Next Generation Space Defense

MILSATMAGAZINE

December 2022 — Year in Review

Publishing Operations

Silvano Payne, Publisher + Executive Writer

Simon Payne, Chief Technical Officer

Hartley G. Lesser, Editorial Director

Pattie Lesser, Executive Editor

Donald McGee, Production Manager

Teresa Sanderson, Operations Director

Sean Payne, Business Development Manager

Dan Makinster, Technical Advisor

Chris Forrester, Senior Columnist

This issue's authors...

Brian Billman

Daniel Gizinski

Dave Micha

David Pesgraves

Rob Spalding

SSC Public Affairs

David Todd

Features

Dispatches

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

SES SPACE & DEFENSE LAUNCHES A NEW SINGLE-PANE-OF-GLASS ICT PORTAL CAPABILITY

The Information & Communications Technology (ICT) Portal provides transparent and consolidated network visibility improving performance and operational decision-making

SES Space & Defense, a wholly-owned subsidiary of SES, announced their new Common Operational Picture (COP) capability, the Information & Communications Technology (ICT) Portal.

The ICT Portal is a modular, web-based, NetOps capability that provides end-to-end situational awareness in a consumable, single-pane-of-glass, user interface.

The ICT Portal uses the same holistic and vendor agnostic approach as the **SES Space & Defense ICT Ecosystem** — providing customers with a comprehensive and flexible monitoring and reporting solution.

Accessible anywhere in the world, the technology agnostic capability is customizable, based on mission and customer operational requirements.

The consolidated network visibility provides the transparency necessary to rapidly identify and diagnose issues across complex networks, including terrestrial and space assets, so networks and applications can be fully optimized to increase performance.

In addition, the ICT Portal allows all SATCOM assets to be viewed as one comprehensive satellite and network architecture, providing customers with access to innovative solutions and making a more resilient satellite architecture a reality.

The ICT Portal is secure by design and incorporates the latest security and data processing technologies, ensuring mission assurance for government and military users.

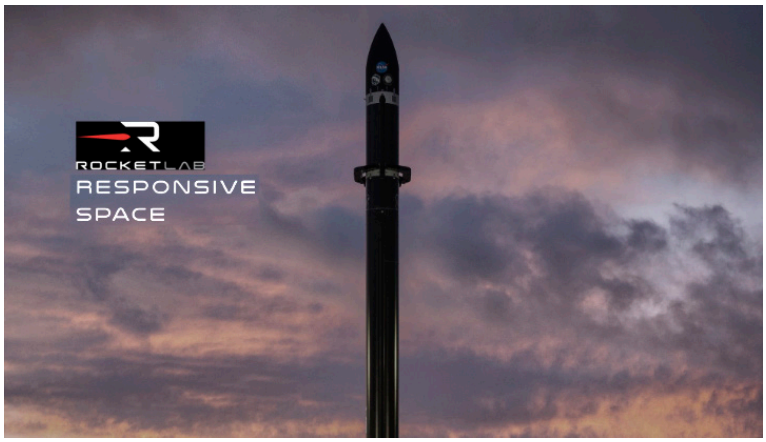
"Today's military and government users are more network-enabled than ever before, and our ICT Portal supports this through increased visibility and control over their network," said SES Space & Defense President and CEO, ***David Fields***. *"The ICT Portal will be showcased at the SIA DoD COMSATCOM Workshop, enabling our most tactical customers to see how performance, network transparency and assurance, makes it a critical capability for successful missions."*

The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

DISPATCHES

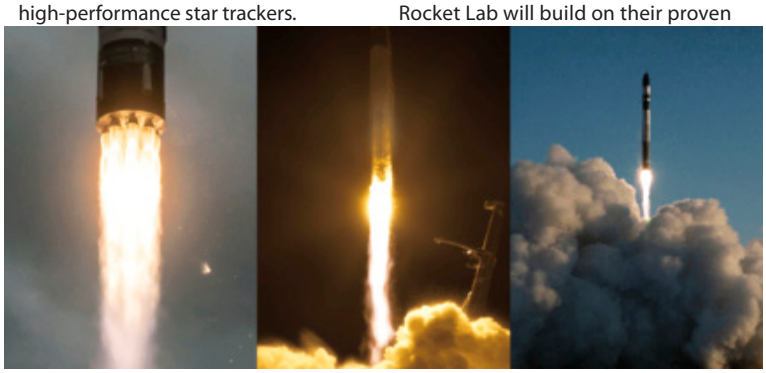
ROCKET LAB INITIATES THE ROCKET LAB NATIONAL SECURITY SUBSIDIARY

***Rocket Lab USA, Inc.** has created a U.S.-based, wholly owned subsidiary to serve the defense and intelligence community — Rocket Lab National Security LLC (RLNS) — this subsidiary will deliver launch services and space systems capabilities to the U.S. government and allies.*



Since the Company's first launch of the Electron rocket in 2017, Rocket Lab has conducted multiple successful launches for national security customers, including missions for the ***National Reconnaissance Office (NRO)***, ***U.S. Space Force*** and ***Defense Advanced Research Projects Agency (DARPA)***.

Rocket Lab Space Systems technology has also been featured in hundreds of commercial and government satellites serving the national security market, from separation systems and flight software to space solar power and high-performance star trackers.



Under the new RLNS subsidiary, Rocket Lab will build on their proven track record to deliver new and existing space capabilities for national security applications.

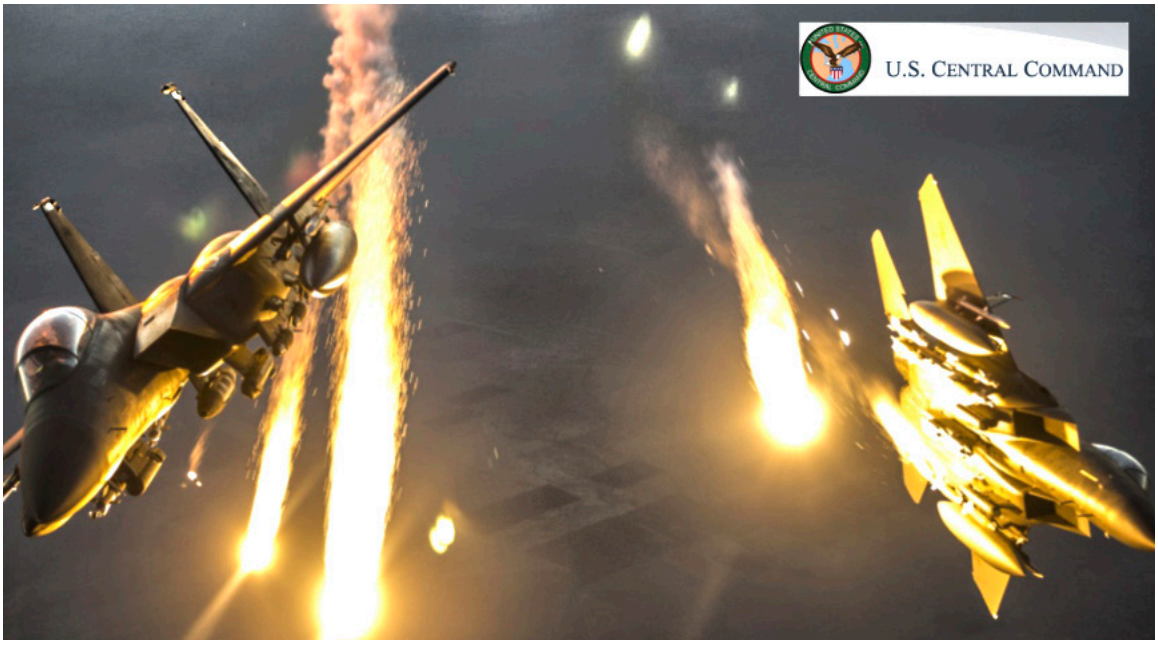
"Across our launch and space systems offerings, we have the privilege of working with the full spectrum of space users from primes, commercial constellation operators and small start-ups, to US and Allied government customers," said ***Brian Rogers,*** Senior Director – Global Government Launch Services. *"Through Electron, Neutron and Space Systems, we've got first-hand experience of each market's unique needs. Top of the list for national security is reliability and responsiveness, something we've delivered on across multiple missions already. With Rocket Lab National Security we're building on this strong heritage to deliver tailored capabilities that evolve as the nation's needs do."*

www.rocketlabusa.com

U.S. CENTCOM ACTIVATES U.S. SPACE FORCES-CENTRAL

***U.S. Central Command** has activated U.S. Space Forces-Central at the component's permanent headquarters located at **MacDill Air Force Base**, Florida.*

The activation of USSPACEFORCENT is another step for the ***U.S. Space Force*** to provide forces to combatant commands, providing combatant commanders with organic space planning and employment expertise. USSPACEFORCENT is responsible for space operations within the CENTCOM area of responsibility including capabilities such as positioning, navigation and timing, satellite communication, missile warnings, and other missions as required.



Activating this component under CENTCOM provides expert Guardians to work with coalition and regional partners to integrate space activities into shared operations and adds another level of commitment to partners by further strengthening regional stability and security within the CENTCOM area of responsibility.

"Just as the evolution of space as a warfighting domain necessitated the establishment of a separate service, USSPACEFORCENT provides CENTCOM a subordinate command focused solely and continuously on space integration across the command, within all domains and all components," said U.S. Space Force Col. ***Christopher Putman***, USSPACEFORCENT commander.

"Space underpins every element of warfighting in the CENTCOM region," said CENTCOM commander, Gen. Michael "Erik" Kurilla. *"…Since the Cold War, space has ceased to be a sanctuary. It is no longer solely the realm of progress and peace. Space is now a domain of conquest, conflict, and – for us – cooperation."*

www.centcom.mil

AvL
TECHNOLOGIES
avltech.com

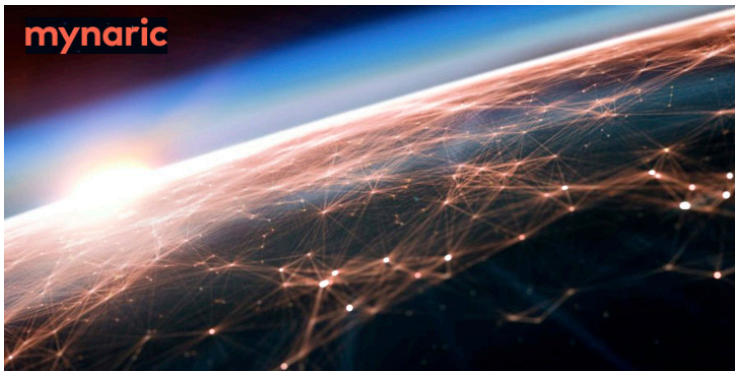
HARSH WEATHER?

Communicate through extremes

1.6m Manual Point Tri-Band Terminal
Operational winds to 60 mph
MIL-STD-810G tested
MIL-STD-188-164C & Skynet compliant

REDWIRE'S CYBERSECURITY TECH TO SUPPORT DARPA MISSION

Redwire Corporation's suite of space cybersecurity tools, developed with BigBear.ai, will be used by Mynaric (in the development of an advanced satellite communication (SATCOM) program that is sponsored by the Defense Advanced Research Projects Agency (DARPA).



Mynaric will use Redwire and BigBear.ai's ***Space Cyber Resiliency through Evaluation and Security Testing*** (**SpaceCREST**) platform to support the cybersecurity evaluation of their optical communications terminal.

The SpaceCREST platform ensures the security of its optical communications terminal design for Phase 1 of ***DARPA's Space Based Adaptive Communications Node*** (**Space-BACN**) program.

The program seeks to develop reconfigurable, multi-protocol communications terminals that are small, lightweight, low-power, inexpensive, and able to connect many different satellite constellations in LEO.

SpaceCREST will be used to identify vulnerabilities that could affect the terminal or disrupt its operation and then find ways to protect against those vulnerabilities.

SpaceCREST will also use Redwire's digital engineering capabilities to make cybersecurity analysis of space assets more streamlined and reliable.

With Redwire's ***Advanced Configurable Open-system Research Network*** (**ACORN**) tools and technologies, SpaceCREST enables users to simulate and emulate various hardware and software systems as they are being designed and built.

Advanced Configurable Open-system Research Network (ACORN)

Using SpaceCREST, Mynaric will be able to ensure that its communications terminals are both secure and resilient.

"*Redwire is proud to support Mynaric in identifying and mitigating potential vulnerabilities within crucial national security programs*," said ***Dean Bellamy***, Redwire's Executive Vice President of National Security Space. "*This application of SpaceCREST demonstrates the value that Redwire and BigBear.ai's collaboration holds for the growing space economy. SpaceCREST will be a critical tool for proactive maintenance and protection of government and commercial customers building the next generation of resilient space architectures.*"

"*As the world has increased its reliance on space assets in both government and commercial operations – ranging from mission-critical national security operations to GPS navigation – the ability to accurately detect and address system vulnerabilities is essential to the everyday lives of billions of people*," said ***Eric Conway***, BigBear.ai's Senior Vice President of Technology, Federal Solutions. "*BigBear.ai is excited to partner with Redwire to deliver SpaceCREST to Mynaric in support of DARPA's efforts to ensure the next generation of satellite communications are resilient to cyberattacks.*"

Redwire Corporation (NYSE: RDW) is a leader in space infrastructure for the next generation space economy, with valuable IP for solar power generation and in-space 3D printing and manufacturing.

BigBear.ai delivers AI-powered analytics and cyber engineering solutions to support mission-critical operations and decision-making in complex, real-world environments. BigBear.ai's customers, which include the U.S. Intelligence Community, Department of Defense, the U.S. Federal Government, as well as customers in manufacturing, healthcare, commercial space, and other sectors, rely on BigBear.ai's solutions to see and shape their world through reliable, predictive insights and goal-oriented advice.

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

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

SES SPACE & DEFENSE

www.sessd.com

TRISEPT + SPIDEROAK JOIN FORCES TO TACKLE GROWING CYBER THREATS IN LEO

***TriSept** and **SpiderOak** are now engaged in a strategic partnership that is aimed at providing a comprehensive, end-to-end, security system capable of ensuring critical commercial and government, space and ground operations are protected from intentional interference and/or attacks.*

Space-based services are critical to everyday life, for the military and civilians, supporting critical services and infrastructure including utilities, aviation, emergency communications, and military operations.

The most significant threat to these space-based assets is a cyber-attack — with the exponential growth of government and commercial satellites in LEO, the vulnerability grows in lockstep.

To address this growing threat, the Linux-™based, ***TriSept Secure Enhanced Layer*** (TSEL) operating system together with ***SpiderOak's OrbitSecure***, zero-trust protocol offers one of the first complete commercially available satellite security solutions capable of protecting both new space and legacy satellites operating on-orbit.

TSEL locks down the spacecraft hardware and OrbitSecure locks down the data exchanged between the spacecraft and ground segment. This complete end-to-end solution for secure data processing, storage, and transmission is the first of its kind.

TSEL was developed to meet rising demand across the satellite industry for a managed, cybersecurity solution. TSEL implements security best practices from 14 security industry standards and has more than 1,000 security controls applied.

By offering a series of automated mechanisms and updates delivering far more detailed audit data, near-real-time security analysis and patch updates along with "***Trust No One***" (TNO) verification layers, TSEL protects against hackers and provides an accurate account of what's happening aboard conventional and smallsats at all times.

TSEL provides protection for satellite embedded controllers of onboard systems and subsystems by detecting, tracking and eliminating known and emerging vulnerabilities. SpiderOaks' OrbitSecure provides equally robust and reliable protections across both the ground and space infrastructure supporting satellite and mission data communications between Earth and entire constellations across LEO, MEO, GEO, and cislunar.

A pure software offering, OrbitSecure leverages a unique combination of no-knowledge encryption and distributed-ledger technology to bring zero-trust security to zero-gravity environments with high assurance and pure peer-to-peer coordination and communication.

"As the new space economy leads to increasing dependence on spacecraft operations, commercial and government operators need a reliable and robust security solution that effectively protects against growing threats across the ground and space infrastructure supporting a broad range of missions," said ***Rob Spicer***, TriSept CEO. *"The partnership between TriSept and SpiderOak leverages our complementary TSEL and OrbitSecure technologies and a shared commitment to safe space operations to deliver a breakthrough in cybersecurity for virtually every mission."*

trisept.com
spideroak.com

THALES AWARDED FRENCH MOD CONTRACT TO BUILD DEPLOYABLE COMMS NETWORKS FOR THEATERS OF OPERATIONS

The French defence procurement agency (DGA) has contracted to Thales the design of deployable and high-speed communications networks for theaters of operations, a major asset for collaborative combat.

Thales will deliver more than 200 modular, mobile stations in the phase 3 of the ASTRIDE 3 contract., thereby enabling France to command coalition forces as a framework nation, as well as provide the French armed forces with an autonomous multi-brigade force projection capability. Thales will work with several partners to deliver a high-speed, mobile and secure command infrastructure for deployment in an extremely wide range of tactical situations.

ASTRIDE 3 integrates new connectivity systems, such as latest-generation satellite terminals (SYRACUSE IV), HCLOS (high-capacity line-of-sight) communications, tactical software-defined radios (CONTACT) and digital wireless services (LTE technology). These assets will interconnect the battlespace and provide a resilient network of connected command posts from theatre level down to tactical units. ASTRIDE 3 could also offer defence cloud hosting capabilities to meet the needs of collaborative command structures and support a broader computer network defence (CND) initiative to deal with cyber threats. ASTRIDE 3 stations will meet the latest FMN (Federated Mission Network) interoperability standards and enable France to act as a framework nation for forces command at Land Component Command (LCC) or Division level.

The integrated, automated ASTRIDE 3 stations will accelerate and simplify maneuvers in the theatre of operations, enabling forces to deploy different versions of the station — hardened container, shelter (transport cases) or pre-integrated in armored vehicles in the SCORPION ecosystem —– to adapt to an extremely wide range of tactical situations. Wireless connections will shorten command post deployment times by significantly reducing the number of manual operations required. In addition, the network planning, command and supervision tools MOSART, will give land forces unprecedented agility in adapting to the tempo of their mission.

