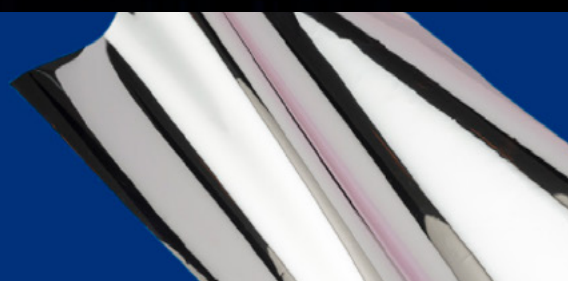
Next Generation Space Defense

MILSATMAGAZINE

June 2024

Cover image is courtesy of ***Advantech Wireless***



Publishing Operations & Issue Contributors

Silvano Payne
Publisher + Author

Simon Payne
Vice President

Hartley G. Lesser
Editorial Director + Author

Pattie Lesser
Executive Editor + Author

Donald McGee
Production Manager

Teresa Sanderson
Operations Director

Sean Payne
Business
Development Mgr.

Dan Makinster
Technical Advisor

Curt Blake
Senior Columnist

Chris Forrester
Senior Columnist

Karl Fuchs
Senior Columnist

Rick Lober
Senior Columnist

Contributors

Karl Fuchs

Nimrod Kapon

Christian Rex-Nielsn

Lisa Sodders

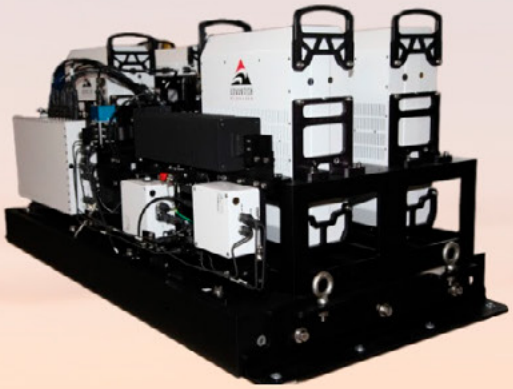
Issue Contents

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 © 2023 SatNews Publishers

ADVANTECH
WIRELESS
A Baylin Technologies Company



OLYMPUS LINE HIGH-POWER SOLID-STATE POWER AMPLIFIER SYSTEMS

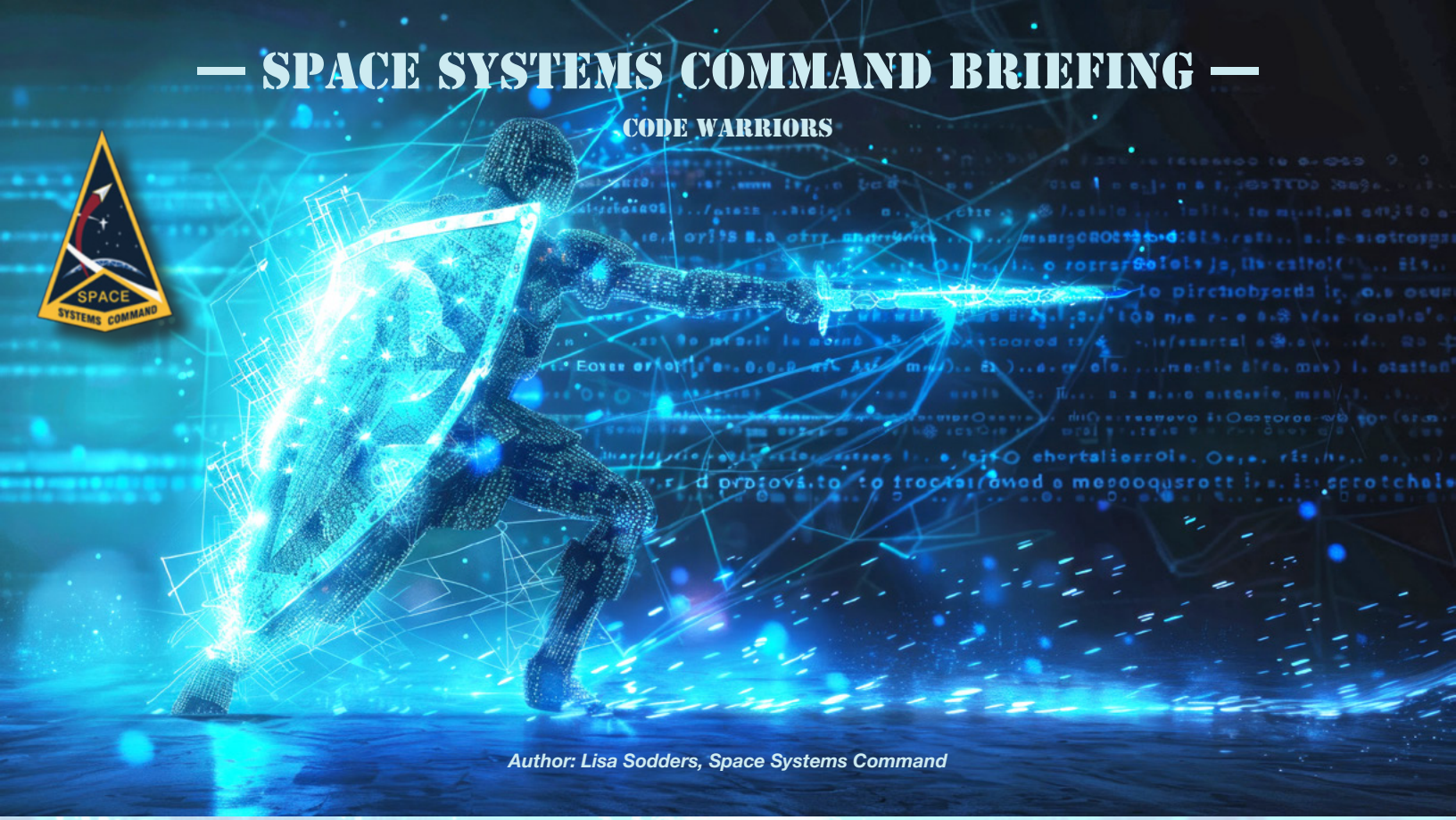
- Delivered as factory-integrated and tested systems up to 1.8kW
- C, X, Ku, and S-Band
- With or without integrated L-band converters
- Full M&C capability
- Weatherproof construction
- CE marking

HIGH POWER SOLID STATE AMPLIFIERS AND SYSTEMS

- 50W to 16kW of transmit power in L/S, C, Low X, Std. X and Ku-Bands
- Communications and Ranging
- Antenna-Pad, Work-Platform, and Side-Arm Mounting Configurations
- Gateway Earth Stations, Deep Space, DTH, Satellite Tracking

— SPACE SYSTEMS COMMAND BRIEFING —

CODE WARRIORS



Author: Lisa Sodders, Space Systems Command

Blinky Lights, Layer 8, and Staff Retention: Space Systems Command's Chief Information Officer reflects on cybersecurity challenges and opportunities in this era of Great Power Competition

