and ***electronic warfare*** (**EW**) sophistication.

Signal intelligence involves the collection of immense amounts of data for analysis and data extraction. Since the exact data-carrying signal is unknown, a lot of raw RF data has to be captured. The data gathered is usually bulky and complex, often requiring the application of AI and machine learning to extract the desired information.

Figure 3: Per Vices's Cyan is an SDR with a storage solution.

Another common application that requires raw RF data is radio frequency fingerprint search. Fingerprints can be a mix of modulation and spreading codes of the signals, the I/Q imbalances and phase noises due to the local oscillator, the power amplifier non-linearity of the transmitters, and the different transients as a result of front-end filtering. An example of fingerprint research is in GNSS fingerprinting.

If the fingerprint of an authentic transmitter is known, then machine learning algorithms for signal classification can be employed to differentiate between real signals from GNSS space segments and fake signals from GNSS simulators. Often this is important in defence applications, such as drones requiring GNSS/ GPS for navigation.

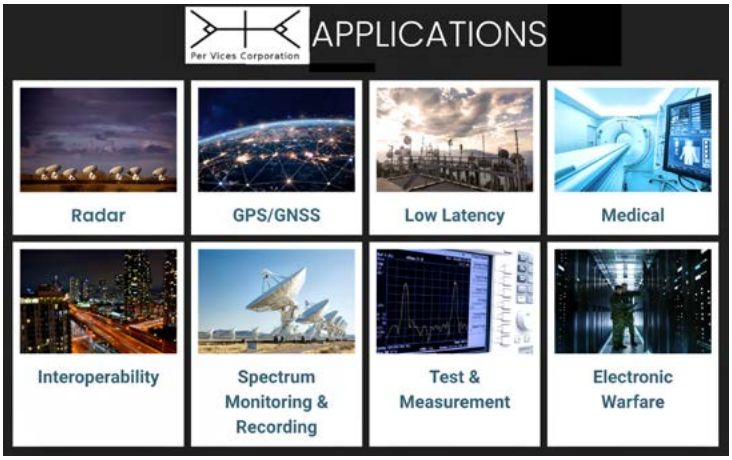
Per Vices offers two of the world's most advanced SDR platforms, ***Cyan***, seen in ***Figure 3***, and ***Crimson TNG***, shown in ***Figure 4***.

Figure 4. Crimson TNG offers a 4 receive and 4 transmit radio chain architecture that supports independent control on each of the radio chain or the ability to share a common LO for better phase coherency and stability performance. Each radio chain has an impressive 325 MHz of bandwidth with 16 bit converters and a tuning range from near DC to 6 GHz. The digital interface for controlling the system is a standard 1G Ethernet port and the data transfer is done over dual 10GBASE-R interfaces, providing users with up to 20 Gbps of data transfer.

With bandwidths of up to 3GHz per radio chain, transfer speeds of up to 400Gbps, and on-board data storage for our SDRs of up to 100TB, our SDRs are the most powerful for all raw RF IQ data applications.

www.pervices.com

Per Vices Corporation



DISPATCHES

DISA AWARDS LEIDOS $11.5 BILLION DEFENSE ENCLAVE SERVICES CONTRACT

Leidos (NYSE: LDOS) has been awarded the *Defense Enclave Services* (DES) contract by the Defense Information Systems Agency.

The single-award, indefinite delivery, indefinite quantity contract has a total estimated value of $11.5 billion and a four-year base period of performance followed by three two-year option periods.

"*We are honored that DISA has entrusted our team to establish the modern infrastructure foundation that will deliver critical combat support capabilities to our warfighters*," said ***Roger Krone***, Leidos Chairman and CEO. "*Leidos is committed to helping DISA and the Defense Agencies and Field Activities (DAFA) further their vision, leveraging our decades of technological expertise to bolster their critical mission*."