Thales' sites in Cholet (Pays de la Loire) and Gennevilliers (Ile-De-France), as well as those of numerous French technology partners and SMEs, contribute to both the development and production of the physical and software components of the ASTRIDE 3 system.

www.thalesgroup.com

USSF' S SPACE DELTA 2 LEVERAGES SDA IN SUPPORT OF ARTEMIS I MISSION

On November 16, 2022, NASA's Artemis I successfully launched from Space Launch Complex 39B. This landmark event marked the first successful launch of the Orion spacecraft and Space Launch System (SLS) rocket. Artemis I reentered Earth's atmosphere on December 11, 2022.

Over the course of Artemis I's flight, ***Space Delta 2*** and its components, the ***15th Space Surveillance Squadron***, ***18th Space Defense Squadron***, ***19th Space Defense Squadron*** and ***20th Space Surveillance Squadron***, collaborated to test capabilities to maintain custody of cislunar objects.

Additionally, they defined ***xGEO*** tracking, which refers to any area beyond the geosynchronous orbit where the standard laws of orbital dynamics no longer apply.

Space Delta 2 also functioned as a liaison by sharing information, data points, and lessons learned among the **Department of Defense**, commercial, academic and other government partners.

Space Delta 2's mission is to prepare and present assigned and attached forces enabled to execute combat-ready, SDA operations.

In other words, they aim to maintain and ensure freedom of action for the United States, its allies and commercial partners in the space domain.

XGEO tracking and the cislunar regime are rapidly receiving more focus from all space-faring nations and must be included in the totality of Space Delta 2's mission.

Space Delta 2's ability to support missions such as Artemis through their operational skillset and integrate with national and global partners help secure our place as a leader for the peaceful use of the global commons.

"*Providing support to the Artemis I mission allows Delta 2 sensors to test cislunar tracking tactics, techniques, and procedures for future crewed missions*," said Colonel ***Marc A. Brock***, Space Delta 2 commander. "*SDA requires Space Delta 2 operators to obtain and maintain a continuous, comprehensive, and combat-relevant understanding of the space situation. This data is critical to satellite operators all over the world in achieving mission success as the space domain becomes more contested and congested.*"

Brock continued, "*SDA is the foundation for all operations occurring in, from and to space. It serves as the cornerstone for Joint Force success. Timely and accurate xGEO space object detection and tracking in conjunction with our traditional SDA operations closer to Earth will be essential to our support for human space flight safety from launch to lunar landing and return, to facilitate human exploration and to promote the peaceful and responsible use of space.*"

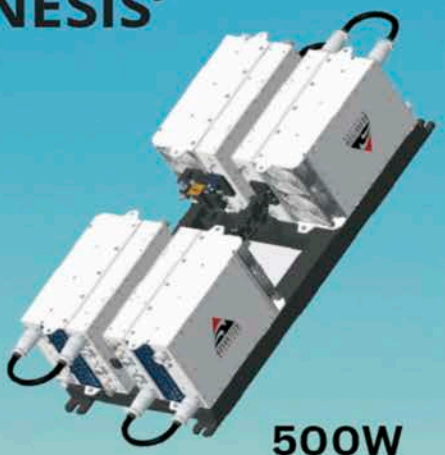
Article is courtesy of 1st Lieutenant Hillary Gibson, United States Space Force

ADVANTECH WIRELESS
A Rajant Technologies Company

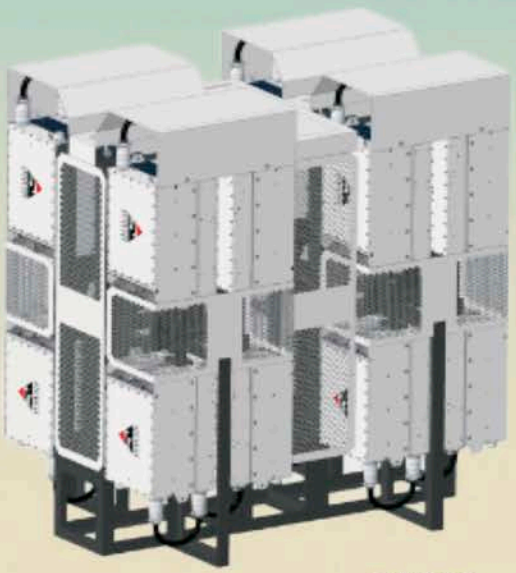
Introducing SUMMIT III

'Powered by GENESIS'

- *Soft-Fail Redundant SSPA System*
- *Delivers 500W to 2kW of linear, Ku-band power*
- *Ethernet SNMPv3 & Embedded Web server*
- *Removable Power Supplies*
- *Compact package, factory assembled and tested*
- *No waveguide switching or external logic controller*
- *High availability and low MTTR*

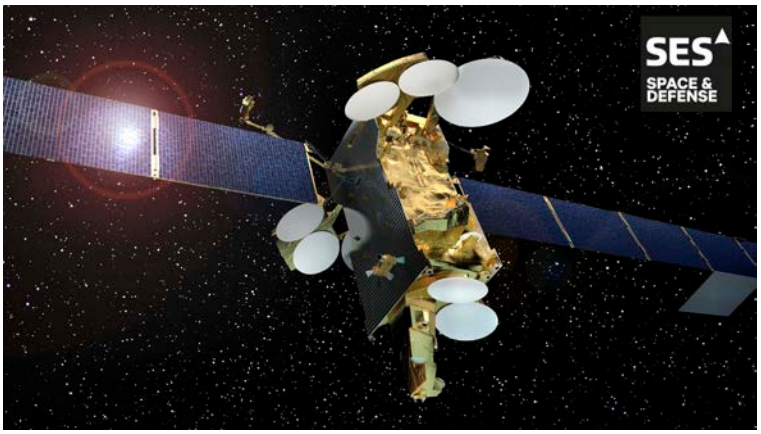


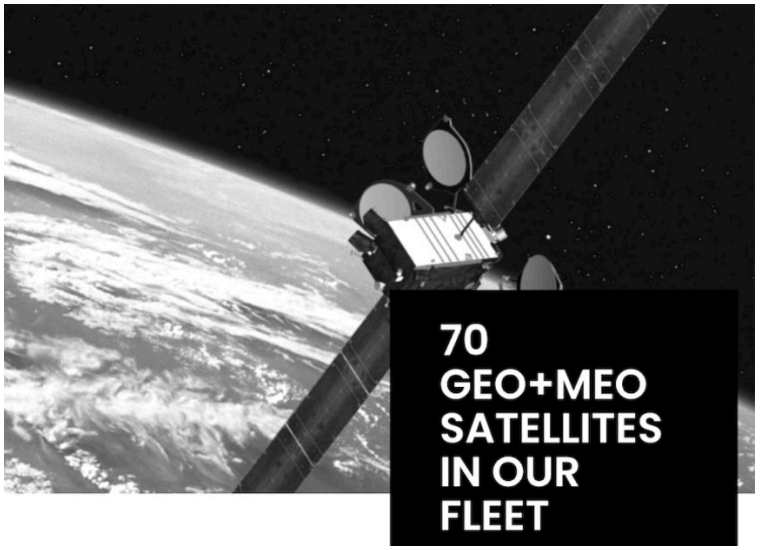
500W Linear Power

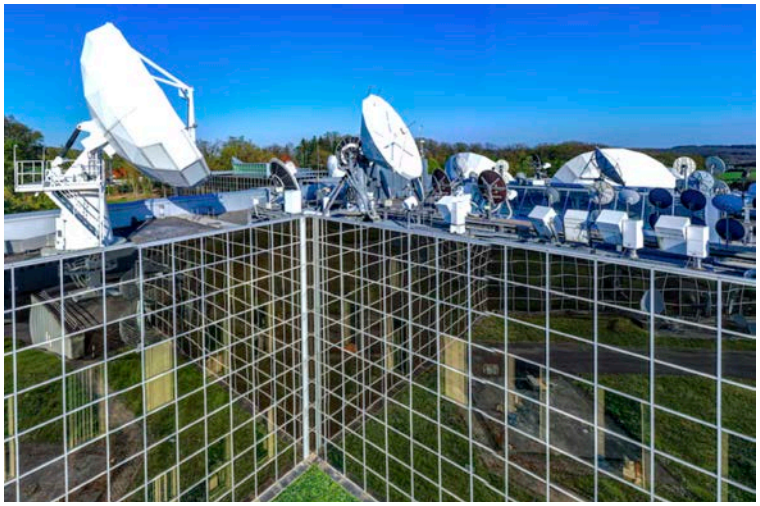


2kW Linear Power

1kW Linear Power







SES GOVERNMENT SOLUTIONS' NEW NAME, SES SPACE & DEFENSE, IS GEARED TOWARD U.S. GOVERNMENT + DOD SPACE AND DEFENSE NEEDS

SES' $450 million acquisition of DRS Global Enterprise Solutions to double U.S. Government (USG) business

SES Government Solutions (SES GS), a wholly-owned subsidiary of SES, will start operating under the new name SES Space & Defense, effective immediately.

The name change comes after combining ***SES Government Solutions*** with the company's recent acquisition of ***DRS Global Enterprise Solutions*** (**DRS GES**).

The SES Space & Defense brand reflects the organization's new positioning and expanded offering serving the needs of the U.S. Government customers.

THE MISSION

The renamed company will provide mission assurance to U.S. Government customers with resilient, low-latency satellite communications (SATCOM), hosted payloads as well as a broad range of effective end-to-end solutions.

Over the past four months, SES Space & Defense saw the appointment of its new leadership team, as well as the integration of capabilities that reflect the newly combined organization and differentiated value proposition.

The company is focused on building, managing and supporting the most advanced satellite network solutions for the U.S. Government and Department of Defense (DoD).

SES Space & Defense has been restructured to serve customers across two integral markets — space and defense — by creating two business units, ***Space Initiatives*** and ***Defense Networks***, to provide best-in-class satellite network solutions.

- ***The Space Initiatives unit targets fleet-centric projects leveraging SES's global, multi-orbit, satellite fleet, infrastructure, and assets.***
- ***The Defense Networks unit is centered on multi-operator managed services and end-to-end, mission-critical communications.***

SES Space & Defense's customers will benefit from new integration capabilities with the addition of the ***Information & Communications Technology*** (**ICT**) ***Ecosystem*** and ***ICT Portal,*** which provides a single pane, glass view into network performance, as well as essential tools in cybersecurity.

"*This is a major milestone for us, and more importantly for our U.S. DoD customers,*" said SES Space & Defense President and CEO, ***David Fields***. "*In August, we consolidated two best-in-class organizations focused on the U.S. Government satellite communications needs, and we remain fully committed to providing innovative world-class space solutions to our most tactical customers. With SES Space & Defense as our new name, we would like our strategic vision and focus to come through brightly.*"

https://sessd.com/

KRATOS RECEIVES MILLION$$ IN INITIAL FUNDING FOR C5ISR PRODUCTION PROGRAM

***Kratos Defense & Security Solutions, Inc.** (Nasdaq: KTOS) has received an initial $30 million in funding on a potential $250 million Command, Control, Communication, Computing, Combat System Intelligence, Surveillance and Reconnaissance (C5ISR) program.*

This new contract is single award to Kratos, a technology company in the National Security market and a leading provider of systems, subsystems, components and solutions for mission critical programs, including in the unmanned aerial drone, hypersonic, space, satellite communication, propulsion system, cyber warfare and microwave electronic areas.

Work under this new program award will be performed at secure Kratos engineering and manufacturing facilities.

Due to competitive, security and other considerations, no additional information will be provided related to this program award.

Yonah Adelman, President of Kratos Microwave Electronic Division (KMED), said, "*Our entire division has been working for an extended period to be successful on this competitive new program opportunity, now the largest single program award in KMED's history.*"

Eric DeMarco, President and CEO of Kratos, said, "*Yonah and his team's success on this new, mission critical, National Security related program opportunity is representative of Kratos' successful strategy of providing leading edge disruptive technology products and systems to our customers at an affordable cost.*"

www.kratosdefense.com

THINKOM + INMARSAT GOVERNMENT TO DELIVER HIGH-BANDWIDTH SATCOM FOR DOD

ThinKom Solutions, Inc. and Inmarsat Government have collaborated to deliver more efficient and reliable satellite communications (SATCOM) for tactical operations.

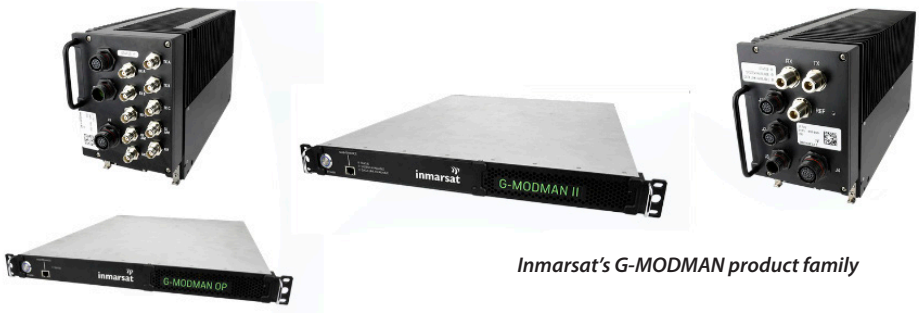
The pair will combine ***ThinKom's ThinAir® Ka2517*** antenna with ***Inmarsat Government's G-MODMAN II*** and ***G-MODMAN Open Platform*** (**OP**) modem managers to support ***Department of Defense*** connectivity around the globe.

The solution enables the vision of Advanced Battle Management System contribution to Joint All Domain Command and Control (JADC2) operations. This unique combination delivers on many facets of the U.S. Government's tactical edge efforts. By enabling cloud-based computing, seamless data sharing, intelligent operations, or autonomous use cases, the innovative solution reduces decision-making timelines for intelligent assets supporting troops in the field.

This configuration is the first of its kind to cover the full Ka-band frequency range in one terminal, providing greater access to current and future satellite constellations and associated services, while significantly lowering the physical profile on the airborne platform. It significantly reduces aircraft downtime and component swap requirements previously required for different mission deployments. The combined technologies bring several additional operational efficiencies to the market, including:

- ***Agility to interoperate seamlessly with satellites in geostationary and non-geostationary orbits, ensuring worldwide connectivity meeting the JADC2 requirements for multi-orbit, multi-constellation operations.***
- ***Improved satellite switching capabilities to ensure uninterrupted connectivity while maintaining network security for all U.S. Government applications.***
- ***Reduced drag, thanks to the ThinAir Ka2517 low-profile radome, resulting in lower fuel consumption and longer time on station, without refueling,***
- ***Flexibility to work on the broadest possible range of aircraft sizes and configurations.***

ThinKom ThinAir® Ka2517 phased array



Inmarsat's G-MODMAN product family

The fully type-approved quad-band version of the ThinAir Ka2517 SATCOM aero terminal can operate on ***Inmarsat's Global Xpress*** (**GX**) worldwide satellite network. This includes seamless switching on the GX commercial network's global service beams and Inmarsat's high-capacity, global military Ka-band network's steerable beams, plus the capability to connect to the U.S. Government's ***Wideband Global SATCOM system*** (WGS).

Artistic rendition of a USSF WGS satellite on-orbit

This flexibility and interoperability provide Inmarsat Government's customers with always-on availability, capacity, coverage and capability for a wide range of mission profiles.

Additionally, the ThinAir Ka2517 antenna and G-MODMAN II combination deliver a future-proof solution for government customers. The offering is compatible with the Ka-band satellites in orbit today, as well as Inmarsat's fully funded technology roadmap.

To meet increasingly complex SATCOM capability and throughput demands, Inmarsat will launch a further six satellites by 2025 and significantly expand its ground network to support them. This includes additional capacity, coverage for both commercial and military Ka-band capabilities worldwide, as well as two highly elliptical orbit satellite payloads for Arctic coverage.

The Ka2517 is based on ThinKom's field-proven, patented ***VICTS*** phased-array technology. VICTS antennas have an unparalleled record of reliability with installations on over 1,550 commercial aircraft with over 31 million hours of accrued flight time and a mean-time-between-failure exceeding 100,000 hours. Ka2517 antennas have been providing continuous service on U.S. government aircraft since 2018.

The G-MODMAN II modem manager is a flexible, easy-to-use solution that seamlessly integrates with the ThinAir Ka2517 and provides the enabling technology to support the implementation of the current and future generation of GX services across aviation platforms.

G-MODMAN II builds on Inmarsat's robust monitoring system and includes high-fidelity monitoring and logging features, allowing easy access to mission-critical data and enabling highly detailed performance and trend analysis that leverages advanced ***Machine Learning and Artificial Intelligence*** (**ML / AI**) techniques.

"Delivering efficient connectivity to our government users around the globe is of paramount importance to ThinKom," said **Bill Milroy**, CTO and chairman of ThinKom Solutions. *"We're proud to work with Inmarsat Government to combine ThinKom's highly reliable and efficient Variable Inclination Continuous Transverse Stub (VICTS) phased-array antenna into a communications package that delivers every time and everywhere."*

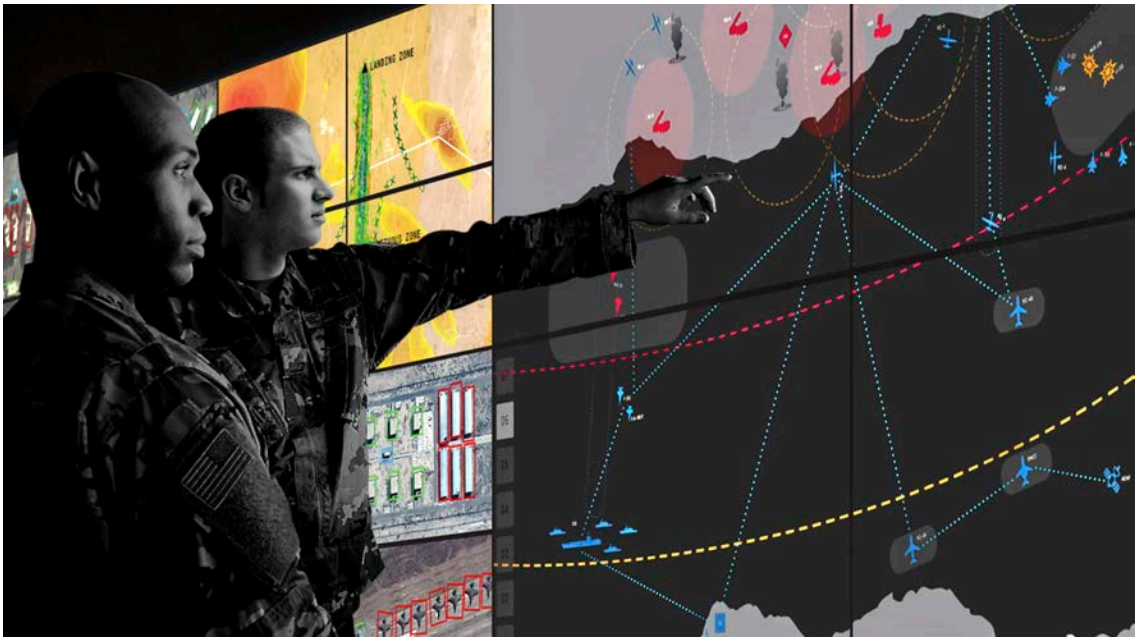
Matt Wissler, Chief Technology Officer, Inmarsat Government said, *"Integrating the spectral efficiency of the ThinAir Ka2517 with Inmarsat Government's G-MODMAN II modem manager delivers a powerful, turnkey solution for our government customers. Our efforts with ThinKom will result in substantially improved satellite communications resiliency while improving airborne platform range through reduced aircraft drag leading to lower fuel consumption."*

ThinKom

inmarsat GOVERNMENT

RAYTHEON INTELLIGENCE & SPACE DEVELOPING A COMMON TACTICAL EDGE NETWORK FOR THE USAF'S ADVANCED BATTLE MANAGEMENT SYSTEM

Raytheon Intelligence & Space, a Raytheon Technologies business, has been selected to develop a Common Tactical Edge Network, or CTEN, in support of the U.S. Air Force's Advanced Battle Management System. RI&S is one of nine companies selected to demonstrate portions of the network.