Just as the U.S. Space Force continues to evolve as the United States' newest military service, so does Space System Command's approach to IT and cybersecurity. The fact that the office is designated as Chief Information Office (CIO) and not S6 — the military designation for communications/IT — indicates just how critical cyber security is to the USSF.

Near-peer competitors and other potential adversaries are relentlessly conducting malicious cyber activity across all sectors of the United States' infrastructure, exploiting valuable data systems during competition, and have demonstrated the ability to deny, disrupt, degrade, destroy, or manipulate vital information and networks during conflict, according to USSF *Gen. B. Chance Saltzman*, Chief of Space Operations, in USSF's Cyber Strategy.

> *Col. Craig Frank, Director of Space Systems Command's CIO office, explains, "From my point of view, a CIO has the ability to create and enforce policy, where an S6 is more at the unit level and enacting that policy."*

For the CIO-level functions, Frank and his team provide cyber oversight and support to SSC's *Program Executive Officers* (**PEOs**) who oversee space capability development and delivery.

> *"On the S6 side, we're really concerned with the care and feeding of the IT side for the command and all the downtrace units. We actually support the three installations (Los Angeles Air Force Base, Vandenberg Space Force Base, and Patrick Space Force Base) with their IT infrastructure," Frank said.*

Whether CIO or S6, Frank said his three top priorities are: making certain SSC data and workstations are secure but still function at the speed of the fight; maximizing partnerships with space industry and academia; and workforce development and retention.