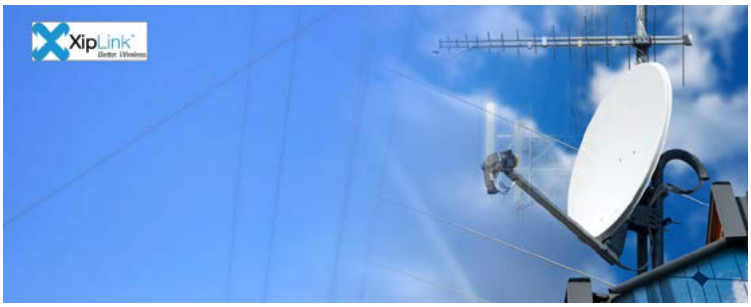
"*The Defense Enclave Services program demands unique expertise and advanced technology solutions*," said ***Gerry Fasano***, Leidos Defense Group President. "*Leidos brings both at unparalleled scale, with a focus on constant innovation. We look forward to delivering an improved user experience and enhanced mission capabilities*."

Through digital modernization and transformation, the Defense Enclave Service (DES) contract will unify the DAFAs on a common network architecture to provide mission services focused on enhanced user experience, improved security, and network reliability.

Headquartered in Fort Meade, Maryland, the Defense Information Systems Agency provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders and other mission and coalition partners across the full spectrum of military operations.

DISPATCHES

XIPLINK JOINS SDN/NFV ALLIANCE



XipLink has teamed with Lanner Electronics to make the company's disaggregated virtual network functions available to the Lanner ecosystem.

Lanner's white-box network appliances are specifically designed for VNF edge deployments in remote areas, such as military, maritime and critical infrastructure. They provide low latency, high availability, crypto acceleration, failover SFP+, Wi-Fi 6, and LTE/5G connectivity, as well as high core counts for network virtualization.

"*We are delighted to provide our service provider partners access to a much wider range of platforms, to address the ever-increasing demand for bandwidth at the furthest edges of the globe*," said ***Jaco Botha***, XipLink SVP of Product. "*The market for hybrid and wireless networking solutions is expanding with fiber, fixed wireless, LTE, 5G, LEO, MEO, and GEO satellite constellations all as viable connectivity options. XipLink Wireless Link Balancing and Bonding technology allows seamless traffic steering and highly scalable acceleration. The Lanner and XipLink collaboration promises to extract maximum value from the available network capacity, in challenging remote areas like maritime, defense and cellular backhaul.*"

"*We work closely with XipLink to advance hardware and software compatibility in solution development to escalate performance*," said ***Sven Freudenfeld***, CTO of Lanner Telecom Applications BU. "*Highly interoperable systems allow service providers to rapidly test combinations of latest components, resulting in reduced time needed for validation, and accelerated time-to-market.*"

Lanner Electronics Inc (TAIEX 6245) provides design, engineering and manufacturing services for advanced and customizable SDN and NFV network computing appliances for system integrators, service providers and application developers. Lanner possesses a wide range of network appliances including vCPE gateways designed for SD-WAN and SD-Security, as well as NEBS-compliant, NFVi-ready platforms with multiple processors, network I/O blades, and high availability features.

XipLink is a technology leader in wireless link optimization using industry-standard SCPS TCP acceleration, UDP enhancements, data/header compression, link and bandwidth bonding, and Internet optimizations to deliver a better wireless experience over-stressed communication links. The company's award-winning XipOS software dramatically improves web experience and optimizes other Internet traffic in markets such as maritime, cellular backhaul, ISP backhaul, military, and hybrid networks. The XipLink solution is packaged into appliances or virtual images and sold through OEM, Integration, and Service Provider partners around the world. XipLink is a private, employee-owned company with headquarters in Montreal, Quebec Canada, and field personnel worldwide.

GEOLOCATION PATENT FOR HORIZON TECHNOLOGIES

Horizon Technologies has been issued a patent by the United States Patent and Trademark Office (USPTO) titled "Techniques for Determining Geolocations."

The patent pertains to a system for using a single LEO cubesat to determine geolocations of Earth-based, Radio Frequency (RF) emitters. A corresponding patent was also recently issued by the ***European Patent Office*** (**EPO**).