CTEN will provide edge networking to help operators enable distributable battle management command and control in highly contested environments to support ***Joint All-Domain Command and Control***.

Raytheon Intelligence & Space will build upon advanced networking products previously developed, to demonstrate an architecture that enables aerial network interoperability. To support this development, RI&S will expand its expertise in model-based systems engineering and DevSecOps as the basis for the design to support this development.

CTEN is RI&S' latest milestone to advance the Air Force's alignment with the DOD's JADC2 vision. Raytheon Technologies was recently selected as an industry partner for the **U.S. Air Force ABMS Digital Infrastructure Consortium.**

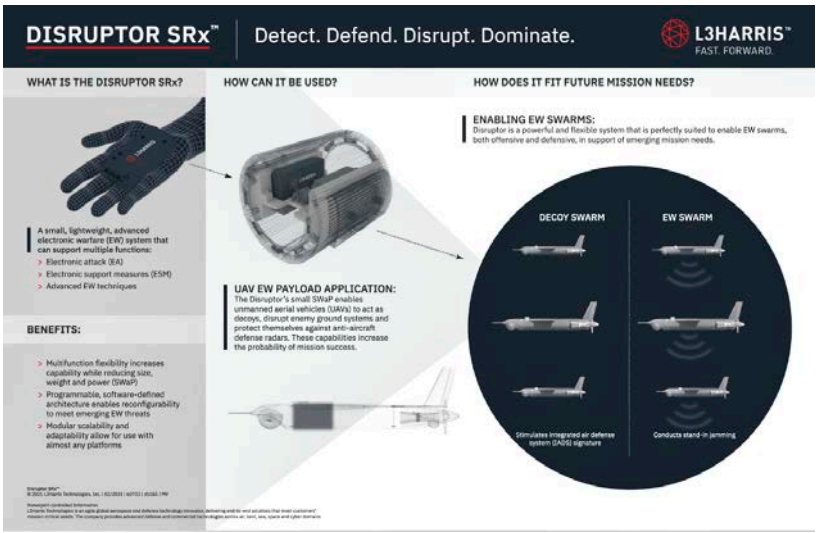
Raytheon Technologies is contributing its multi-domain footprint of capabilities in space systems, resilient communications, sensors, effectors, secure processing, artificial intelligence, machine learning and mission software to the DOD JADC2 architecture.

Raytheon Intelligence & Space work will be completed out of the Air Force Life Cycle Management Center, Aerial Networks Division at ***Hanscom Air Force Base***, Massachusetts. The selected companies will demonstrate their solutions in the fourth quarter 2022.

"We have a rich history of creating resilient, collaborative and secure networks," said Paul Meyer, president, Department 22 at RI&S. "This enables us to put forward a solution ready to meet the U.S. Air Force's need for an interoperable and integrated convergence layer."

"*At Raytheon BBN, we've been advancing state-of-the-art wireless communications systems since the 1970s*," said ***Jason Redi***, Raytheon BBN president. "*Today, we have focused investments in creating networked communications that span every domain from underwater to outer space. We are ensuring these new advancements provide our customers critical advantages faster, as they layer secure communications across multiple platforms in joint, all-domain, distributed, disrupted, disconnected and denied environments.*"

www.raytheonintelligenceandspace.com



L3HARRIS AWARDED A POTENTIAL MILLION$$$ CONTRACT IN SUPPORT OF ENHANCED BATTLESPACE ISR

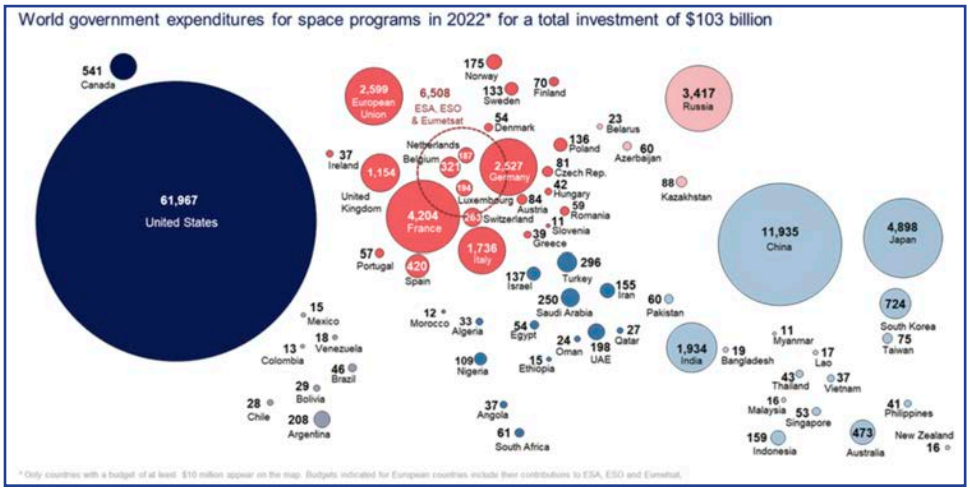
The U.S. Army Communications-Electronics Command has awarded L3Harris Technologies a contract worth as much as $886 million to support intelligence, surveillance and reconnaissance (ISR) capabilities for the U.S. Army, Department of Defense and the intelligence community.

The ***indefinite delivery, indefinite quantity*** (**IDIQ**) contract includes a five-year base award with five one-year follow-on options to provide datalink architecture, network design enhancements for aerial and ground-based communications, and lifecycle management support.

Applying its ***Trusted Disruptor*** approach, L3Harris continues to evolve its ISR and resilient communication solutions that helps inform prudent planning and timely decision making, with innovative multi-beam, active electronically scanned array techniques, multi-constellation orbit data transports for aerial and ground systems, and protected datalink and smart network exploitation capabilities.

"*These links will deliver resilient, fast and discreet multi-domain communications across the globe*," said ***Brendan O'Connell***, President, Broadband Communications Systems, L3Harris. "*As a provider of Army aerial ISR, ground line-of-sight and satellite communications terminal solutions for over 40 years, we look forward to continuing to build on this legacy of providing timely, relevant solutions that meet the expanding needs of our customers.*"

L3Harris Technologies is an agile global aerospace and defense technology innovator, delivering end-to-end solutions that meet customers' mission-critical needs. The company provides advanced defense and commercial technologies across space, air, land, sea and cyber domains. L3Harris has approximately $17 billion in annual revenue and 47,000 employees, with customers in more than 100 countries. L3Harris.com.



REPORT REVEALS RISING GOVERNMENT SPACE DEFENSE SPENDING

The new 2022 edition of Euroconsult's "Government Space Programs" report provides detailed insight into rising government space budgets in civilian and defense applications for the decade ahead, highlighting spending patterns and specific areas of investment from nations around the globe.

Euroconsult has released the 22nd edition of its annual " revealing a continued increase in global governments' space budgets. This year has seen a cumulative spend of $103 billion in 2022, a 9% increase since last year and a record high for the sector. Despite the recent pandemic crisis, governments have increased their investments in the sector to further support the development of their industry and sustain their ambitions.

This growth is notably significant in the defense area, reaching 16% in 2022 and topping a new record at $48 billion. Current geopolitical tensions have confirmed space as a strategic operational theater for hybrid warfare tactics, pushing governments to sustain their investments in 'traditional' space applications such as ***Telecommunications***, ***Navigation*** and ***Earth Observation*** (**EO**) , but also more prominently in ***Space Security & Early Warning*** systems to further protect their space assets.

On the civil side, government expenditures are increasingly driven by Human Spaceflight missions, which now attract more and more new entrants encouraged by the socio-economic benefits and prestige brought by these programs.

While civil expenditures have historically always been higher than defense spendings, the gap between the two continues to decrease and is expected to reach 50/50 parity by 2031, according to Euroconsult's projections.

In terms of national rankings, the U.S. remains, by far, the largest investor worldwide. However, its share of global spending has been reduced, from 76% in 2000 to 60% in 2022 as more and more countries join the sector. This year, Euroconsult counted more than 86 countries invested in space activities. Some regions have shown a particular dynamism over the past few years, notably in the Middle East with countries as **Saudi Arabia**, the **UAE**, **Qatar** and **Oman** accelerating their development in the sector.

Charlotte Croison, Senior Consultant at Euroconsult, said, "*The new edition of the Government Space Programs report confirms the growing interest of countries in the space sector, notably in the defense area where space militarization has never been stronger.*"

Euroconsult's 22nd edition of "Government Space Programs" provides a comprehensive assessment of countries and organizations investing in space. The report is available on Euroconsult's Digital Platform, enabling customers to easily sort, compare, customize and visualize datasets of their choice. For additional details, ***access this direct infolink...***

GOVERNMENT SATELLITE REPORT (GSR)

How AI/ML is the key to protecting the U.S. Army's space assets

Author: David Pesgraves, Government Satellite Report (GSR)

At the October 2022 Annual Meeting of the Association of the United States Army (AUSA), digital transformation took center stage as U.S. Army leadership and representatives from commercial industry explored the new and innovative software that is delivering immense benefits to America's largest military branch.

These advancements arrive at a critical moment, as U.S adversaries continue to aggressively develop new technologies that can potentially interfere with and degrade Army warfighting capabilities on the ground, and in the air and space domains as well.

During the modernization and digital transformation sessions at AUSA 2022, attendees learned that the U.S. Army has begun to adopt cutting-edge technologies to be able to maintain both deterrent and warfighting advantages over its adversaries.

Autonomous technologies, such as artificial intelligence (AI) and machine learning (ML), are top of mind for the Army, especially as it pertains to protecting its assets in space.

The U.S. Department of Defense's (DoD) interests in space do not end with the U.S. Space Force and Air Force.

All military branches have a deep reliance on space, as most of the military connectivity, communications, intelligence, surveillance, and reconnaissance activities likely pass through the DoD's space architecture at one point in time.

This is particularly true for the Army.

For warfighters in off-grid environments, connectivity provided by satellite communications (SATCOM) can sometimes be their only line of communication to mission leaders and decision-makers at central command.

Army leadership relies on SATCOM to make intel-based decisions and then transmit those orders to the warfighter in theater.

Without SATCOM, warfighters can be left in the dark, putting their mission and lives at risk, and senior decision-makers would lack the real-time intelligence they need to make data-driven decisions.

ARMY AUTOMATION THROUGH AI/ML

U.S. near-peer competitors are fully aware of how critical SATCOM services are to the U.S. Army and look to undermine and degrade them by any means necessary.

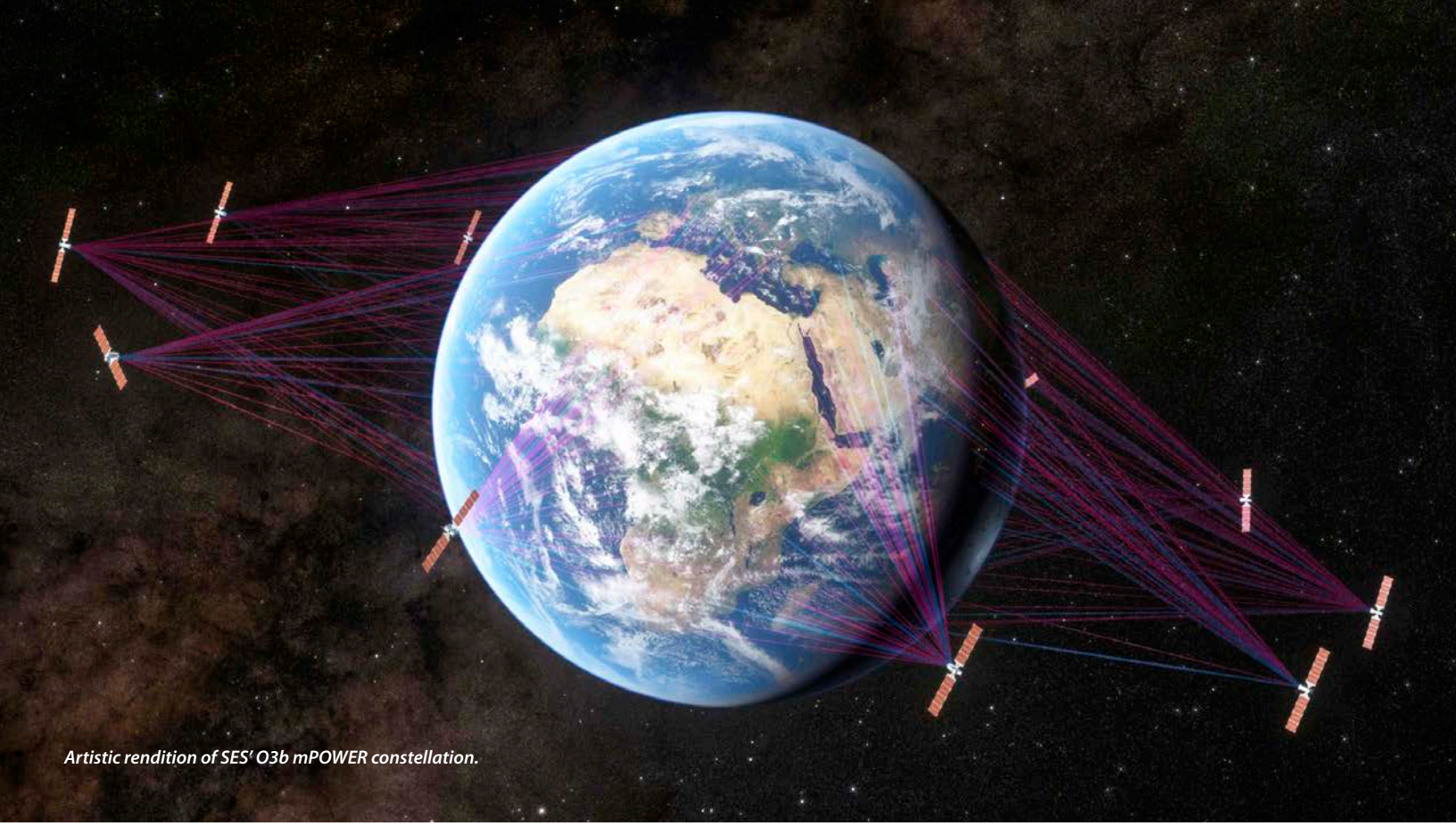
From jamming to kinetic attacks — which adversaries such as China and Russia have proven to be capable of employing — the Army must protect its satellites and other space assets from these types of threats by developing and employing new technologies that are capable of defending against such attacks.

Apparently the Army has found that cutting-edge defensive solution in AI/ML. Thankfully, these solutions couldn't have come at a more opportune time, as U.S. adversaries are now explicitly calling for the attacks of American commercial satellites.

In recent news coming out of Russia, senior foreign ministry officials at the Kremlin have stated that U.S. commercial satellites and their "*quasi-civilian infrastructure may be a legitimate target for a retaliatory strike.*"

As the threat to Army assets in space moves from theoretical to looming reality, the DoD has kicked its vision for a resilient space architecture into high-gear, with military leadership looking to AI/ML for automated threat detection and defense of American space assets.

One area of particular interest to the Army is having the ability to switch frequencies and signals across satellites and orbits.



Artistic rendition of SES' O3b mPOWER constellation.

If a satellite were about to be jammed, degraded, or destroyed, the Army can now start to deploy AI/ML software that can detect an attack before such occurs and transfer service over from the soon-to-be compromised satellite to another protected and available asset within the space architecture.

Through advancements in AI/ML automation, detection and response of potential interference or targeting occurs much faster than it would with manually monitoring.

If a space asset has indeed been compromised, AI/ML enables satellite frequencies to automatically roll over to another satellite in the same orbit, or even a different orbit, denying any enemy attempts to interrupt service.

This new technology is invaluable, as Army decision-makers cannot afford to have congested or degraded communications, especially when critical missions and lives on the ground are at stake.

O3B MPOWER + SMART TECH

For commercial satellite companies like ***SES Space and Defense***, these AI/ML advancements will complement the natively smart capabilities that have been installed on their newer satellites.

The company's highly anticipated ***Medium Earth Orbit*** (**MEO**) constellation — ***O3b mPOWER*** — will be inherently hardened against such adversarial attacks and will have automated detection and response capabilities already baked into the assets.
To take it a step further, SES has also successfully tested O3b mPOWER's multi-orbit capability set, which is a critical component for AI/ML technology to operate seamlessly.

In September of 2021, ***SES*** and ***Hughes*** successfully used the ***Hughes Resource Management System*** to seamlessly switch signals across SES satellites in **MEO** and Geostationary orbit (**GEO**).

According to ***Jim Hooper***, SES Space and Defense's Senior Vice President for Space Initiatives, the successfully multi-orbit tests illustrated, "*…the power of next-generation satellite services and technologies to provide mission-critical, assured communications to the government and military, at a time when connectivity is increasingly essential.*"

Increasingly autonomous COMSATCOM software that leverages AI/ML, combined with the smart technology that has already been built into commercial satellite constellations, such as O3b mPOWER, can provide the U.S. Army with a more resilient space architecture.