Col. Craig Frank, Director, Space Systems Command's Chief Information Office, spoke at the recent Space Symposium in Colorado Springs, Colorado.

Col. Craig Frank talks to attendees at the 39th Annual Space Symposium in Colorado Springs, Colorado, in April of 2024.

"What keeps me up at night is not SIPRNET (a highly secure network used to transfer classified information), JWICS (Joint Worldwide Intelligence Communications System, another secured network), or sat networks where someone walks in with a pop music CD and walks out with a bunch of classified documents, and the tens of thousands of unclassified, unencrypted laptops out in the witheld, sometimes sitting in the back of a car and getting stolen – and the ability of the enemy not to be this super-smart keyboard warrior, but someone who just happened to be in the right place at the right time, grabbed a laptop and the next thing you know, they have 30,000 personnel records. Most jobs, particularly at SSC, require the use of computers. Anyone can be a target for a cybercriminal, which is why cybersecurity is everyone's job," Frank added..

*"Cybersecurity is a critical tool to protect not only organizations and individuals, but also to defend our nation against attacks from adversaries, who have demonstrated the clear intent to disrupt our national ground and space systems," said Joy White, executive director of Space Systems Command, who delivered opening remarks at the Command's annual **Cyber Expo** in April. "Here at SSC, we're collaborating with our mission partners, industry, and academia to make sure our acquisitions are cyber-hardened and that the United States is training more cybersecurity experts to join the fight. Our Chief Information Office has been tireless in its efforts to improve the tools and technologies we use, as well as how we support and develop our cybersecurity and IT workforce."*

Ms. Joy White, Space Systems Command's executive director, provided opening remarks during SSC's Cyber Expo April 23, 2024, at Los Angeles Air Force Base in El Segundo, Calif. The annual event provides attendees with insight about the use of cyber resilience through panel discussions and hands-on demonstrations showcasing how SSC is using cyber resilience to protect current and future space systems and acquisitions. (U.S. Space Force photo Van Ha)

Under Col. Frank's helm, SSC is increasingly moving to the Cloud and ***Virtual Desktop Infrastructure*** (**VDI**) that allow users to access enterprise computer systems from any device securely.

"My big push is to get as much VDI and as much virtual capability as possible so that if a device gets stolen, all they have is a $3,000 laptop and we have to do a FLIPL (Financial Liability Investigation of Property Loss) and the person has to pay for it," Frank said. "It's not that cyber criminals can't access data on the computer – it's that there is no data on the computer. The computer is merely a window into where the data is on the server. The virtual desktop infrastructure is basically a choose-your-own-adventure video, because all you're doing is looking at screen scrapes, it's all on the server. So (cyber criminals) could steal a laptop, but they're never going to get the data because there's nothing there."

Frank also is working to embed cybersecurity teams within the Program Executive Offices to "*bake in*" cybersecurity from the very beginning.

"What we see sometimes is that something is engineered, designed, and built to work, but at the end they say, 'Oh yeah – we gotta do cybersecurity – somebody grab the ATO checklist and start marking things off,' without putting active cybersecurity controls into the program," Frank said. "The whole point of having those teams is that there's somebody there to speak for cybersecurity right from the very beginning, not just when we're getting ready to launch a satellite."

SSC also has been working with the ***National Security Agency*** (**NSA**) at the behest of *Frank Calvelli*, Assistant Secretary of the Air Force for Space Acquisition and Integration, to develop a crypto roadmap to make sure cryptography was not becoming the critical path in programs, or the longest sequence of activities that must be finished on time to complete a project.

"In other words, when a satellite is being put up, and it has to have an encryption device on it, we want to make sure that the time it took to get the encryption device designed, certified manufactured, and put on the system was not holding up the deployment of the satellite all together," Frank said. "One of the things we had to look into was, do we have crypto that is being designed without checking with the accreditation offices that it was actually encryption that NSA and other entities approved for transmitting classified information? It was determined that yes, there are satellites that are using one-off special encryption devices rather than the standard, but that didn't look like it was holding up any satellite development or deployment."