The patented invention is part of Horizon Technologies' growing patent portfolio relating to its ***Amber***™ technology, which enables more accurate, and efficient, geolocation without necessitating clusters of cubesats.

Amber™ data will be used worldwide for protecting the world's oceans via "*dark target detection*." Amber™ data, when available later this year, will help companies and governments combat such problems as illegal fishing, pollution, transshipment, piracy, GNSS spoofing, and smuggling.

Horizon Technologies is developing a portfolio of patents and patent applications to protect our key product technologies and thus increase shareholder value.

"*We are pleased that the US Patent Office has yet again recognized Horizon Technologies' unique technology by granting this patent concerning the Amber™ system*," said ***John Beckner***, CEO of Horizon Technologies. "*Today's real-world events clearly show the need for innovation in space-based, multi-domain ISR (Intelligence, Surveillance, and Reconnaissance). This patented invention is especially important for our government and commercial customers addressing their maritime domain awareness requirements. Due to our unique technology, Horizon Technologies will not provide 'RF Mapping on command,' but rather a unique commercial RF intelligence data collected 24/7 and provided to our end-users.*"

Select this direct link to access the Amber™ information video…

Horizon Technologies offers innovative SIGINT and Space-Based, Maritime Domain Awareness (MDA) intelligence solutions. The company is a world leader in airborne Sat Phone monitoring systems for Intelligence, Surveillance, and Reconnaissance (ISR) applications, equipping governments worldwide by enhancing their SIGINT capabilities. Horizon Technologies is the Original Equipment Manufacturer (OEM) for the FlyingFish™ and BlackFish™ SIGINT systems which are in operation on numerous platforms worldwide and the firm participate daily in ISR and SAR missions via NATO and FRONTEX in Europe as well as being heavily involved in international operations around the globe. Horizon Space Technologies is the prime contractor for the UK Government's Amber™ program. The Amber™ Program will consist of Amber™ CubeSats in multiple orbital planes providing global Maritime Domain Awareness (MDA) data to the UK JMSC (led by Britain's Royal Navy).

DISPATCHES

GENERALS BROWN + RAYMOND HIGHLIGHT THE STRENGTHS + THE 'INTERTWINED' NATURE OF THEIR SEPARATE SERVICES

U.S. Air Force Chief of Staff Gen. CQ Brown, Jr., and Chief of Space Operations Gen. John W. "Jay" Raymond, often point out that while each service is independent, the U.S. Air and U.S. Space Forces are designed to work seamlessly and side-by-side to enhance the capabilities of each in protecting the nation's security and interests.

In a 45-minute session moderated by former Air Force Chief of Staff Gen. John Jumper, both Brown and Raymond offered frank assessments of their service's current status, the challenges each service faces, how each is building and changing for the future and, importantly, how the Air and Space Forces complement each other in those efforts.

Chief of Space Operations Gen. John W. "Jay" Raymond, left, and Chief of Staff of the Air Force Gen. CQ Brown, Jr., center, continue their discussion, 'Airmen and Guardians in the Fight,' which encompassed topics to include modernization, sustaining readiness, expeditionary abilities and more, with focus on placing the power in the hands of young Airmen and Guardians.

(U.S. Air Force photo by Staff Sgt. Elora J. McCutcheon)

"The transition has gone very, very well," Brown said about how separating space two years ago into a new and independent service has progressed. "It's about mutual support and having each other's back. The thing Jay and I spoke about a lot in terms of development was the balance of how much do we hug each other close and how much do we spread out and grow? We are so intertwined; we are dependent on each other not just from a base operating support construct, but also operationally. We could not do what we do as joint force without the Air Force and the Space Force."

Raymond agreed. "We're one team as the Secretary [Frank Kendall] has said from day one. And we are one team, but I think we're a better team with two, independent services. I think the strength we all bring now, where Gen. Brown can focus on the air domain and my team can focus on the space domain, make us an even stronger Department," Raymond said.

While the Air and Space Forces are technically separate, with different and distinct missions and responsibilities, Brown and Raymond noted they also have similar and, in some ways, parallel objectives. Both the Air Force and Space Force are foundational to America's national security, they said, and as the highest ranking military officers of each, they said it was their obligation to provide Airmen and Guardians the tools they need to succeed.