As a result, the Army will be fully prepared to thwart adversarial attacks and continue to deliver seamless and interrupted connectivity, communications, intel, and other mission-critical services to warfighters on the ground.

To learn more about how Hughes and SES successfully switched signals between GEO, MEO, and LEO satellites, ***select this direct infolink...***

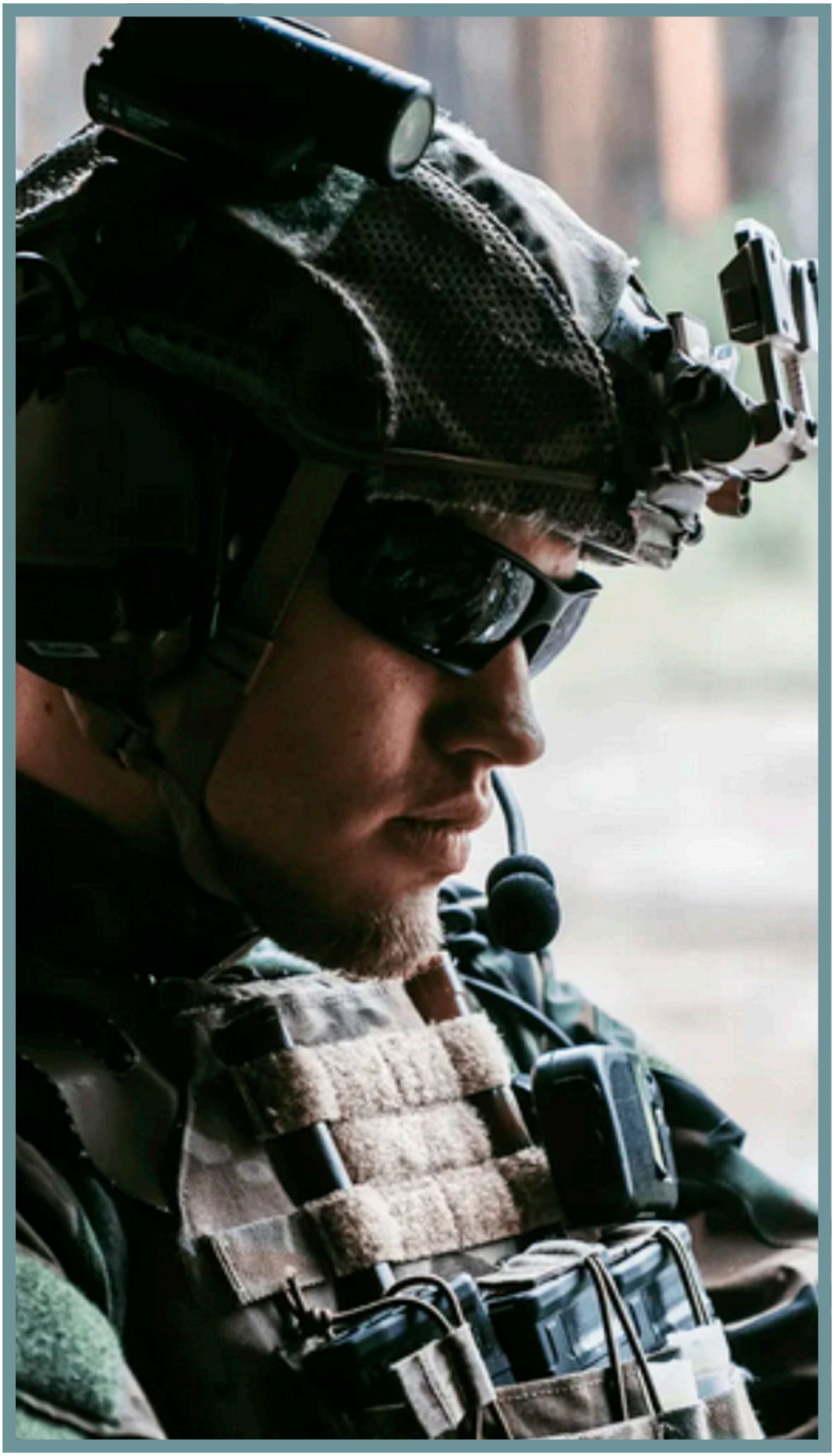
sessd.com/govsat/

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

DEFINING RESILIENT + SECURE ARCHITECTURE

Infrastructure is only as good as the ability to secure the data and make it available and accessible

Author: Rob Spalding, Chief Executive Officer, SEMPRE.ai



When SEMPRE was founded in 2019, it was premised on the belief that 5G was moving cellular infrastructure increasingly to software, away from bespoke hardware — it was a seized opportunity to rethink architecture for telecommunications.

The idea was to take non-resilient and unsecure infrastructure and make it hardened and secure. It's been a long four years, but SEMPRE has shown that such is possible. This article is about the principles that went into developing that architecture.

When the ***iPhone*** came out in 2007, there were technologies in the phone that had yet to evolve. Today, one sees the full evolution of ***Steve Job***'s vision, but unfortunately, infrastructure has not kept pace with software.

For example, in a sense, a smartphone can be turned into an infrastructure device by making it a Wi-Fi hotspot. Why not apply the concept to infrastructure by consolidating all the software into an autonomous, self-enclosed infrastructure node?

Like the iPhone, SEMPRE thinks of its network nodes as devices, or rather, as decentralized infrastructure architecture that can be made resilient and secure, using ORAN and other technology initiatives.

It is important to note that it is the evolution of cellular into software that makes this possible. The evolution could not have happened until ***3GPP*** specifications introduced the widespread use of network function virtualization, software-defined networking and software-defined radios.

5G is taking all the pieces of the hardware and bringing them into software. Yet the architecture the telecom industry is using, even in the newest 5G stand-alone networks, is the same architecture used to build 4G LTE networks.

For instance, the ***Core Network/Centralized Unit*** (**CU**), ***Distributed Unit*** (**DU**) and the ***Radio Unit*** (**RU**) are all geographically separated. Anywhere along the way if access to any of these is severed, a cell tower won't work.

Fragility has been built into the current system despite the fact almost the entire network is software running on ***Commercial-Off-The-Shelf*** (**COTS**) servers.

SOFTWARE CONSOLIDATION

The first principle for creating security and resiliency is **software consolidation** into a single node.

The second is **hardening**; as zero trust is important in security and resiliency, it is not sufficient to only consolidate.

All the technology that goes into powering smartphones today can be run by software in self-enclosed autonomous infrastructure nodes that allow all the security and resiliency to be built into the node.

Pairing that infrastructure node with satellite backhaul puts the internet anywhere on Earth.

Latency and bandwidth issues are less of an issue as the datacenter is in the node for ***Edge processing*** running applications and caching data.

This creates a fiber experience at the very edge of the network with satellite constellations. In other words, cellular for the first time allows the fusion of space and terrestrial networks in a more secure, resilient, efficient, and cost-effective way.

Today network operators cannot get the most out of the network infrastructure because the industry looks at satellite networks and terrestrial networks separately. This is because the telecom industry has been highly centralized and satellite networks were thought to enable distinct use cases and customers.

Consolidating all of the capabilities of today's networks into software can enable interesting things like having multiple satellite modems in software, thereby giving enormous flexibility and resiliency.

SECURE CONTROL PLANE

Satellite networks can be used for more than a transport layer where communications are concerned.

In SEMPRE's architecture, the control plane is run through a secure satellite constellation for globally assured secure command and control of SEMPRE's infrastructure nodes. SEMPRE's encrypted data plane, on the other hand, liberally uses existing constellations to ensure the most cost-effective paths for back haul. This creates a hybrid network that is both open and closed providing secure yet interoperable services to the customer.

HARDENING

Consolidating software into a single. self-enclosed. autonomous network node gives the ability to harden it against threats in a way that wasn't possible before — threats such as **EMP/HEMP** events.

Hardening is not an additional expense because 5G allows one to share the ***Radio Access Network*** (**RAN**) at the edge. That means savings of up to 40% on ***Capital Expenditures*** (**CAPEX**).

Tamper resistance is another important, zero-trust feature as infrastructure nodes are physically available, without restrictions on a person simply walking up and touching one. Today we have tamper-evident seals that may give an indication that something's been tampered with, but how often are the actual sites visited to check the seals?

Building tamper resistance into infrastructure, making it **EMP-hardened**, and pairing it with multiple, satellite backhaul networks enables resiliency. Today, resiliency is not built into infrastructure, and that makes our nation and our communities vulnerable. This was evident two Christmases ago when a domestic terrorist blew up his Winnebago near the AT&T switching center in Nashville, Tennessee.

Tennessee and the surrounding states lost mobile service and e911 for up to two weeks. Fully functioning cell towers didn't work because they had lost connection to the core Network.

ENCRYPTION

Encryption is a necessity when it comes to survivable and secure infrastructure. Post-quantum encryption is important for ensuring it isn't broken by a quantum computer.

NIST (***National Institute of Standards and Technology***) and the **NSA** (***National Security Agency***) are putting forward potential candidates for post-quantum encryption.

DATA MODEL

Another principle to consider is the data model itself. Today the industry looks at security using a "*rings around things*" model. They put ever higher walls around data, but ultimately when one gets to that data it's open and often unencrypted. Ensuring data is encrypted — no matter whether it is being moved, stationary or being acted upon— is an important part of resilient and survival infrastructure.

Ultimately the infrastructure is only as good as the ability to secure the data and make it available and accessible.

A NEW COLD WAR

Finally, when considering what the future holds, whether it be Russia's invasion of Ukraine or Chinese threats to invade Taiwan, the world is witnessing a lot of nuclear saber-rattling.

This is going to accelerate as the world moves deeper into the second Cold War.

Today, the world is split into two halves — the free and the unfree.

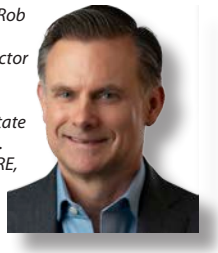
Consider...

Nuclear weapons are still out there, and they are enormously dangerous. This will affect the satellite industry in technology, business models as well as risk.

It is important that the industry starts to consider these things and takes advantage of the consolidation of infrastructure in software and initiates the effort to fuse terrestrial and satellite networks in ways that make them more secure, resilient, cost-effective and efficient.

sempre.ai

SEMPRE
INTEGRITY | SERVICE | INNOVATION



U.S. Air Force Brigadier General (ret) Rob Spalding is the former White House National Security Council senior director for strategic planning and served in senior positions of strategy and diplomacy within the Defense and State Departments for more than 26 years. Rob is the founder and CEO of SEMPRE, a technology company created to protect and secure our most critical resource: data. Rob has served in senior positions of strategy and diplomacy within the Defense and State Departments for more than 26 years, retiring as brigadier general. He was the chief architect for the widely praised 2017 National Security Strategy and the Senior Director for Strategy to the President at the National Security Council. Rob's innovation while serving in the White House has led to a reset in national security and public policy regarding telecommunications in the U.S. as well as across the globe.

Rob has written extensively on national security matters. His academic papers and editorial work are frequently published and cited, nationally and internationally and he is the author of "STEALTH WAR: How China took over while America's elites slept" and "War without Rules. Rob is a skilled combat leader and a seasoned diplomat.

SPACE SYSTEMS COMMAND: A COMMAND CENTER CONVERSATION

Brigadier General Timothy Sejba

How an exploit, buy, build strategy is fueling rapid, resilient acquisition

Authors: SSC Public Affairs Team

Brig. Gen. Timothy Sejba directs two diverse Space Systems Command (SSC) portfolios of more than 60 space programs. He serves as Program Executive Officer (PEO) for SSC's Space Domain Awareness (SDA) and Combat Power office and for the Space Development Agency's Battle Management, Command, Control, and Communications (BMC3) office.

Gen. Sejba oversees mission areas including space domain awareness, space control, strategic warning and surveillance, defensive cyber operations, innovation and prototyping, data transport, and operational and tactical command and control systems.

His responsibilities include approving program strategies, overseeing all aspects of his teams' delivering programs to meet warfighter needs, and engaging with Headquarters United States Space Force (USSF), the Office of the Secretary of Defense, and other military forces, departments and government agencies.

Recently, the general discussed recent successes, how ***space domain awareness*** (**SDA**) is changing, and what SSC is doing to meet the threats and become more resilient in protecting our nation.

General, you are the PEO for SSC Space Domain Awareness & Combat Power and Battle Management Command, Control and Communications —how do those mission sets fit in with the USSF's overall mission?

GEN. TIMOTHY SEJBA

The Space Force is a military service whose mission is to defend U.S. and allied interests in space. For years, service and joint commanders have stated that ***space domain awareness*** *(***SDA***) is their highest priority need.*

Perpetual and prolific SDA is the foundational requirement to enable decisive action in the space domain. SDA is essentially how we '*see and avoid*' in space — that is one of the major capabilities we provide.

Our nation recognized space as a vital U.S. national interest decades ago. Additionally, the increasing ability of nations such as China and Russia to hold our space assets at risk via counter-space weapons created the clear need for a military service dedicated to organizing, training and equipping forces for a contested space domain.

SSC develops and operates national security deterrence capabilities to provide continued sustainable use of space by countering threats and aggression and, when necessary, to prevail in a multi-domain conflict that extends to space.
We focus on quickly responding to warfighter requirements by designing, building and maintaining unrivaled offensive and defensive counter-space capabilities required for space superiority.

Space superiority means we can conduct operations in space at any time or any place without prohibitive interference from terrestrial or space-based threats.

Battle Management Command, Control and Communication contributes to the missions above by developing and fielding critical ***Operational Command and Control*** capabilities for a contested space domain. ***Space Command and Control*** provides capabilities that enable our warfighters to make timely, quality driven battlespace decisions for the space domain fight.

SSC's portfolios are intertwined through key mission threads. I use the term intertwined purposely, and our Commander's intent really centers around that philosophy — that the portfolios are tied together. They have a highly symbiotic relationship as both a prime contributor to and a prime recipient of the outputs and capabilities of each portfolio.

You recently spoke at Space Industry Days about Lt. Gen. Michael Guetlein's new SSC Guiding Principles — Focus on the Threat; Exploit/Buy/Build; Unity of Effort and Build a Culture of Experts. Would you tell us more about the Exploit/Buy/Build investment strategy?

GEN. TIMOTHY SEJBA

'***Focus on the Threat***' is really where everything starts. While China and Russia are peer competitors — make no mistake about that — China is the pacing challenge. Rapidly evolving threat demanded a new approach to acquisition, so we will be ready for the fight tonight, the fight in 2026... **and beyond**.

'***Exploit What We Have***' means squeezing all the juice (*mostly data*) out of the systems we have online today for the '***Fight Tonigh***t' scenario.

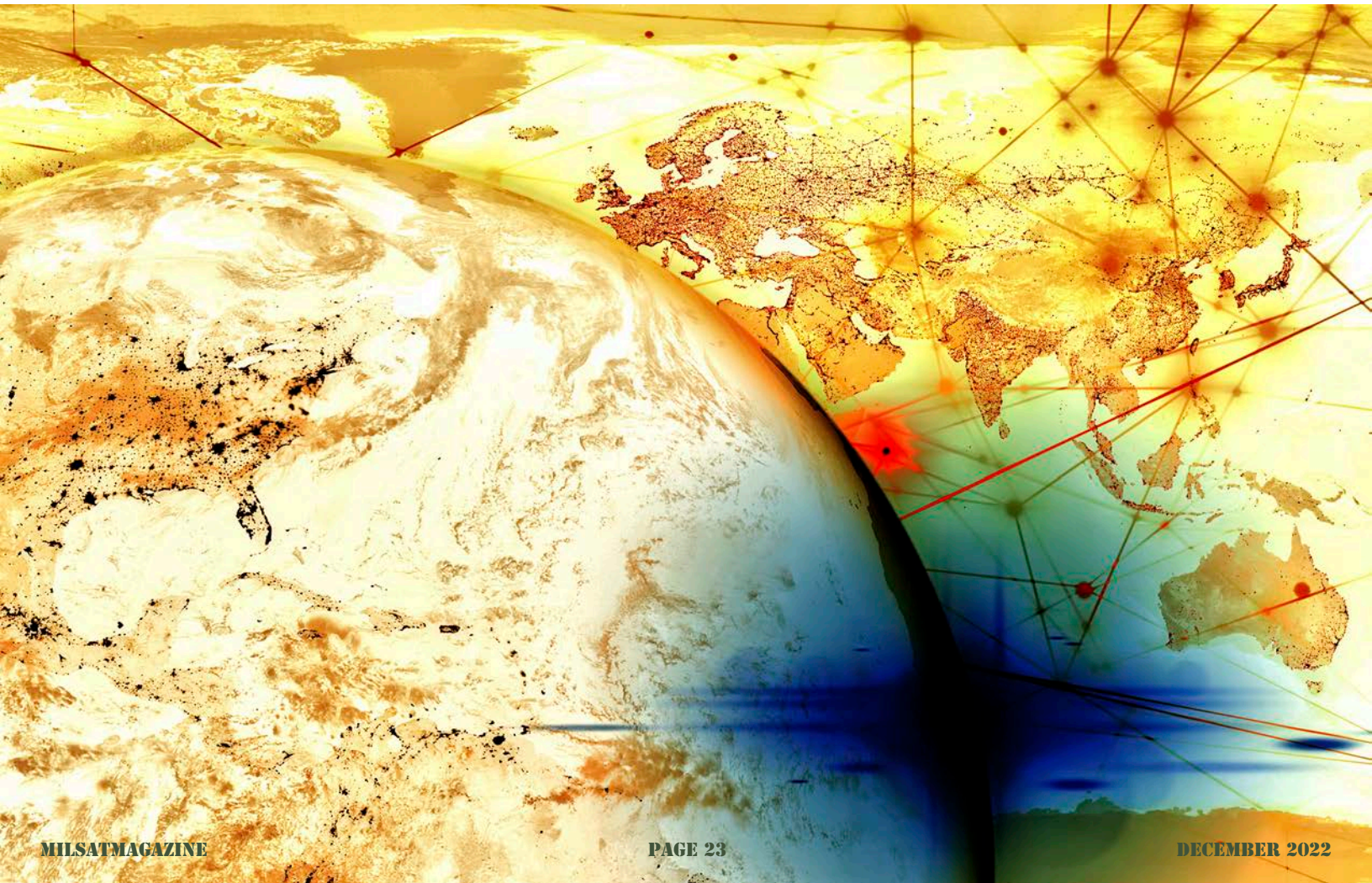
'***Buy What We Can***' is the cornerstone of going after the 2026 threat and involves everything from commercial purchases and services to commercial launch.