Frank said his office also is working to develop a cryptography office – either within CIO or within SSC's ***Space Systems Integration Office*** (**SSIO**) to work with the program offices and keep them current on recommended encryption devices. As is the case with this initiative and others, an ongoing challenge is staffing and retention.

Just as the U.S. Air Force has had to deal with losing trained USAF pilots to higher salaries in the commercial industry, Frank said the U.S. Space Force features stiff competition from the private sector for cybersecurity professionals,. According to the ***National Institute of Standards and Technology***, more than 1 million people in the U.S. are employed in cybersecurity in 2024, but there are only 450,000 cybersecurity jobs open. For every 100 cybersecurity jobs, only 82 people had the necessary education, experience, and qualifications to fill them. On average, cybersecurity roles take 21 percent longer to fill than other IT jobs.

Obtaining more cybersecurity experts in the pipeline is complicated, for numerous reasons, Frank said. For one thing, what most people call "*cyber*" isn't just one field: in the USSF, there are three separate categories – ***Defense Cyberoperations Space*** (**DCO-S**); ***Mission Comms***, which is command and control for satellites; and ***Base Operating System Information*** technology (**BOS IT**), covering SIPR and NIPR terminals.

"There's a difference between an information systems manager and a cyber defender," Frank added. "We have those very defined trainings and certifications so that when you have a defensive cyber operator, they can actually defend, and not just someone who can configure a network switch so you throw them in a chair to do cyber defense."

Cybersecurity is also more typically a mid-level career, requiring certifications — including training and certifications on specific cyber tools — and real-world experience, rather than an entry-level position and is certainly not as glamorous as Hollywood has defined the technology.

"The hacker movies and TV shows, typically show somebody sitting at a desk and there's this giant screen wall, and the next thing you know, the hackers get in and there's all these lights and buzzers going off on the big screen wall," Frank said. "That's not what it is at all. It's a cyber defender looking through massive amounts of system logs, trying to find that one line a hacker didn't delete, to identify that someone was in our network nefariously."

That's where partnerships such as ***CHIRP*** (**Cyber Halo Innovation Research Program**) can help. CHIRP, a collaboration between SSC and ***Pacific Northwest National Laboratory*** (**PNNL**) is a college-to-career program that brings government, industry, and colleges and universities together to provide students with a direct two-year pathway to a cybersecurity career at SSC or an industry partner. Frank said PNNL also is helping SSC develop a cybersecurity test range.

Keeping these highly trained professionals once SSC has acquired them may require USSF offering some additional, financial incentives, Frank said, just as other services have done over the years. Some will choose to stay on because they like the mission or the idea of serving their country in a cause greater than themselves. However, working for the military definitely has other advantages.

"The military is the only profession where you can drastically change your career several times and not have to go back to square one," Frank said. "I've been in the military for almost 31 years now, and I've had 10 different military occupational specialties, seven of which required me to go to formal training or school," Frank said. "I moved from being an Explosive Ordnance Disposal (EOD) officer to an information systems manager and, every time I transferred, it wasn't like I was starting an entirely new career where I'd lost all my seniority and all my pay rates — I just kept going from that moment forward."

As prevalent as computers and technology are in the modern workforce, people don't always understand how they work. You don't have to understand what ***SMTP (Simple Mail Transfer Protocol)*** is to send an email, but leaving everything to the cyber professionals can leave users vulnerable to cyber criminals.

"When somebody asks me, 'What do you do?' my answer is: I am the master of the blinky lights." Frank said. "If a blinky light isn't working right, who do you go to? You go to the IT and cyber people, and we wave our magic wands and change a port number and magically everything works while keeping it all secure. We always say that the biggest threat in cybersecurity is layer 8," Frank said. "That's a joke, because when you talk about the internet, you talk about the ***OSI model*** *(***Open Systems Interconnection***) which is 7 layers: the physical layer, layer one, all the way up to the application layer, which is layer 7. Layer 8 is the human user — that's where the biggest weakness rests. The vast majority of major hacks that we've had in the last 20 years were all social engineering from the help desk and telling you to give them your login and password. That's why VDI and a lot of these cross-connect systems that we're looking at will help protect against these internal threats, because sometimes these internal threats aren't intentional."*