While there was debate about the need for a separate service devoted to space before Space Force was born in December 2019, that debate has been settled. In the past three years alone, Raymond said the number of items the U.S. must track in space has spiked from 22,000 to more than 40,000. Likewise, the number of satellites that must be tightly monitored has risen from 1,500 to 5,000.

Even more important, according to Raymond, space has moved from a benign environment to a recognized warfighting domain. That change has occurred at the same time that space's importance to military operations with global positioning, communications and virtually every other aspect of joint operations has emerged as well.

"*Our adversaries now have the advantages [in space] we've always enjoyed. It's a different domain that required a different approach,*" Raymond said. That explains why the Space Force was created, and since its birth, he said, the service has been "*purpose built from the ground up. We couldn't have done that without support from the Air Force. It's been a very powerful partnership*," Raymond said.

Both Brown and Raymond emphasized the need for each service to move fast, to innovate and modernize.

Brown said meeting those goals was the catalyst for authoring "*Accelerate Change or Lose*," the philosophy driving his thinking and decision-making. That document is accompanied by a series of "action orders" that detail how those concepts are to be made real.

Chief of Space Operations Gen. John W. "Jay" Raymond, left, and Chief of Staff of the Air Force Gen. CQ Brown, Jr., center, continue their discussion, 'Airmen and Guardians in the Fight,' which encompassed topics to include modernization, sustaining readiness, expeditionary abilities and more, with focus on placing the power in the hands of young Airmen and Guardians. U.S. Air Force photo by Staff Sgt. Elora J. McCutcheon.

While both Brown and Raymond have taken steps internally to remove barriers, reduce bureaucracy and increase efficiencies, they pointed out external factors that affect how they succeed or fail. Foremost is the federal budget process that in recent years has failed to produce a new budget tailored to meet specific, real-time needs.

Instead of a new budget, the federal government has operated under a series of continuing resolutions, or CRs, which recycle the previous year's spending plan to provide additional time to complete work on a new budget. Operating under long-term CRs "*is absolutely devastating to us*," Raymond said, because it hampers new programs, modernization and the ability to target money to programs and policies where it's most needed. The current CR expired on March 11, more than halfway through the fiscal year, which began October 1, 2021.

Budgets are important, both leaders said, because the nature of conflict and the capabilities of adversaries such as China and Russia are changing. Brown said the Air Force needs to adapt by using such tactics as agile basing, known in the Air Force as Agile Combat Employment, or ACE. The idea is augmenting large, fixed bases with smaller, more mobile and nimble bases that make it more difficult for adversaries to find and target them.

"*We've gotten used to going someplace where everything is all set up and already there. In the future, we're going to go places where we haven't gone to before*," Brown said. He added "*[ACE] is a capability, but it's also a mindset of our multi-capable Airmen; the ability to go into a base you haven't gone to before, set it up and tear it down, but also the ability to stretch our Airmen and allow them to use all their skills and talent*."

Brown and Raymond also emphasized the importance and value of allies and partners in much the same way Kendall did in his remarks to the Symposium an hour before the fireside chat. Despite the challenges and threats, Brown and Raymond said they remain optimistic because of one overriding factor — the quality of Airmen and Guardians.

"*They are incredible*," Raymond said about the Space Force's Guardians. "*They are collaborative, they're connected, they want to serve. They are bold, they've got ideas and it requires a different kind of leadership style*."

Brown sees the same attributes in Airmen.

"*I really do think about this generation and the aspect of how connected they are, how much they want their leadership to know them and care, and they really want to contribute. We have to make sure we get out of the way and let them contribute. That, to me, is the exciting part. And if we, as leaders, don't get it right, they aren't going to stick with us. We need to really think about that*," he said.