This concept involves transitioning dual-use technology that may have been developed for other industries, commercial ride shares — using excess capability on commercial satellites — and purchasing analytic services or new tools to maximize **Guardian** bandwidth.

Finally, '***Build Only What We Must***' is our investment strategy for the future fight. In a contested environment, we need to design with resilience as a top priority.

Not all mission areas are mature enough to '*buy*' or have stringent security or warfighter requirements that demand exquisite systems. This three-pronged approach ensures we are delivering resilient, warfighting capabilities for all aspects of the fight and delivering space superiority when it is most needed.

'***Unity of Effort***' ties everything together. Working alone cannot guarantee U.S. space superiority. Countering the threat demands a concerted, united effort from across the government, industry, academia, and our international partners.



Lastly, SSC is committed to '***Building a Culture of Experts***,' to prepare the entire organization for the challenges that will come. That means building a diverse group of experts across all disciplines; having diversity of thought and a diverse workforce; being threat experts; and creating the environment where all of that can be enabled.

The 2026 threat challenge requires a short-term reliance on experts from sources I previously mentioned — government, industry, academia, and our allies. As we continue to grow and align with these experts, SSC is organized to pool expertise for end-to-end mission delivery.

What are some of your portfolio system in the field doing today to support Combatant Commands (CCMDs)?

GEN. TIMOTHY SEJBA

Our ***Space Domain Awareness*** (**SDA**) portfolio fields a broad set of capabilities which support numerous combatant commands.

For example, we are responsible for a broad set of systems that monitor the space environment and watch objects in space, characterize what is happening, generate indications and warnings for anyone who might need to be made aware of a potential threat — nefarious or environmental, such as space debris — and ultimately enable U.S. Space Command's operations.

Our cyber operations division currently has two product lines satisfying defensive requirements for cybersecurity and national security called ***Manticore*** and ***Kraken***.

Manticore is fielded on multiple United States Space Force (USSF) mission systems. Kraken is currently integrated into several mission systems to establish a pattern-of-life baseline.

Manticore and Kraken support Space Operations Command's ***Space Delta 6*** and its squadrons to protect their assigned mission systems, which support combatant commands.

Today, the capabilities we provide to cyber operators are protecting our mission systems through an enhanced cyber defensive posture.

Manticore is fielded on 11 ***United States Space Force*** (**USSF**) mission systems. Kraken is currently integrated on to two mission systems to establish a pattern-of-life baseline.

On the BMC3 side, in May of 2022, ***United States Special Operations Command*** (**USSOCOM**) operationally accepted our ***Unified Data Library*** (**UDL**) to track operations across the SOCOM enterprise and the real-time locations of their forces.

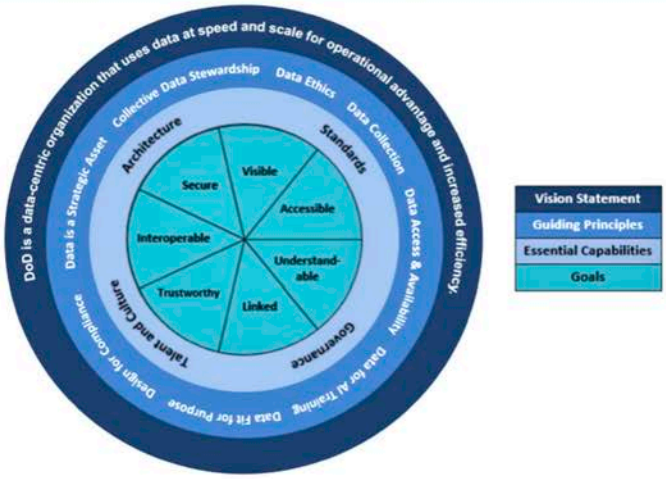
As such, UDL is the first cloud-based **U.S. Air Force / U.S. Space Force** system to receive a three-year ***Authority to Operate*** at each classification level (*Unclassified, Secret, Top Secret*), an astounding testament to UDL's solid security barriers.

SDA Systems Operating Today

- **Upgraded Early Warning Radars** - with a primary mission of Missile Warning but also see objects in Low Earth Orbit - and we take full advantage of that.
- **Ground-Based Electro-Optical Deep Space Surveillance System** - a worldwide telescope network which monitors objects in Geosynchronous Earth Orbit where spacecraft such as missile warning, military and commercial communications, and some weather satellites live.
- **Ionospheric Ground Sensors System** - a world-wide set of sensors which monitors the Ionosphere to anticipate when warfighters may experience disruptions to their satellite communications and proactively plan to ensure no impacts to operations.

Partial list

DOD Data Strategy Framework:
The application of UDL as a data layer in the USSOCOM Mission Command system/Common Operational Picture is a new benchmark for the use of UDL, which primarily supports USSF SDA. This milestone actively supports the Department of Defense Data Strategy and move to Joint all-domain operations.



Can you tell us about some of your recent successes in either portfolio?

GEN. TIMOTHY SEJBA

In April 2022, ***Space Operations Command*** accepted our ***Geosynchronous Space Situational Awareness Program*** (**GSSAP**) satellites 5 and 6 as operationally capable and has presented them to the ***U.S. Space Command*** for operational use... four months ahead of schedule.

Our expanded GSSAP constellation will allow for even more opportunity to respond to real-world threats. GSSAPs 5 and 6 launched from Cape Canaveral Space Force Station, Florida, last January.

GSSAP satellites collect ***space situational awareness*** (**SSA**) data that allows for more accurate tracking and characterization of man-made orbiting objects. GSSAP satellites operate near the geosynchronous belt and have the capability to perform ***Rendezvous and Proximity Operations*** (**RPO**).

RPO allows for the space vehicle to maneuver near a resident space object of interest, enabling characterization for anomaly resolution and enhanced surveillance, while maintaining flight safety.

Brig. Gen. Sejba speaking at Space Industry Days on Oct. 19, 2022, in Los Angeles. Photo by Van de Ha, SSC

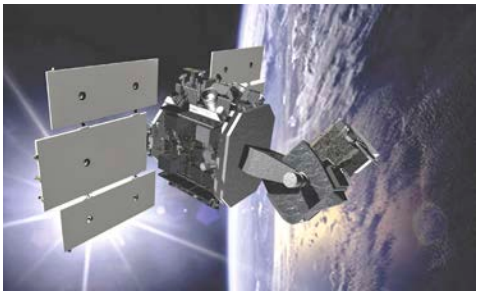
Data from GSSAP uniquely contributes to timely and accurate orbital predictions, enhancing our knowledge of the geosynchronous orbit environment, and further enabling space flight safety to include satellite collision avoidance.

In September, the ***Australian Department of Defence*** and USSF declared initial operational capability for the ***Space Surveillance Telescope*** (**SST**) at ***Naval Communication Station Harold E. Holt, Exmouth, Western Australia***.

The Space Surveillance Telescope. Image is courtesy of DARPA.

The SST is a military telescope that provides ground-based, broad-area search, detection and tracking of faint objects in deep space to help predict and avoid potential collisions, as well as detect and monitor asteroids.

The SST will contribute to the ***U.S. Space Surveillance Network,*** a U.S. Space Command capability operated by the USSF to detect, track, catalog and identify artificial objects orbiting the Earth. The telescope's strategic location in Australia provides unique space domain awareness coverage in the region.



Artistic rendition of a Space Surveillance Telescope on-orbit. Image is courtesy of USSF.

We led this international partnership to move SST to Australia in the spirit of strengthening our allied partnerships while exploiting existing capabilities.

The space objects that SST locates are natural phenomena — asteroids and comets — as well as the growing problem of space junk. This collaboration is a win for both countries.

What are the challenges to pivot the Space Domain Awareness mission in a congested and contested environment?

GEN. TIMOTHY SEJBA

Today's threat environment feels reminiscent of the Cold War, when the Soviets fielded significant counterspace capabilities. It stressed our then-SSA operators and demanded urgency of understanding the environment should a response be required.

Unfortunately, over time we lost our way a bit as part of the Post-Cold War Peace Dividend. SSA became synonymous with catalog maintenance and time, criticality, took a back seat to catalog accuracy.

We've rebranded SSA to Space Domain Awareness to re-emphasize threat mindedness. We must know not only where objects are in space but also what they might be doing, what their capabilities might be, what their patterns of life are, what their operational states are.

USSF Chief of Space Operations, ***General Saltzman***, has coined this type of SDA as "***Combat SDA***" — the level required for the joint fight.

As the lead acquirer of SDA capabilities, we must deliver what is required to enable Combat SDA.

We must field systems that eliminate our adversaries' freedom of action.

We must ensure all relevant data is available to warfighters and systems on tactically relevant timelines.

We must work with the Department of Commerce so some workload can be offloaded allowing our warfighters to focus on supporting the joint fight.

The U. S. Space Force successfully launched the Tactically Responsive Launch-2 (TacRL-2) mission on a Northrop Grumman Pegasus XL rocket from Vandenberg Space Force Base T, delivering a technology demonstration satellite to LEO.

We're opening the aperture and changing the focus from TacRL (*launch*) to the broader TacRS mission area.

End-to-end capability requires more than just launch — Space Safari responds to high-priority, urgent space needs in support of USSPACECOM and other combatant command requirements.

They use mature technology and existing production lines to quickly repurpose assets from multiple organizations.

TacRL-2, successfully launched in June of 2021, was able to turn around a launch within 11 months, as opposed to the previous average of two to five years.

Today, the benchmark for typical mission timeline is less than 12 months (*from initiation through launch*) and in 21 days or less from decision to launch to an asset being on-orbit... ***but that's not good enough***.

We are leaning further forward to execute the next rapid response mission in 2023 — ***VICTUS NOX*** (***Latin for "conquer the night"***) will perform an SDA mission from **LEO**.

This will be an operational demonstration against an operationally relevant threat using operational crews on operationally relevant timelines.

The SSC Commander, Lt. Gen. Guetlein, has stated the operationally relevant timeline for the next mission will feature an attempt to launch a satellite within 24 hours of receiving the "*go*" order.

The bottom line is that the SDA community is evolving in many ways.

Please tell us about SDA and Combat Power's role in the emerging Tactically Responsive Space (TacRS) mission area?

GEN. TIMOTHY SEJBA

First, ***TacRS*** is all about rapidly responding to on-orbit threats and augmenting existing capabilities.

For example, deterrence today can only succeed if our adversaries find our TacRS capability credible enough to enable military operations even in a contested environment.

Our peer adversaries must know the U.S. will retain superior warfighting capability, even after an attack — TacRS is a key capability in the concept.

SSC's ***Space Safari*** group and ***Assured Access to Space*** (**AATS**) program office partner aggressively on the TacRS challenge.

Those are our marching orders, and we are getting after the solution.

What are some of the cyber challenges SSC is facing?

GEN. TIMOTHY SEJBA

Much of the American way of life depends on computers, data — and that's just one more avenue our adversaries are pursuing to deny, degrade and destroy U.S. space assets.

Brig. Gen. Sejba, standing next to the bronze statue of Gen. Bernard A. Schriever in the Space Systems Command courtyard. SSC photo by Van de Ha

I previously mentioned our Manticore and Kraken cyber programs, but on a broader front, cyber defense is a requirement across the military's entire space architecture, on-orbit and on the ground.

If we're going protect and defend the architecture, it can't just be something we do against the space threat. It has to be against the holistic threat of both space and cyber.

Defensive cyber operations and capabilities are part of our portfolio. We protect and defend the entire mission and the architecture against threats from both.

At SSC, that means we're focused on everything from making sure we have the best-trained cybersecurity experts, to making sure our systems are resilient enough to withstand a variety of cyberattacks.

We are also teaming with our commercial partners and allies to ensure the systems we build and put into place are cybersecure.

We also leverage talent from ***DEFCON*** to bolster defensive practices in software development. DEFCON is the largest and longest running security research and hacking convention in the world.

This non-traditional approach leverages talents of academia, industry, and researchers across the globe by hosting an open competition.

DEFCON's "*capture the flag*" style competition uses representative ground and space infrastructure. Captured competitor tactics, techniques and procedures enhance the defensive postures for our critical space systems.

Finally, General, what's one thing you think people may not know about USSF/ SSC that you'd like them to know?

GEN. TIMOTHY SEJBA

I firmly believe that many Americans lack full awareness of two important facts.

First, s
pace is fundamental to U.S. prosperity. The United States harnesses the benefits of space for communications, financial transactions, public safety, weather, agriculture, navigation and more.

Space enables the modern world, and the United States needs to maintain its progress in this critical domain if it hopes to lead in the future.

When most Americans think of space, they think of NASA and space exploration, but they don't necessarily think of all that space brings to their daily lives.

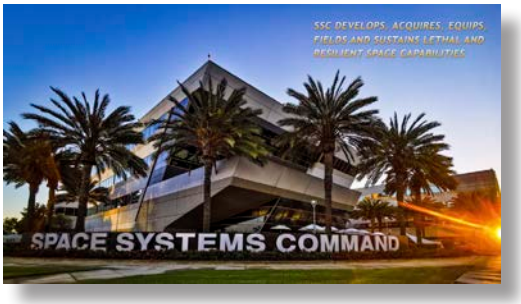
Every day, on countless occasions, billions of people are either directly interacting with or benefiting from a space asset. GPS, weather forecasts, gas station pumps, contactless credit cards, ATMs, satellite phone services, broadband internet services and countless more daily parts of our lives rely on information transmitted through the space domain via satellite.

The application on a hand-held device that gives directions, calls a rideshare or locates a lost package is enabled by the GPS constellation operated by the U.S. Space Force.

Second, the challenges to U.S. space leadership are real. China and Russia view space as vital to modern warfare and the U.S. and allied economies.

Those nations have developed counterspace capabilities to deny our access and diminish our military and economic effectiveness through space. Hence, space must be thought of as a warfighting domain just like air, land, sea and cyber.

Let me be very clear — we do not want a conflict that extends into space. We must be capable of fighting and winning if that conflict is to occur.



Space Systems Command (SSC) is the U.S. Space Force field command responsible for rapidly developing, acquiring, equipping, fielding and sustaining lethal and resilient space capabilities. SSC mission capability areas include launch acquisition and operations, communications and positioning, navigation and timing (PNT), space sensing, battle management command, control and communications (BMC3), and space domain awareness & combat power. SSC is headquartered at Los Angeles Air Force Base in El Segundo, California.

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

ONE YEAR AFTER THE RUSSIAN ASAT TEST

What has changed?

Author: David Todd, Head of Space Content for Seradata, a Slingshot Aerospace company

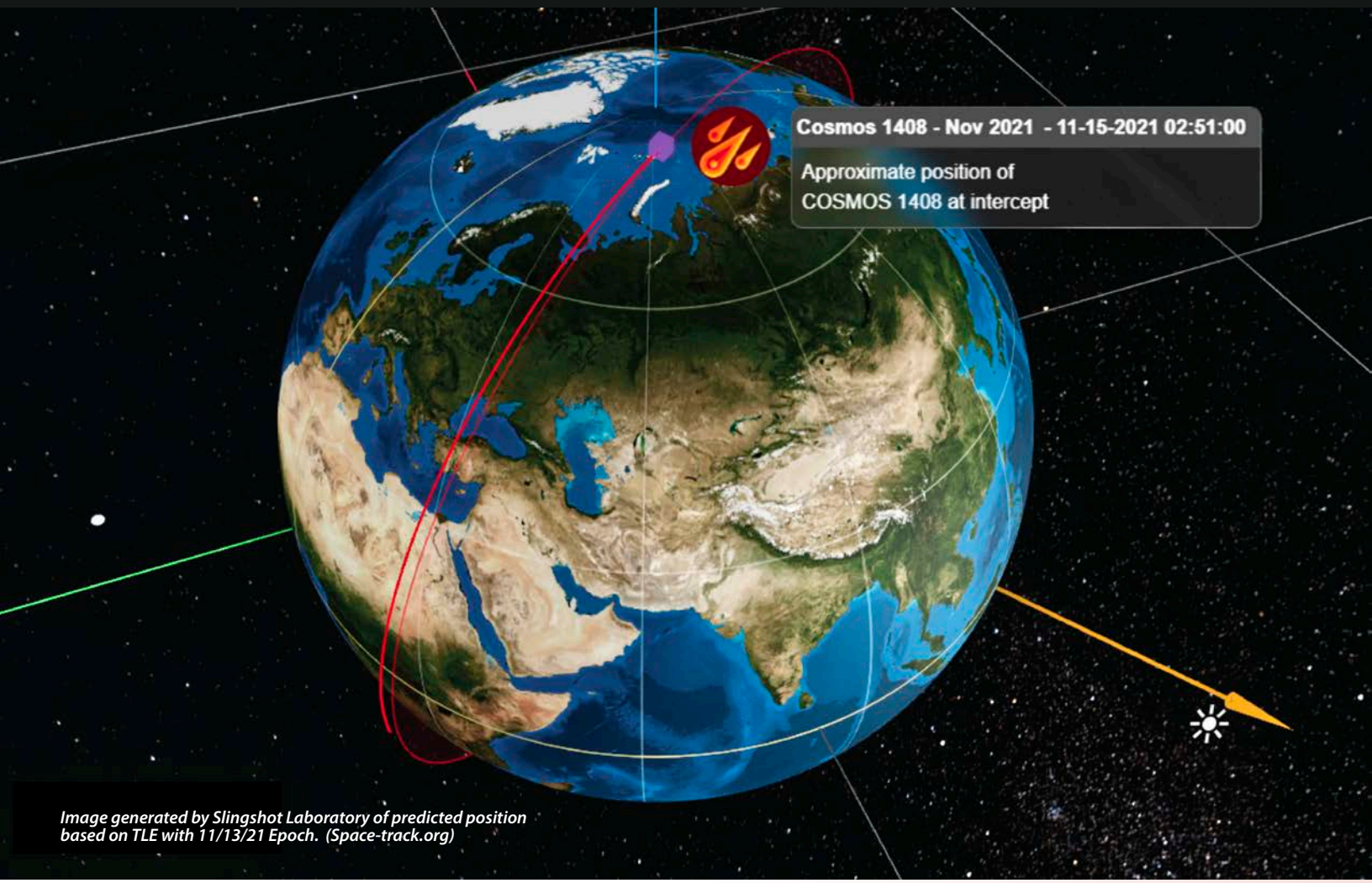


Image generated by Slingshot Laboratory of predicted position based on TLE with 11/13/21 Epoch. (Space-track.org)

A year has now passed since Seradata, a Slingshot Aerospace company, and Numerica Space (also now part of Slingshot Aerospace), broke the news to the world that Russia had destroyed one of their own satellites in Low Earth Orbit (LEO). What has happened since that destructive, anti-satellite (ASAT) test?