Frank added, "Sometimes, somebody made a mistake and clicked the wrong button and accidentally sent off a bunch of information. The more we virtualize our systems and data, the more it's centrally controlled in the server, the less chance there is for it to be exfiltrated out. Additional basic training isn't always the solution, because a lot of times you have to experience the result for yourself," Frank said. "You have to be in a job or a position where you actually physically or personally see what can happen when things go wrong. For a lot of our users, they're like 'Yeah, yeah, I have to do this cybersecurity training, let me put it on autoplay while I do whatever else.' Because for a lot of them, it's just a rehashing of the same things they already know "To really get to the point where you have a true cybersecurity mind, you have to live the experience and start getting some of that higher level training where you realize, this is real and it's a real problem. And we just don't have the time or money to do that, and that's why it's so important to have cybersecurity professionals embedded with the different organizations who can advise the users where the threats are and what has to be done."

At the same time, stiff penalties are needed for people who do the wrong thing — and don't immediately self-report to security managers so the cyber professionals can stop or mitigate the damage, Frank said. He recalled a contractor at a previous job who not only lost her ID badge, but also the SIPR token attached to the badge, which happened to have a sticky note on the back with her PIN. That contractor was fired the next day.

"I like to call IT the greatest disaster known to man," Frank said. "It's 100 percent our own construct. We designed and created it, but we've made it an absolute disaster to run. When I started out, there wasn't a lot of networking, the internet didn't exist, it was all basically sitting down at a computer and playing a game that you got somehow – which was difficult because there was no online purchasing – or you wrote your own programs."

Frank entered the Space Force in July of 2023 after serving 30 years in the Army, including two tours in Iraq, one tour in Afghanistan, two tours in Germany, and three tours in the Republic of Korea.

How Cyber-Savvy Are You?

The U.S. Space Force (USSF) may be a digital service, but cybersecurity relies heavily on its people: both the trained cybersecurity experts and IT personnel, as well as the everyday users who must have a solid understanding of the critical importance of cybersecurity, said Col. Craig Frank, director of Space Systems Command's (SSC) Chief Information Office.

Cyber criminals are always looking for weaknesses they can exploit – don't be your company's weakest link! Test your knowledge of cybersecurity dos and don'ts with this quiz based on tips from SSC, the Federal Trade Commission, National Institute of Standards and Technology, and the U.S. Small Business Association and Homeland Security.

1. *What's the best way to protect your computer files and devices?*

A. Regularly update your software, including apps, web browsers and operating systems.

B. Back up important files offline, on an external hard drive or in the cloud. Important files stored off-site or on a server your company doesn't control should be encrypted. Make sure you store your paper files securely, too.

C. Use multi-factor authentication and require secure passwords.

D. All of the above.

2. *What is the best way to protect your wireless network?*

A. Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

B. Choose a cool but intimidating name for your network, such as "FBI Van No. 3."

C. Make sure your router offers WPA2 or WPA3 encryption and that it's turned on.

D. Use an easy-to-remember password, like PASS123, so you don't get locked out of your network, then jot it down on a sticky note so you don't forget.

E. Answers B and D

F. Answers A and C

3. *In a company, who needs to be trained on cybersecurity?*

A. Just the head of the IT department

B. The head of the IT department, the President, and Susie, who's in charge of payroll.

C. Everyone who uses computers, devices and networks.

4. *Hal gets an email from a sender he doesn't recognize that includes a link to download a free white paper on a topic he's interested in. He clicks on it, and suddenly, everyone in the*

building is locked out of the network – the email is a scam and now the attackers are holding the company's data hostage. What should Hal do? Select the best answer.

A. Try turning the computer on and off to delete the ransomware.

B. Immediately step away from the computer and call his company's security manager or alert his supervisor.

C. Pay the ransom using the company credit card.

5. Sarah, the marketing manager, becomes aware that someone is sending email messages that look like they're coming from her company. Scammers do this to get passwords and bank account numbers, or to get someone to send them money. What should Sarah – and her IT team – do to protect their company? Mark all that are true.