Article authored by Charles Pope, Secretary of the Air Force Public Affairs

DISPATCHES

PROMIN AEROSPACE: UKRAINIAN SPACE COMPANIES ARE UNITED IN DEFENDING THE COUNTRY

The full-scale Russian invasion of Ukraine has united the space community in the Ukraine and across the globe. International space companies are supporting their Ukrainian colleagues and Ukrainian companies are deploying volunteers who are directing their work to ensure the companies are securing their employees and assisting the nation's army.

From the first days of the war, world space organizations have rallied to our side. To support the Ukrainian Army, captain of the ***SpaceX Inspiration 4*** crew ***Jared Isaacman*** personally brought aid to the Ukrainian military. Satellite images of the movement of Russian troops were provided by the company ***Capella***, and Ukrainians received Starlink satellite internet reception stations as a gift from Elon Musk at the request of Ukrainian Minister of Digital Transformation, ***Mykhailo Fedorov***.

Elon Musk said that SpaceX had reprioritized its work to ensure the cybersecurity of their Starlink stations. Because of this, the company even postponed planned releases of new versions.

As the world watches the Ukraine fighting against Russian aggression, Ukrainian companies must ensure the safety of their employees. To do this, most companies have switched to remote work formats and flexible schedules.

Several Ukrainian space companies, including startups and large companies, have managed to continue operations, combining work responsibilities with volunteer work. Some high-tech companies are opening up new fields of operations to support the military and the Ukranian population. For example, the mobile application, ***Reface***, has launched a logistics project called ***KOLO*** to supply ammunition to the Ukrainian army. Their engineering team is now working on new software to analyze enemy movements via satellite images.

Space Companies During The War

Many private and state aerospace companies in Ukraine develop spacecraft, aircraft, and parts. They include SETS (***Space Electric Thruster Systems***), ***Kurs Orbital***, ***Flight Control Propulsion***, startups ***Orbit Boy***, ***Promin Aerospace***, and ***Elliscope***. The state-owned ***Pivdenne*** and ***Pivdenmash*** enterprises are developing rocket engines and rockets in collaboration with ***Orbital Sciences Corporation*** and the ***European Space Agency***.

All of these companies have continued their normal work. At the start of the war, some of them adopted remote working schedules, but they already had experience with such plans from the pandemic. Most companies have also created volunteer programs.

The former head of Ukraine's State Space Agency and founder of Kurs Orbital stressed that Ukrainian space companies have great potential that will be fully shown after victory over the invaders. "*No one believed that Ukraine could resist the Russian army crossing our borders, but we are doing it. New space startups have appeared almost every month, and there will be more,*" he said.

The engineering team at Promin Aerospace remains in Ukraine and is continuing its work on developing the company's rocket. Our other team members are working remotely. They have also added responsibilities for territorial defense and volunteering to their daily routine.

"Each of us has had to be flexible for the needs of wartime and to perform new duties to protect our country. Some are strengthening the defense of their cities, some are helping refugees and the armed forces, while others are arranging supplies of medicines, ammunition, and food," wrote ***Misha Rudominsky***, CEO and co-founder of Promin Aerospace.

Sanctions Against Russia

The Russian invasion has sparked serious responses by the international community in the field of space. Several countries have imposed sanctions against the aggressor, making previously planned international projects impossible.

This resulted in the withdrawal of OneWeb satellites from the Russian cosmodrome at Baikonur, the Russian-European Mars mission was suspended, and more than half of high-tech imports were frozen, all of which will do considerable damage to Russia's state space program.

Moreover, Russia has also cut itself off from activities that did not fall under sanctions. Roscosmos has refused to export RD-181 rocket engines and cooperation on the ISS.

The aggressor's withdrawal from international projects definitely opens up more opportunities for other space companies.

COMMAND CENTER: TOM EATON

President, Telesat Government Solutions

Tom Eaton is the President of Telesat Government Solutions, a U.S.-incorporated, wholly-owned subsidiary of Telesat. Mr. Eaton is responsible for defining the government division's commercial, operational and strategic activities. Mr. Eaton has more than 30 years of experience in the telecommunications industry, holding a range of executive leadership positions across the global satellite operator and network services markets, including providing secure communications services to the armed forces and national security community. Most recently, Mr. Eaton served as Vice President of International Sales at Telesat, where he successfully increased the use and revenue on the company's international satellite fleet.