Around 0246 GMT on November 15, 2021, a Russian **A-235/PL-19 Nudol missile** (*photo to the right*) was launched from Plesetsk in Northern Russia. Approximately five minutes later, the missile intercepted a defunct Soviet-era satellite — **Cosmos 1408** — at an altitude of 470km, causing 1,789 pieces of tracked debris, some of which are likely to last for at least 15 years in orbit.

Cosmos 1408 was a 2,000kg., **Tselina-D** class, signals intelligence satellite that was launched in 1982 and which had been out of service for several decades. When the satellite was struck, it exploded, causing a "*debris cloud*" that threatened other spacecraft — including the ***International Space Station*** (**ISS**).

A-235/PL-19 Nudol missile launch. Courtesy: Russian Ministry of Defence via Globalsecurity.org

A few hours after that impact, the United States State Department confirmed that an ASAT test had taken place and that an alert had been sent to the American, German and Russian crew onboard the ISS.

This "*safe haven*" protocol alarm procedure was activated at 0900 GMT on the ISS. The seven crew members aboard were instructed to don their space suits, shelter in their spacecraft (***Crew Dragon Endurance*** and ***Soyuz MS-19***) and prepare for possible evacuation, should the ISS be struck. They remained in these shelters for approximately six hours before getting an all-clear to return to their normal activities.

It was the relative proximity of the orbits and the short warning that was of particular concern. The ISS's orbit was close enough to the debris field to potentially experience a conjunction threat every 93 minutes due to the wreckage that had been generated by the Russian ASAT test. (*See image above.*)

The creation of the respective debris cloud caused international protest. Then-NASA Administrator, ***Bill Nelson***, said, "*I'm outraged by this irresponsible and destabilizing action. With its long and storied history in human spaceflight, it is unthinkable that Russia would endanger not only the American and international*

partner astronauts on the ISS, but also their own cosmonauts. Their actions are reckless and dangerous, threatening, as well, [to] the Chinese space station and the taikonauts on board."

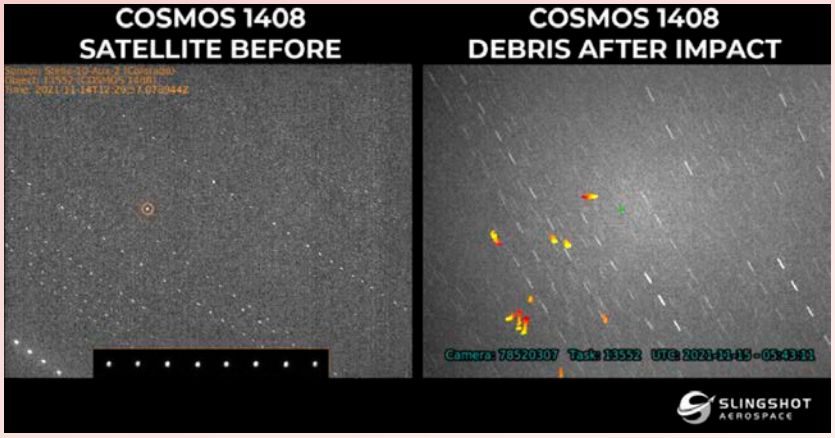
The initial emergency for the ISS crew was not the only one the crew members had to face. The ISS maneuvers infrequently, on average once a year, to avoid space debris. Since the ASAT in November of 2021, the ISS has had to maneuver multiple times to dodge the Cosmos 1408 debris.

On October 25, 2022, the docked ***Progress MS-20*** (**Progress 81P**) cargo spacecraft had to fire their thrusters for 5 minutes and 5 seconds in a ***Predetermined Debris Avoidance Maneuver*** (**PDAM**). This was to drive the spacecraft and the attached ISS complex an extra measure of distance away from the predicted track of a fragment of Cosmos 1408 debris.

In addition to the ISS, other spacecraft have had several close encounters with Cosmos debris. According to data from ***Slingshot Beacon***, the event has generated 2,587,750 ***conjunction data messages*** (**CDMs**), meaning there have been more than 2.5 million proximity alerts that operators have had to evaluate from this single, debris-generating event.

DEBRIS CLOUD REMAINS WITH US

According to ***Space-Track.org***, one month after the interception, 500 pieces of debris had been tracked, a total that later rose to nearly 1,800 pieces.
Based on the TLE data available at space-track.org, before impact and first available after impact days later, the main Cosmos 1408 body was likely impacted from behind as the resulting fragment's orbital energy was of a larger magnitude after the collision.



Although this data would suggest the relative velocity of the two objects at impact would be lower, this type of collision could be considered more perilous in the sense that the resulting debris would remain on-orbit for years and, potentially, more than a decade, due to the increase in orbital energy magnitude.

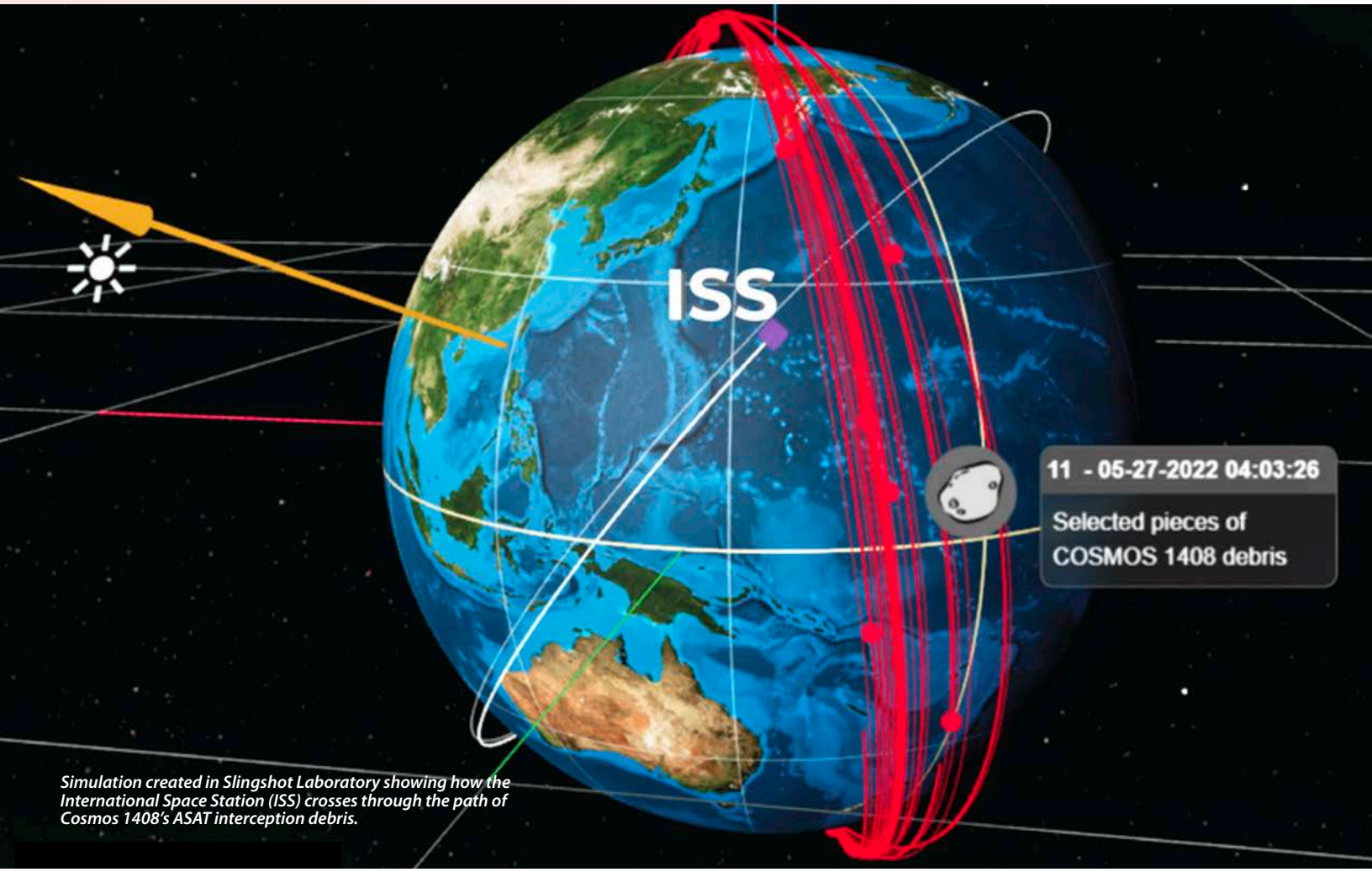
Additionally, the steeper geometry of the collision dispersed the resulting fragments — at higher velocities — in wider spread.

Whichever way the debris gets there, the concern remains that some orbits are now becoming increasingly populated with spacecraft — especially those used by the large satellite constellations — and any debris intersecting respective orbits of these constellations might, one day, result in a chain reaction of cascading debris formation, potentially causing the "***Kessler Syndrome***" theory that was posed by ***Donald Kessler*** in 1978.

As it is, with so much space junk and live satellites already in these orbits, adding more debris further aggravates the problem. Without a clear, global, space traffic coordination solution geared toward this level of scale (*such as Slingshot Beacon*), space sustainability faces a serious threat.

HOW SERADATA + SLINGSHOT DISCOVERED THE ASAT TEST

Slingshot received early news of the ASAT missile launch through the ***Slingshot Global Sensor Network*** that had been monitoring Cosmos 1408. The telescope system in Morocco detected the debris cloud within a few hours after impact. With this early detection, Slingshot was able to release the first images of the aftermath of the collision (*image above*).



Simulation created in Slingshot Laboratory showing how the International Space Station (ISS) crosses through the path of Cosmos 1408's ASAT interception debris.

The images revealed that the debris was rapidly moving away from a point of origin within a few hours of the impact. These first images also indicated

that some of the larger pieces were breaking apart in the process, creating even more debris.

Additionally, at the time, the space industry's leading launch and satellite database provider, Seradata (now a Slingshot Aerospace company) was involved in a **SACT** (***Sprint Advanced Concept Training***) exercise.

SACT was a method for the United States and its allies to technically assess commercial ***Space Domain Awareness*** (**SDA**) capabilities and does so via global exercises based on real and simulated space events. Real world events are included in the exercise and sometimes they can dominate, which was the case on November 15, 2021. Because of this exercise, Seradata was the first to break the news to the world via Twitter.

THE HISTORY OF DIRECT ASCENT ASAT MISSILE TESTS

ASAT missile tests have been carried out since the late 1950s. The first successful close pass was made by a **B-47 Stratojet**, air-launched, **Bold Orion/Altair missile** that attempted to intercept Explorer 6 on October 13, 1959.

A B- 47 aircraft with a Bold Orion missile in position. Photo is courtesy of the U.S.A.F.

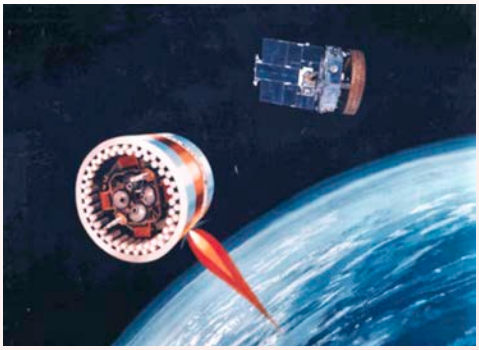
The realization was that, given the 6.4km pass distance, a nuclear warhead would have been required to reach the spacecraft and put it out of action. Exploding nuclear weapons in space to cause damage was explored as a secondary effect of Starfish Prime.

Photo of the Starfish Prime nuclear explosion in space as seen from Honolulu, Hawaii, 900 miles away.

On July 9, 1962, the United States Air Force detonated ***Starfish Prime,*** the highest space nuclear test ever conducted. The effects of the test created an artificial solar storm that included auroras, geomagnetic activity, and damaged electric systems as far as 800 miles away from the explosion. ***Six satellites*** were reportedly damaged.

Air-launched missiles gave way to other methods with the Soviet Union. In 1968, the Soviets began testing explosive "*killer satellite*" technology. The testing stopped when the ***Soviets declared the first official moratorium on ASAT testing***. Yet, two years later, in 1985 when the United States was preparing to launch their first ASAT, the Soviets "***considered themselves free***" to lift their two-year-old moratorium on ASAT weapons.

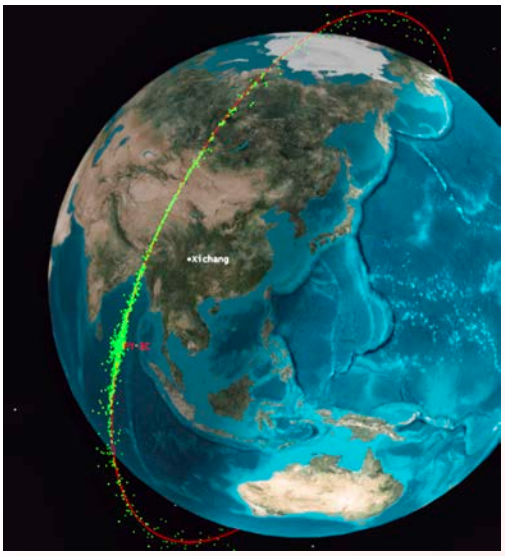
The return to air-launched ASATs happened with an **F-15A Eagle** fighter jet launch of the ***Vought ASM-135A missile***, which successfully intercepted **Solwind P78-1**, a U.S. gamma ray spectroscopy satellite, at an altitude of 530km on ***September 13, 1985*** (*images below*). Hundreds of pieces of tracked debris were detected, all of which quickly decayed.



Rather than an explosive warhead, the missile used an infrared, guided, direct interception technique controlled by a solid rocket thruster. While the test was successful, the United States turned away from ASATs and, instead, concentrated efforts on directed energy beam weaponry.

More recently, as inspection and service satellite technology have matured, China has been developing satellites not to service and repair spacecraft, but to conduct ***remote operations*** to physically attach to and manipulate other satellites.

China decided that it needed to demonstrate a direct interception capability of its own. On January 11. 2007, China used a ground-launched SC-19 missile as an interceptor to strike the Chinese ***Fengyun-1C weather spacecraft at an altitude of 863km***.



Artistic rendition of the Chinese ASAT test impact 5 minutes after the impact.
Kelso, TS, "Chinese ASAT Test", Celestrak.com, www.celestrak.com/events/asat.asp

The resulting debris was found to have more than 3,000 tracked pieces, the majority of which still remains in orbit. The debris cloud triggered international protest over the test. Apart from the space debris risk, the military implication was that any satellites flying in a ***sun-synchronous orbit*** (**SSO**) — as most reconnaissance satellites do — were now at risk of missile strike.

On February 20, 2008, as part of ***Operation Burnt Frost***, a **United States Navy Standard Missile-3** (**t**) missile was fired from the USS Lake Erie. The mission was quickly designed to destroy a non-operational, orbitally decaying, ***United States National Reconnaissance Office*** (**NRO**) satellite, ***USA-193***, to stop its stainless-steel tank of hydrazine fuel from surviving re-entry, which was a threat to human life.

The SM-3 missile intercepted the satellite USA-193 at 220km altitude, causing it to break up. It was known from the start that the debris would re-enter and burn up within a short time period and would not create a lingering debris field.

Images showing explosive SM-3 "Burnt Frost" interception of the USA-193 satellite. Courtesy of the Missile Defence Agency (MDA).

The final piece of detectable USA-193 debris re-entered on October 28, 2009.

India performed that nation's first ASAT missile test on March 27, 2019, when a used **PDV-Mk 2** missile destroyed an Indian ***Microsat-R*** satellite on-orbit at an altitude of 285km — that impact resulted in 400 pieces of tracked debris. All have now re-entered.

As previously discussed, Russia returned to ASAT missile technology on November 15, 2021, when a Nudol missile struck the Cosmos 1408 spacecraft at

Date	Country	ASAT System	Target	Intercept Alt (km)	Target Launch Mass (kg)	Tracked Debris	Debris still in orbit	Total Debris Lifespan (Years)
13 Sep 1985	US	ASM-135A	Solwind P78-1	530	850	285	0	18+
11 Jan 2007	China	SC-19	Fengyun 1C	863	958	3547	2812	15+ est
20 Feb 2008	US	SM-3	USA 193	220	2275	174	0	1+
27 Mar 2019	India	PDV-Mk II	Microsat-R	385	744	400	0	2+
15 Nov 2021	Russia	A-235/PL-19 Nudol	Cosmos 1408	470	2,000	1789	439	15+ est

Table 1: Five successful ASAT missile test interceptions to date. Sources: Secure World Alliance/NASA/Seradata SpaceTrak/Space-Track.Org as of November 10, 2022.

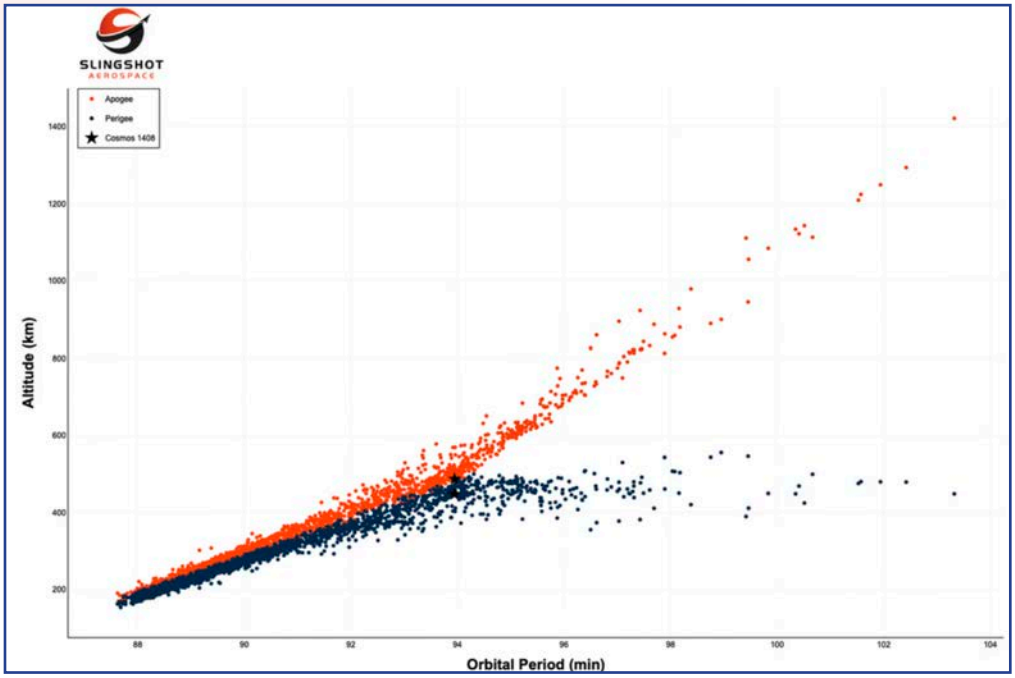
an altitude of 470km, causing 1,789 pieces of tracked debris, some of which are likely to last for at least 15 years in orbit.