A. Ask the scammers nicely to stop, maybe by offering them a coupon.

B. Use email authentication – when you send an email from your company's server, the receiving servers will be able to confirm it's really from your company, and not an imposter.

C. Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You also can forward phishing emails to spam@uce.gov and to reportphishing@apwg.org

D. Notify customers as soon as possible by sending an email without hyperlinks. Remind them not to share any personal information through email or text. If your customers' data was stolen, direct them to IdentityTheft. gov to get a recovery plan.

E. Alert the staff and use the experience to update the company's security practices.

6. Elias gets a call on his personal phone from a man who claims to be from Microsoft, who tells him there's a virus on his computer and he needs Elias to give him remote access to his computer. What should Elias do? Select the best answer.

A. Hang up and then call his supervisor or security manager and tell them about the call.

B. Allow the caller to have remote access. He SAID he's from Microsoft, so it's probably OK.

C. Tell the man on the phone he doesn't own a computer..

D. Tell the man on the phone he doesn't own a computer.

7. Harriet owns a large company that does business with a number of smaller vendors. What should Harriet do to make sure her company's networks aren't compromised if a vendor gets hacked by a cyber-criminal? Mark all that are true.

A. Include provisions for security in all Harriet's vendor contracts, including a plan to evaluate and update security controls.

B. Secure her network with multi-factor authentication and strong passwords ± at least 12 characters, with a mix of numbers, symbols and both capital and lower-case letters.

C. Verify compliance by establishing processes to confirm that vendors are following the rules.

D. Harriet shouldn't worry about it. The risk is probably low enough that she can ignore it.

8. Marty attends an industry conference where one of the vendors is handing out free USB sticks shaped like really cool r rockets, but he arrives too late to get one. Later, he sees one of the USB sticks on the floor. What should Marty do with the USB? Select the best answer.

A. Give the USB to the head of IT or his security manager.

B. Plug it in to his laptop to make sure it works.

C. Return it to the vendor.

Answer key

1.— D. All of the above. Make sure you use passwords for all laptops, tablets and smartphones — and don't leave them unattended in public places.

2. — F. Choosing a silly name for your network and a password anyone can guess will NOT secure your network.

3. — C. Make sure employees understand their personal risk in addition to their crucial role in the workplace. If employees don't attend training, consider blocking their access to the network.

4. — B. Bob shouldn't try to fix it on his own. He should immediately notify his supervisor or security manager. In addition to scam emails, attackers also can start a ransomware attack using infected websites, server vulnerabilities and online ads — even on websites you trust.

5.— B, C, D, and E. Be sure your staff is trained on how to avoid phishing schemes.

6.— A. Never give anyone your password, and don't give remote access to your computer to someone who contacts you unexpectedly. If you DID share your password with someone you later suspect was a scammer, change it on every account that uses that password. If your computer is connected to a network, get a trusted security professional to check the entire network for security intrusions.

7. — A, B and C.

8. — A. Marty doesn't know where that USB has been. It could have been infected with malware and planted just for him — or anyone else — to find. He should immediately give it to IT or his security manager and not plug it in to any laptop device. Returning it to the vendor isn't smart. If it's been tampered with, the vendor's computers could be affected.

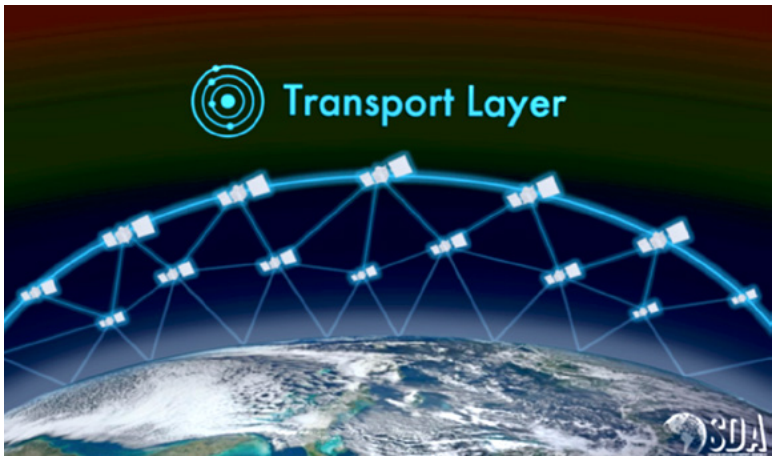
Space Systems Command is the U.S. Space Force field command responsible for acquiring, developing, and delivering resilient capabilities to protect our nation's strategic advantage in, from, and to space. SSC manages a $15.6 billion space acquisition budget for the Department of Defense and works in partnership with joint forces, industry, government agencies, academic and allied organizations to outpace emerging threats. Our actions today are making the world a better space for tomorrow