Before joining Telesat in 2014, Mr. Eaton was President of Harris CapRock Communications, where he played an instrumental role in the formation of a global provider of end-to-end, mission-critical communications networks for government, energy and maritime customers. Mr. Eaton holds a Master of Business Administration from Mercer University and a Bachelor of Business Administration from the University of Georgia.

What are the biggest challenges surrounding connectivity for defense and government personnel today?

TOM EATON

From Telesat's experience, the defense and government sectors' biggest concerns for connectivity are reliability, resiliency, security, and ease of access.

In terms of reliability, the expectation is that mission critical data can be transmitted from a terminal in-theater back to the command center — and vice versa — in real-time without any outages. This means the networks government customers leverage must be resilient, with no single points of failure. Resilient network architectures must be self-healing with the ability to mitigate interference, data detection, data interception and to bypass third-party terrestrial infrastructures to deliver the assured connectivity required for this

Security is paramount. Forward terminals can expose government operators' location and activity, so the need to ensure terminal location confidentiality is imperative. Additionally, the need to ensure the defense-grade encryption of the data being transmitted is intact and cybersecurity measures are maintained as it transports through the network.

The ability to access commercial satcom networks in a seamless way is critical. ***Commercial-Off-The-Shelf*** (**COTS**) equipment and standards-based systems allow government customers to access and operate services, just as they would access terrestrial infrastructure.

Equally critical, the government's administrative contracting process must evolve to increase flexibility in the acquisition of commercial communication services over Low Earth Orbit (LEO) networks such as Telesat Lightspeed.

How is Telesat working with the industry to address these challenges today?

TOM EATON

Telesat is developing the first enterprise-grade Low Earth Orbit (LEO) network, ***Telesat Lightspeed.*** Telesat's commercial customers, which include leading telecom operators, enterprises, and aviation and maritime connectivity providers, require carrier-grade services with committed service level agreements, resiliency, and high security.

As Telesat looks at the needs of government and defense customers, we believe our system architecture and cybersecurity measures established for Telesat Lightspeed will be compelling for MILSATCOM requirements.

Telesat has adopted the ***National Institute of Standards and Technology*** (**NIST**) ***Cybersecurity Framework*** and expects to meet the government standards for ***Transmission security*** (**TRANSEC**) and the ***Infrastructure Asset Pre-Assessment Program*** (**IA-PRE**). In addition, the Telesat Lightspeed network will be a **MEF 3.0** certified, layer 2 interface with validated communications security compatibility.

Telesat is working closely with industry partners to develop a wide range of user terminals (antennas and modems) to access the Telesat Lightspeed network. Ecosystem vendors can incorporate the Telesat Lightspeed waveform and system specs into their terminal offerings.

Some terminal providers already have an ability to upgrade, plug-and-play, and support multi-orbit, multi-frequency, multi-waveform services and we are working with those vendors. In addition, we are developing commercially-based contracting models for the government's consideration in simplifying access to LEO networks, such as Telesat Lightspeed.

Defense organizations are aggressively seeking to invest in low earth broadband constellations to advance connectivity forward. What capabilities of LEO technology are so advantageous?

TOM EATON

Defense organizations need high data rate, low latency, persistent communications at any point on Earth, including Polar regions. At Low-Earth Orbit (LEO), Telesat is able to provide a service that has very low latency. Government and military applications are becoming increasingly sensitive to latency and LEO networks can provide a faster, ***observe-orient-decide-act*** (**OODA**) ***loop decision cycle.***

Telesat Lightspeed satellites each have four optical inter-satellite links (**OISLs**), creating a mesh network in space. This results in multiple transport routes of user traffic across the space network. A government user can communicate directly from anywhere with the Telesat Lightspeed network constellation satellites and its optical satellite-to-satellite communications path before using a downlink — even on the other side of the Earth. This eliminates the need to transit a gateway anywhere near a contested or degraded operational environment or to ever use a "*non-trusted*" terrestrial network. This is particularly valuable for embassies, key government facilities, bases, sensors and defense platforms, wherever they are located.