WHERE IS THE RUSSIAN ASAT TEST DEBRIS TODAY?

As of October 23, 2022, there were 1,789 pieces of tracked debris from the Russian ASAT interception of Cosmos 1408, of which 439 pieces are still on-orbit (November 10, 2022).

The Gabbard diagram (*shown below*), which shows the apogee and perigee of Cosmos 1408 and the resulting debris, indicates that the apogees of some parts were boosted all the way up to 700km, with one piece close to 800km. Some pieces were sent downwards, with perigees now significantly below the interception altitude of 470km — some debris were close enough to present a potential, conjunction threat to the ISS.

Space object decay prediction is an inexact science with several variables, not the least of which are the solar weather effect on the thickness of the Earth's atmosphere. Nevertheless, a rough assessment is possible, using data from the earlier ASM-135A test at a similar altitude. We can, therefore, predict that debris from the Russian test is expected to last on-orbit for approximately 15-20 years.



Sources: Secure World Alliance/NASA/Seradata SpaceTrak/Space-Track.Org as of November 10, 2022

PUTTING AN END TO ASAT TESTS

As it stands, only four nations have demonstrated a direct ascent ASAT capability: China, India, the United States and Russia.

While the environment surrounding the use of these weapons has many unknowns, it stands to reason that their use, if carried out against a spacecraft from another country, would have a high likelihood of being regarded as a Casus Belli "*act of war*" by the receiving party.

As of an announcement in April of 2022, the United States has committed to not conduct destructive, direct-ascent anti-satellite (ASAT) missile testing and has called on other nations to do the same.

Several other countries have made similar commitments including **Canada**, **New Zealand**, **Germany**, the **United Kingdom**, **Japan**, **Australia**, **South Korea**, and **Switzerland**.

Furthermore, the United Nations is concerned about ASAT testing and is moving toward establishing a new set of rules and norms for responsible behavior in space.

In the Fall of 2022 the ***U.N. First Committee*** voted on a resolution from the United States to forgo the testing of destructive, debris-creating anti-satellite weapons — 154 countries voted in favor of the resolution, with 10 abstaining and eight opposing, including permanent Security Council Members, China and Russia.

While this is not a legally binding commitment, it is a strong indication of the global interest in restricting the use of such weapons, as well as the work yet to be done to gain international consensus on this topic.

WORKING TOGETHER TO KEEP SPACE SAFE

Creating more space debris is not in any nation's best interest as a chain reaction of conflict could quickly render the space domain unusable for humankind. We must push to accelerate work already underway at both international organizations and the national level to ensure a global ban on destructive, debris-causing, ASAT tests.

We must also increase accountability for safe space operations in the orbital environment. Initiatives such as the ***Space Sustainability Rating*** are taking the global community in the right direction by challenging space operators to be held to the highest standards of stewardship, but there is still much more to be done.

Today, the highly skilled team at Slingshot Aerospace is developing and deploying cutting edge technologies like ***Slingshot Beacon***, ***Slingshot Digital Space Twin***™ and the S***lingshot Global Sensor Network***.

These products provide space operators with actionable insights and complete data, so that when faced with the consequences of dangerous or reckless behavior on orbit, such as ASAT tests, they're able to rapidly and confidently make critical decisions to ensure safety of their operations and of the space operating domain as a whole.

ASAT tests, and the debris they create, are not just a threat to a single satellite — they are a threat to humanity's future.

At Slingshot Aerospace, we are steadfast in our commitment to accelerating space sustainability and will continue to strongly denounce ASAT tests and other behaviors that endanger the sustainability of our planet and the orbits we all depend on.

slingshotaerospace.com

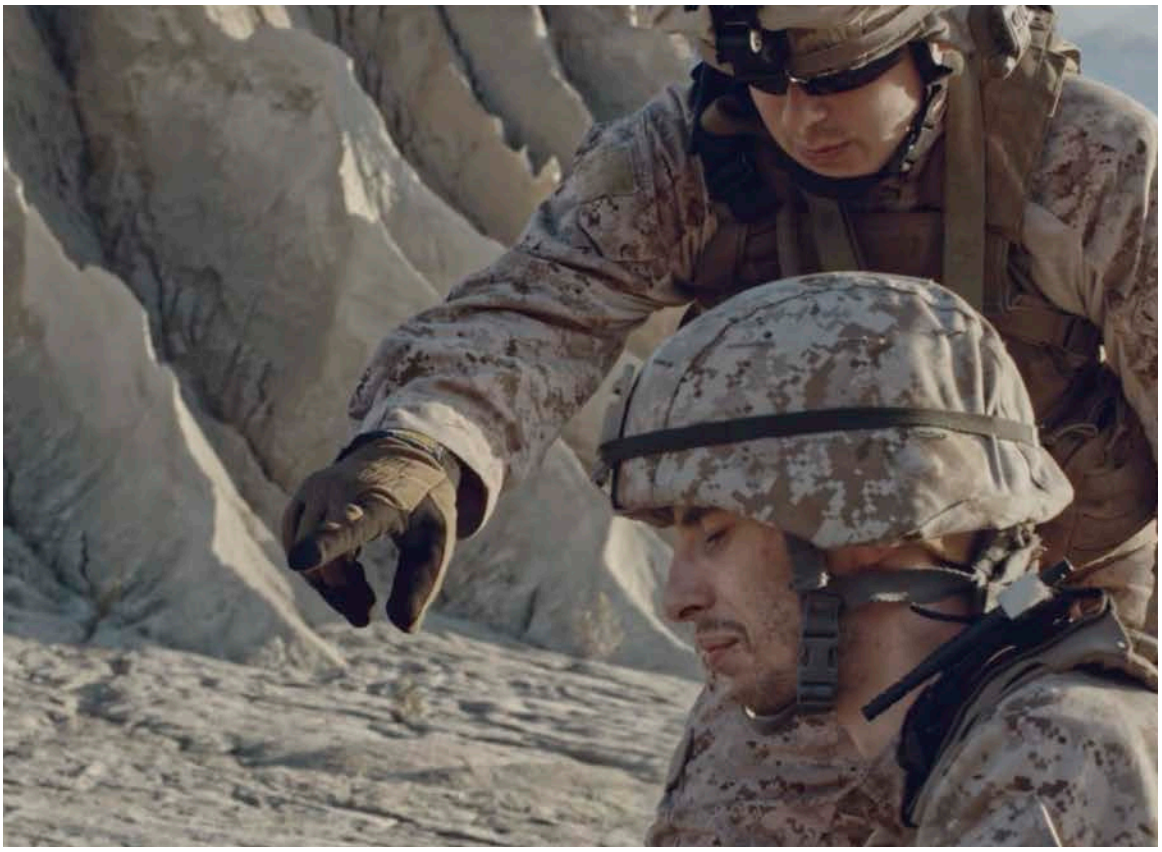
SLINGSHOT AEROSPACE

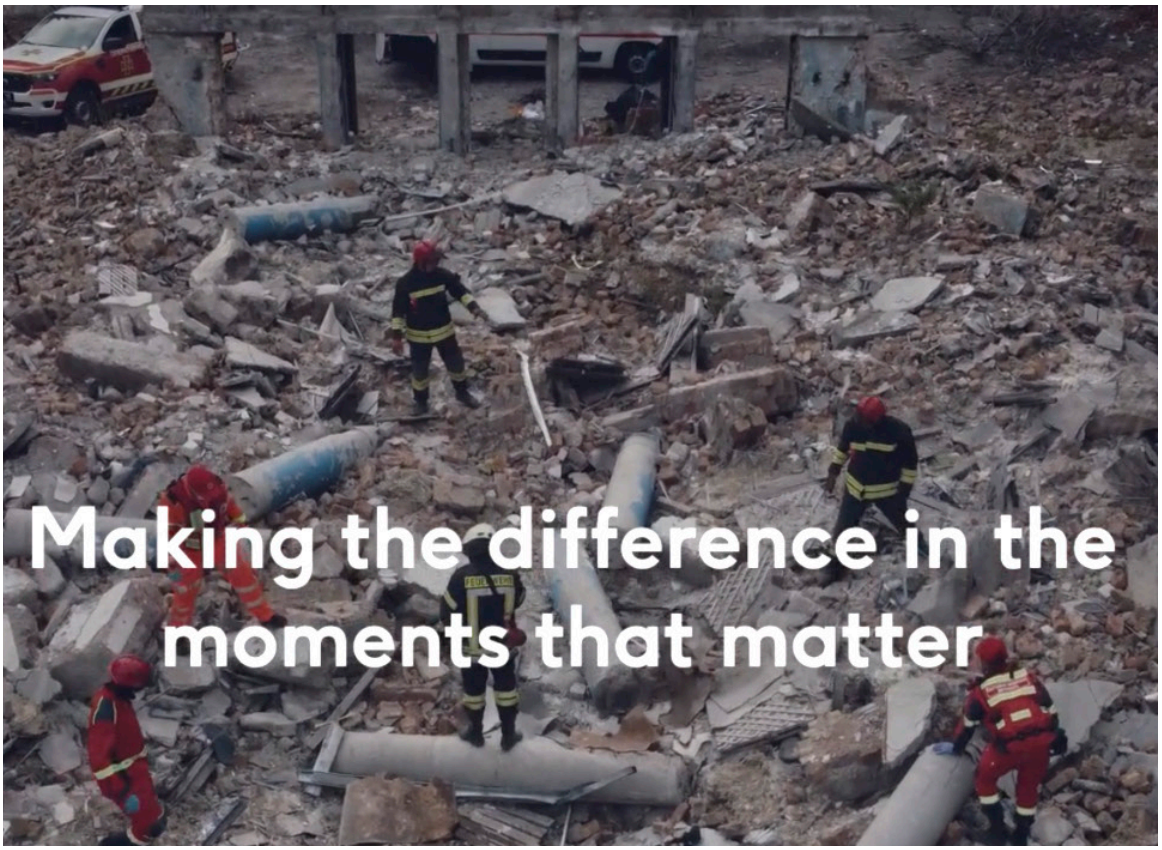
David is Head of Space Content for Seradata, a Slingshot Aerospace company, with overall responsibility for the SpaceTrak launch and satellite database. He is also Editor of Seradata's news service, Seradata Space Intelligence. David has been a space analyst and consultant working on the ***SpaceTrak*** *database since 1997 when he acted as the editor for the launch of the original version, then produced by Airclaims.*

YEAR IN REVIEW
ALL.SPACE

The initial production of the world's first multi-network, multi-orbit platform

Author: Brian Billman, Chief Marketing Officer





2022 will be remembered by many as the year ubiquitous connectivity across multiple networks was made possible with a single, smart terminal, marking the start of a new era of ground system technology developed and proven by ALL.SPACE.

Until now, satellite systems were closed off, often proprietary, and unable to communicate with other satellite, cellular or terrestrial networks.

Our mission to converge advanced communications over multiple networks and operators over one terminal began about nine years ago and led us to breakthrough discoveries in the new field of transformational optics.

This year, ALL.SPACE developed the world's first and only smart terminal, a software-defined platform that is capable of connecting across networks via multiple, simultaneous, full-performance links that converges satellite and cellular network access, intelligent routing, edge computing and specialized modems into a single, integrated solution.

The smart terminal's unique ability to connect satellite operators across orbits and cellular operators across all available networks creates the world's most convergent communications platform.

A YEAR OF HISTORIC FIRSTS

Over the past 12 months, ALL.SPACE successfully completed a series of historic, first-of-their-kind, multi-orbit terminal trials, focused on meeting specific communications requirements for commercial, government and defense markets.

At the start of the year, together with ***SES Government Solutions***, ALL.SPACE demonstrated the smart terminal's multi-link capabilities to meet the rigorous conditions and challenging connectivity demands of U.S. and NATO Forces during GEO and MEO resiliency tests at the U.S. Army proving grounds in Aberdeen, Maryland.

During the spring, ALL.SPACE successfully completed field tests with ***Telesat*** showcasing the smart terminal's ability to link with satellites in LEO and GEO orbits, proving the platform's world-first, all-orbit capability.

The growing ALL.SPACE team has constantly refined and extended the capabilities of the terminal, improving the performance, enhancing software-defined capabilities, and increasing the ruggedness of the smart terminal to ensure it delivers the needed connectivity in the moments that matter.

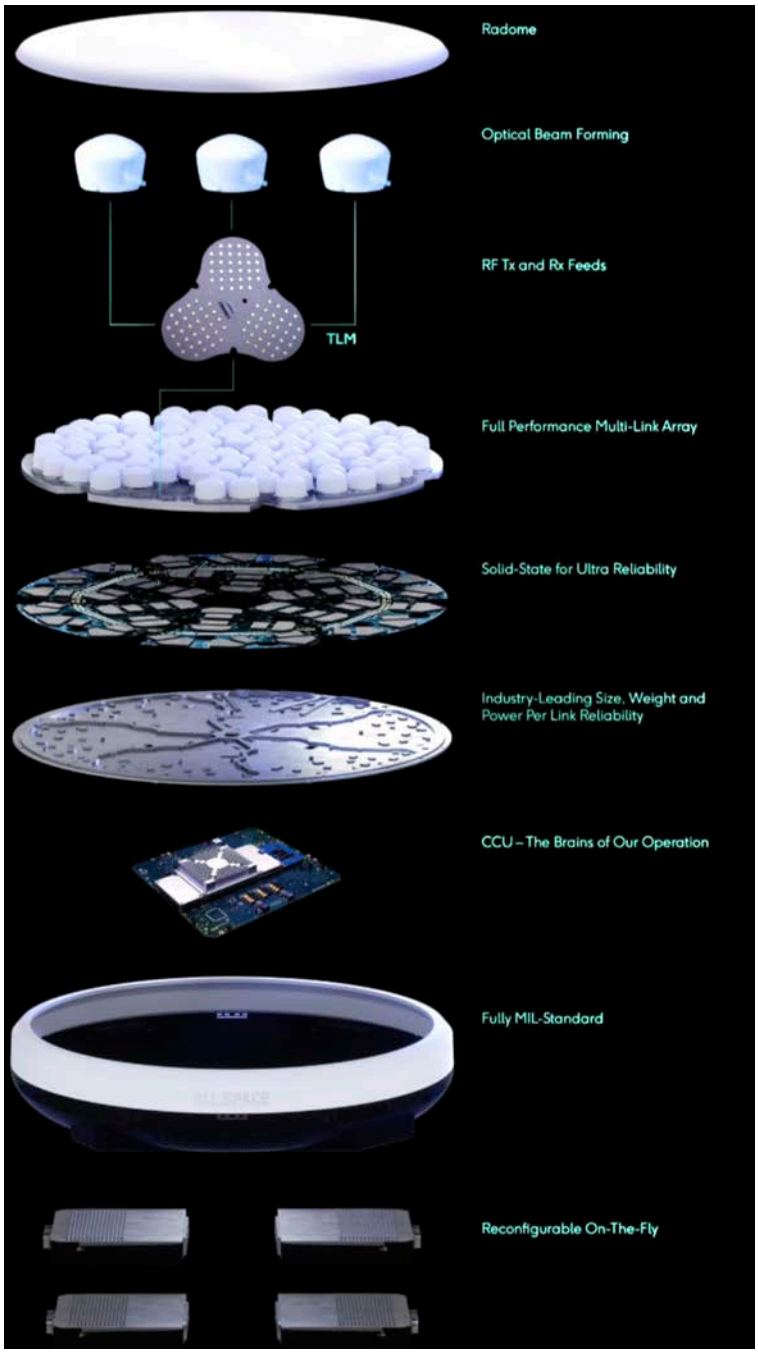
The company is currently working with the ***U.S. Department of Defense*** to fully qualify our terminal for their use, proving the breakthrough platform with an eye on our upcoming product rollout.

Our commercial and government customers will ultimately leverage the terminal to unleash the full potential of their existing and advanced satellites, constellations, and cellular networks to support a new age of connectivity across a broad range of vertical markets over the coming months and years.

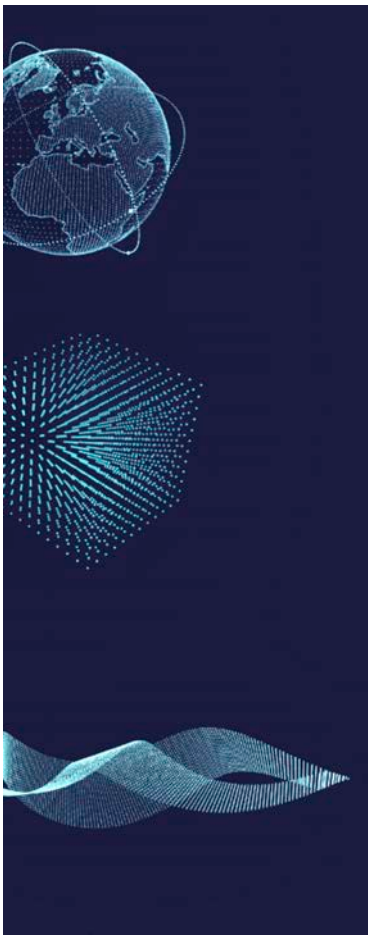
REDEFINING CONNECTIVITY

2022 has witnessed a flurry of satellite launches into ***non-geosynchronous orbit*** (**NGSO**), as well as new deals and partnerships between the traditional satellite operators and new LEO operators.