Adversaries seeking to determine the location of user terminals on Telesat Lightspeed will face significant challenges vs. legacy, wide-beam communications satellites used today. Using small Ka-band beams, LEO satellite motion relative to a fixed Earth location, OISLs and variable carrier frequency assignments defeats traditional remote interferometric geolocation attempts that quickly reveal highly precise user terminal locations on legacy geostationary communications satellites. The Telesat Lightspeed LEO architecture is designed so information about customer terminal location remains protected from unauthorized persons.

What are your plans surrounding Telesat Lightspeed today?

TOM EATON

Telesat Lightspeed is designed to be a multi-purpose, standards-based system serving clients across the globe. When you add in our 52-year heritage of engineering excellence as a satellite operator, we're building a system that can meet the needs of today's government and defense applications. We're deliberate in building a superior network with reliability, resiliency, security and ease of access built in from the very beginning.

During the Fall of 2020, the Defense Advanced Research Projects Agency (DARPA) awarded Telesat a contract to aid the Blackjack constellation. Can you provide an update on this?

TOM EATON

While we can't share much detail, we are continuing to fulfill work as contracted by DARPA. Telesat is on-target to deliver two LEO ***Croupier*** spacecraft buses to DARPA. The Telesat Lightspeed constellation includes several distinctive features that align with the Blackjack program vision, including spacecraft buses with native OISL capability, self-healing mesh networking, onboard processing and a full global network architecture backed by global priority spectrum allocations.

Are there any other opportunities that Telesat is looking to pursue to help aid the military industry in the U.S. and across the world?

TOM EATON

Allied Nations are keenly interested in Telesat Lightspeed due to its high capacity, security and resiliency. The truly global footprint of the network with over 15 Tbps of capacity provides a compelling value proposition across the globe.

There is an interest in "hosted satellites" — government-developed and designed satellites that are focused on scientific, humanitarian and defense related initiatives. Hosted satellites can connect to the Telesat Lightspeed constellation, performing their missions while using satellite-to-satellite linking over OISLs or Ka-band user beams to move the hosted-satellite's data securely to any location in the world via the Telesat Lightspeed network.

As an example: A hosted LEO weather satellite with sensors can detect weather patterns in real-time and quickly transmits the data via OISL or Ka-band links to the Telesat Lightspeed space relay network to deliver data to a command center.

What is Telesat's vision for military connectivity and communications a decade from now?

TOM EATON

Ten years from now we want to continue being a trusted and reliable provider to the government and military — even more so than we are today. Telesat's 52-year heritage in the satellite communications space is seen as a benchmark and we've developed the reputation of having some of the best developed and engineered products on the market serving a global customer base. If I can say anything with certainty about Telesat's future it is that we will continue to provide innovative, reliable, resilient and secure products well beyond today.

www.telesat.com

SILICON VALLEY

SPACE WEEK

SATELLITE INNOVATION & MILSAT SYMPOSIUM JOIN FORCES

SATELLITE INNOVATION

October 11 - 12, 2022
SATELLITEINNOVATION.COM

2022 MILSAT SYMPOSIUM

October 13 - 14, 2022
MILSATSHOW.COM

SAVE THE DATE!

OCTOBER 11-14, 2022


Information & Communication Technology (ICT) Solutions
Daily Host Alerts Trend (Last 5 Days)
Reliable.
Resilient.
Secure.
Own the edge.
For over 20 years, Leonardo DRS has supported custom end-to-end satellite-based ICT solutions for maritime, airborne, and ground-mobile operations. As the top SATCOM integrator for the U.S. Federal Government,* we consistently deliver optimal levels of availability, integrity, and confidentiality. This unwavering security makes Leonardo DRS the only choice when success is critical – so you can own the edge.
*Source: GovWin IQ Total Federal Market Overview – Top Contractors 2016-2020 – NAICS 517410 Satellite Telecommunications
Learn about best-value ICT Solutions at LeonardoDRS.com/ICT
LeonardoDRS.com/ICT
LEONARDO DRS