These multi-orbit strategies are aimed at driving more efficient and resilient networks in space, leveraging the different LEO, MEO and GEO resources to take advantage of each platform's best attributes. all the while creating a new network greater than the sum of its parts.



The ALL.SPACE smart terminal is the key element missing from this critical equation, the missing piece of the network that makes a new age of convergence possible.



Over the last few years, there has been increased focus on the new, highly advanced satellites and constellations headed for space.

During this time we have been laser focused on the development of a modern ground system capable of aggregating these systems and networks for an unprecedented connected experience everywhere.

This is the year our strategic vision played out with the first smart terminals being readied to ship to government and commercial customers across the globe.

We are excited to see what new and unimaginable applications our multi-network, multi-orbit platform empowers in the next year and for years to come.

www.all.space

ALL.SPACE

Brian Billman

YEAR IN REVIEW
COMTECH SATELLITE NETWORK TECHNOLOGIES

Comtech delivers game-changing battle ground infrastructure amid a year of rising near-peer threats

Author: Daniel Gizinski, President of Comtech Satellite Network Technologies Inc.

With an array of near-peer threats reaching Cold War levels, the US and allied global communications requirements have quickly shifted to ground-sector advancements where Comtech excels. Comtech has designed and delivered software-defined gateway and portable modems into the defense market for more than a decade, offering software-only upgrades to fielded in-use hardware to instantly bridge the gap between old standards and new JADC2-level capabilities.

It has been a game-changer for our in-theater forces. In 2022, Comtech unveiled breakthrough systems that have had an immediate impact on the battlespace.

A YEAR OF COMTECH DEFENSE INNOVATIONS

Comtech introduced groundbreaking, military-grade, communications solutions for the defense market this year — all key to the Department of Defense modernization program.

Comtech's new ***CDM-780 Gateway modem*** is the latest and most powerful in a long line of backbone modems, now capable of managing unprecedented amounts of data delivered over new and complex wideband GEO, MEO and LEO satellites and constellations. (***See Figure 1 on the following page.***)

Our new ***SLM-5650C2*** portable software-defined modem can be carried and operated in manpacks, enabling multi-orbit, on-the-fly comms capabilities on the frontline for a real competitive edge. (***See Figure 2 on the following page.***)

Comtech is dedicated to bringing high-speed broadband to the fingertips of warfighters with our growing lineup of integrated, end-to-end communications platforms and solutions.

In 2022, Comtech not only introduced new technologies, we also enabled third-party manufacturers and service providers to implement and integrate some of our intellectual property and communications waveforms into non-Comtech hardware solutions.

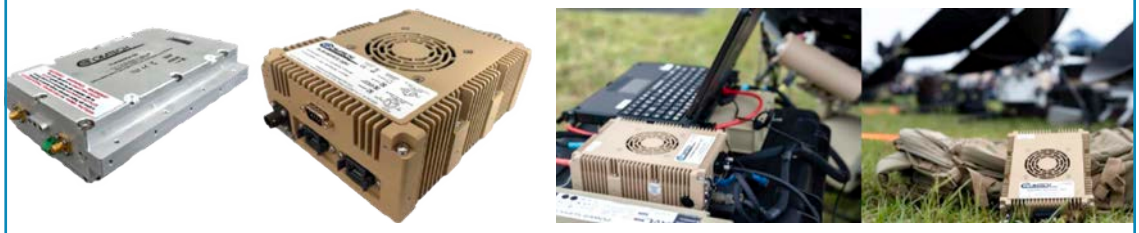
This will help ensure users have access to existing infrastructure across a range of platforms and locations.

PRIDE-DRIVEN TECHNOLOGIES

One of the things I'm most proud of in 2022 is our ability to deliver solutions based on our customers' problem sets rather than a defined path to addressing requirements.

We've been able to deliver advanced satellite communications capabilities, resilient troposcatter networks, and supporting equipment, based on real challenges and issues our customers are experiencing with their gear in the field.

CDM-780 Gateway modem



SLM-5650C2 portable software-defined modem

Our defense customers have stated both privately and publicly this year that our products have proven to provide reliable communications in contested theaters where other offerings simply could not. That's what it's all about — enabling a communications lifeline when lives are on the line.

When our team hears directly from defense customers about how much they trust and rely on Comtech products, there's a strong sense of pride across the company that we're playing a role in defending U.S. and Allied interests around the world.

This really all starts with our ability to listen to and meet customer challenges, as we roll up our sleeves and meet with our end users on the technology proving grounds during tech and solution demos in the field.

In the early stages of the Russian invasion in Ukraine, Comtech donated several small form factor troposcatter systems and upgrade kits for fielded gear in the region.

The ability to understand the challenges and move fast to support them and enable comms in a denied environment is critical. And as a result of our work in Ukraine, we have seen demand for and are filling dozens of follow-on system orders via foreign military sales channels.

We are also proud of our longstanding dedication to manufacturing defense products in the U.S., making Comtech a strong source for military products and innovation.

We are on the verge of a major 150,000 square foot expansion of our manufacturing and engineering center of excellence in Chandler, Arizona, as we build on our mission to connect commanders and every U.S. and allied warfighter across the battlespace with fast, resilient communications capabilities around the world.

www.comtech.com

Daniel Gizinski was named President of Comtech Satellite Networks Technologies, Inc. (a U.S. Corporation) on January 3, 2022. Previously, he held various senior management positions at Comtech, including Vice President of Product and Strategy for Comtech Systems Inc. Prior to joining Comtech in 2019, Daniel held program management and leadership roles at General Electric, Sierra Nevada Corporation and L3Harris Technologies. Daniel holds a Bachelor's degree in Electrical Engineering from the University of Virginia and a Master's degree from Duke University.

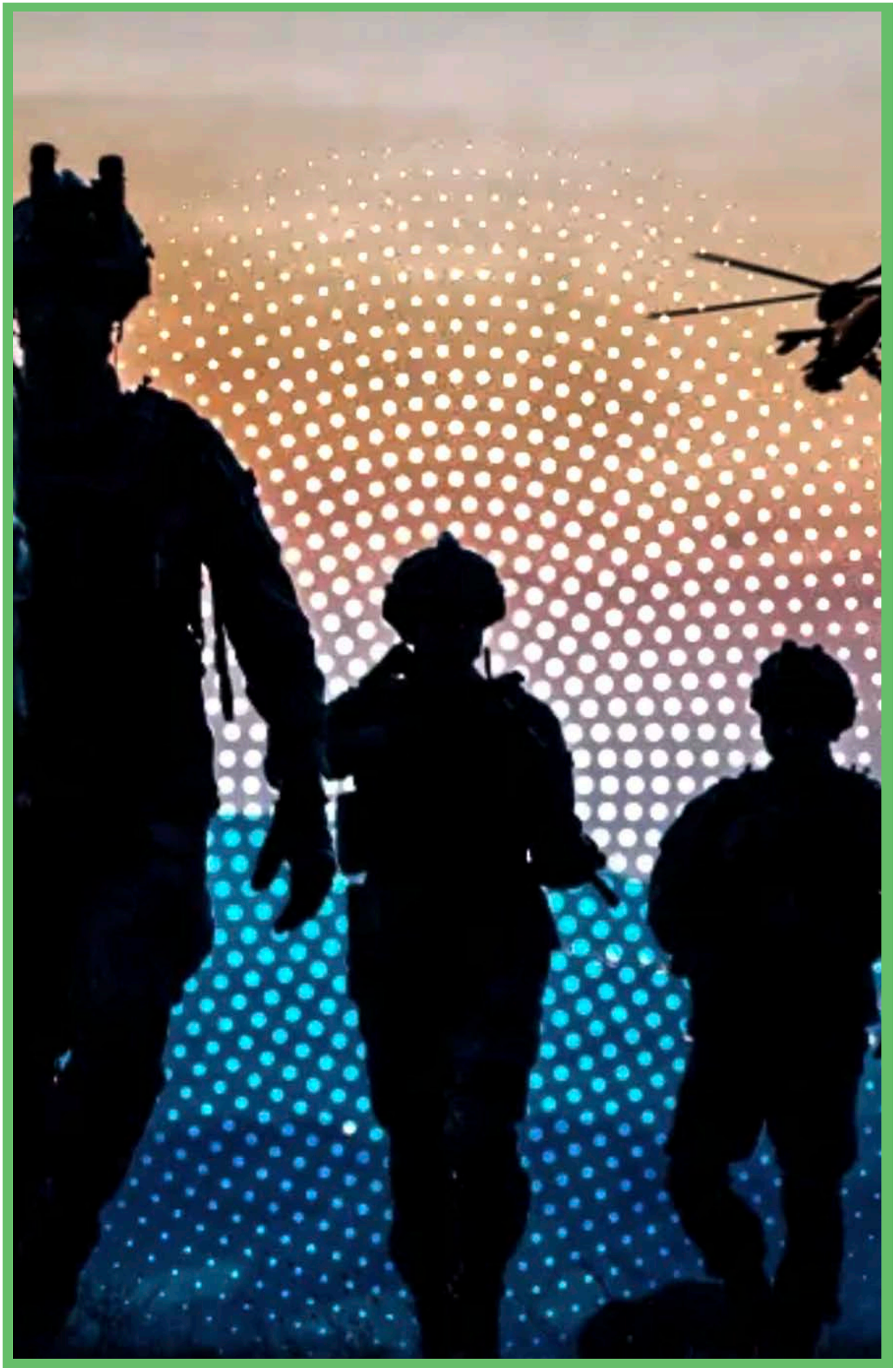
Daniel Gizinski

YEAR IN REVIEW
INTELSAT GENERAL

Keeping warfighters connected

Author: Dave Micha, President, Intelsat General Communications

Intelsat is the largest provider of commercial satellite communications to the U.S. government, and our role is to deliver mission-critical communications services that empower our customers' success.



We are collaborating with partners and key industry players to build the next-generation unified network infrastructure needed to deliver resilient multi-layered connectivity everywhere.

Years in the making, and now with broader adoption of open standards, Intelsat's satellite connectivity has advanced to a new level.

Intelsat General is more than ready to deliver reliable broadband for more sophisticated **C5ISR** (***Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, & Reconnaissance***), innovative warfighter applications, and all-domain communications.

This comms technology enables and supports government and military communications in contested and remote locations.

Intelsat has shifted toward a multi-layered approach to connectivity — migrating away from solely relying on ***geostationary*** (**GEO**) satellite-based communication, which adds the benefits of ***Low Earth Orbit*** (**LEO**) connectivity to our reliable connectivity solutions.

Our ***software-defined satellites*** (**SDS**) will be the core of the future, next-generation ***Unified Network*** we are creating.

SDS's advantages include *fast reconfiguration*, *enhanced capabilities*, *dynamic bandwidth allocation*, *"follow-me" beams*, *automatic frequency switching*, *tailored geographic coverage*, and *asset awareness/tracking* across aligned operations.

Intelsat and our partner ***OneWeb*** have already demonstrated to the **U.S. Department of Defense**, fiber-like connectivity with transport layer diversification between GEO and LEO constellations that will be crucial in delivering uninterrupted mission-critical broadband connectivity for global armed forces.

The company is well-positioned to meet the dynamic needs of today's military missions through its next-generation Unified Network — which will be a step-change transformation in the delivery of satellite connectivity.

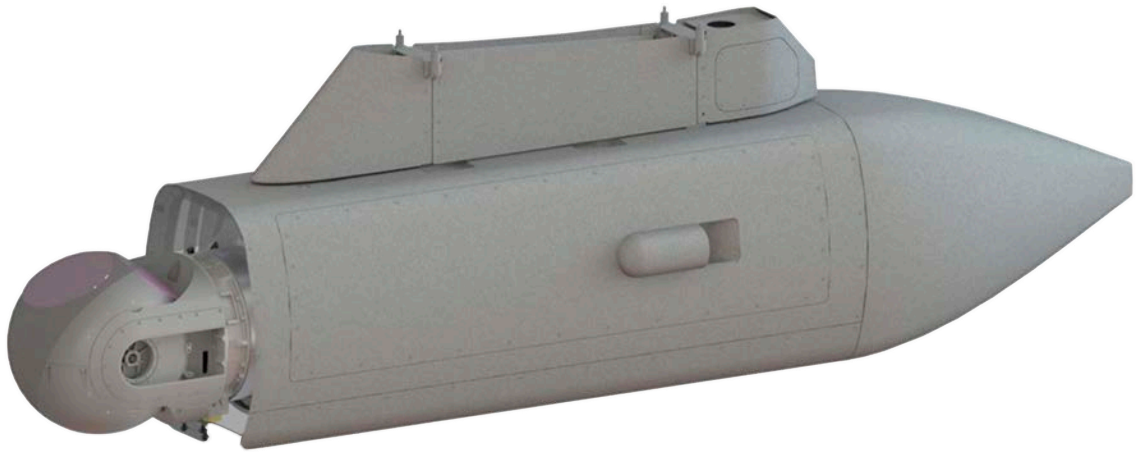
www.intelsat.com/solutions/government/

INTELSAT General

GA-ASI DEMOS NETWORK RELAY USING LASER COMMS

General Atomics Aeronautical Systems ***(GA-ASI) completed a fully-networked demonstration using multiple Laser Communication (lasercomm) terminals.***

The network included ground, mobile and airborne terminals. During the demonstration, a live video and audio feed of operators at each terminal was shared in the networked communication display.



Airborne Laser Communications System (ALCoS)

Lasercomm is in demand for military applications because of its inherent ***Low Probability of Intercept/Low Probability of Detection*** (**LPI/LPD**) and anti-jam characteristics, as ell as the ability to support much higher data rates (*greater than 1 Gigabit per second*) than traditional ***Radio Frequency*** (**RF**) systems.

The demonstration occurred at ***Naval Information Warfare Center*** (**NIWC**) ***Atlantic*** located in Charleston, South Carolina, in November of 2022, as part of a GA-ASI-funded test to highlight extended multi-point networking communications using lasercomm.

During the demonstration, which was facilitated by organizers of NIWC Atlantic's optical communications-focused ***Advanced Naval Technology Exercise*** (**ANTX**), the team maintained lasercomm links at 1 ***Gigabit per second*** (**Gbps**) and exchanged high quality video and voice data.

GA-ASI has developed a family of optical communication capabilities and is poised to play an important role in transitioning these capabilities to users in a variety of domains, from air to sea. Laser communications will enable GA-ASI's ***Remotely Piloted Aircraft*** (**RPA**) to perform secure, multi-domain communications to airborne, maritime, and ground users, as well as with future satellites.

This capability can be applied as a podded or fully integrated solution to GA-ASI's full line of unmanned aircraft, including ***MQ-9B SkyGuardian***®/***SeaGuardian***®, ***MQ-9A Reaper*** and ***MQ-1C Gray Eagle 25M***.

"*This fully networked lasercomm demonstration is a major milestone for GA-ASI and a significant achievement for the lasercomm community as it featured the extended use of this technology beyond point-to-point communications*," said GA-ASI Vice President of Mission Payloads and Exploitation, ***Satish Krishnan***. "*The successful execution of this demonstration shows how lasercomm can be utilized in an operational theater to truly provide LPI/LPD high-capacity comms for the warfighter.*"

www.ga-asi.com

General Atomics Aeronautical Systems, Inc. (GA-ASI), an affiliate of General Atomics, is a leading designer and manufacturer of proven, reliable Remotely Piloted Aircraft (RPA) systems, radars, and electro-optic and related mission systems, including the Predator® RPA series and the Lynx® Multi-mode Radar. With more than seven million flight hours, GA-ASI provides long-endurance, mission-capable aircraft with integrated sensor and data link systems required to deliver persistent flight that enables situational awareness and rapid strike. The company also produces a variety of ground control stations and sensor control/image analysis software, offers pilot training and support services, and develops meta-material antennas. For more information, visit www.ga-asi.com

YEAR IN REVIEW
KRATOS

Kratos receives multiple awards to bolster military space initiatives

Author: Chris Badgett, Vice President of Technology, Kratos Space

MAINTAINING DECISION SUPERIORITY

This year, Kratos became a partner recipient on awards for two separate advanced, strategic, government programs.

These programs will incorporate ***Kratos' OpenSpace Platform***, a software-defined, satellite ground system. In the past, standing up new satellite services commonly required weeks or even months using traditional hardware-based ground systems.

This platform enables warfighters to instantiate new services in minutes. OpenSpace was designed to be interoperable across domains, with enhanced resilience and flexibility, assuring communications access and the ability to maintain decision superiority.

SATCOM MODERNIZATION

Kratos was also awarded a ***U.S. Army Futures Command*** contract to demonstrate SATCOM modernization capabilities enabling the government to field SATCOM networks. This modernization effort will be powered by Kratos' OpenSpace platform and includes streamlining gateway and remote terminal capabilities supported by multiple vendors, reducing life-cycle costs and supporting adaptive, dynamic space operations.

Today's hardware-based networks cannot deliver the speed, interoperability or agility to meet these goals, whereas a standards-based architecture that is layered and extensible and software-defined, such as OpenSpace, can drive digital transformation and SATCOM modernization efforts.

SPACE DOMAIN AWARENESS

Kratos presented new ***Space Domain Awareness*** (**SDA**) services at the ***Advanced Maui Optical and Space Surveillance Technologies*** (**AMOS**) ***Conference*** that are now available to the military and commercial markets.

In today's contested and congested environment, a complete operational picture of space domain awareness is critical.

Kratos is the only company to offer SDA services integrated across the orbital, link, and terrestrial segments to support the commercial, civil, and defense markets.

Powered by sites collecting and analyzing data from 140+ sensors at over 20 global locations , Kratos' services offer critical insights that augment today's traditional resources and tools for understanding and responding to emerging on-orbit threats.

www.kratosdefense.com

KRATOS
READY FOR WHAT'S NEXT

Chris Badgett is vice president of technology for Kratos Space. Prior to Kratos, Mr. Badgett served in the U.S. Air Force as a weapons engineer in the Air Force Research Lab. Mr. Badgett holds a BS in Electrical Engineering from University of Tennessee and an MS in Space Systems from the Air Force Institute of Technology.

SatNews

CONNECTIONS ON EARTH FOR CONNECTIONS IN SPACE

JOIN US ONLINE!

Free subscriptions and access
Timely news and editorials
Complete archives

satnews.com/reg

SatMagazine | MilsatMagazine | SatNews.com