For additional information, contact Space Systems Command at ***SSC@spaceforce.mil*** and/or follow on ***LinkedIn***.

Author Lisa Sodders writes the monthly Space Systems Command column for MilsatMagazine.

Opportunity Announcement

The Space Development Agency (SDA) has released a new type of solicitation using other transaction authority (OTA) to select a pool of potential performers called the Hybrid Acquisition for Proliferated LEO or HALO — those selected to join the HALO pool will be eligible to compete for future demonstration prototype orders. HALO is an acquisition approach to solicit and award rapid, affordable mission feasibility demonstrations.

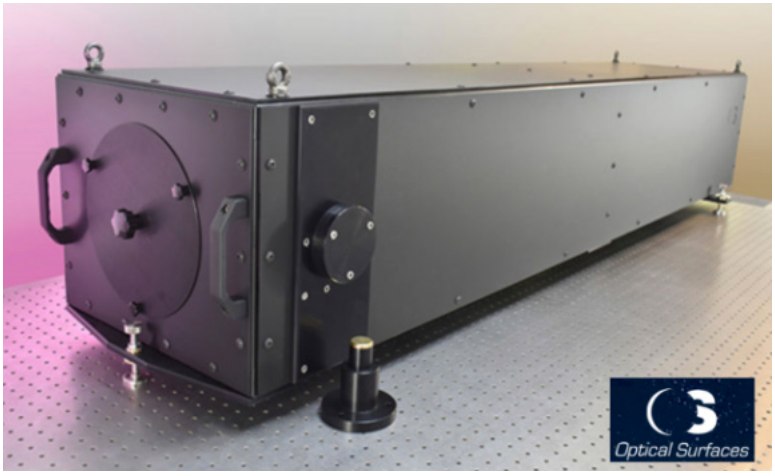


This solicitation provides an opportunity for industry to join a vendor pool to compete for specific on-orbit demonstration opportunities. Only vendors in the HALO pool will be able to bid against specific future prototype orders geared toward this effort, with the anticipation of multiple prototype orders being initiated and awarded per year.

A key goal of HALO is to put in place a flexible and fast contracting mechanism to compete and award Tranche 2 Demonstration and Experimentation System (T2DES) and other SDA demonstration projects. HALO may also increase the pool of performers capable of bidding on future SDA programs, including participation in layers of future tranches.

HALO will provide opportunities for companies to gain valuable experience working with SDA on demonstration projects. HALO pool members will also be able to work directly with SDA to ensure their security capabilities are sufficient to perform on SDA missions. HALO is structured as a multiple step competition, with initial selection into the HALO pool limited to non-traditional defense contractors. SDA is expecting multiple initial pool members and intends to review the pool periodically.

For more information on the HALO pool requirements for mission success and representative prototype orders, view the full solicitation ***at this direct link***. Initial proposals to join the HALO pool are due by 12:00 pm ET on July 11, 2024.



HIGH STABILITY BEAM COLLIMATORS FOR MILITARY OPTICS TESTING

Optical Surfaces Ltd. has supplied two reflective beam collimators to a leading European supplier of high precision optics to military and defence contractors.

Reflective beam collimators are mirror assemblies that take divergent or convergent incoming light and produce parallel output

They can be used to replicate a target at infinity without parallax. Consequently, reflective beam collimators are the device of choice for performing *Modulation Transfer Function* (MTF) measurements over extended wavelength ranges.

Benefiting from a lightweight design and new assembly technique — Optical Surfaces beam collimators uniquely combine high stability, high performance, and short delivery time all at a market competitive price.

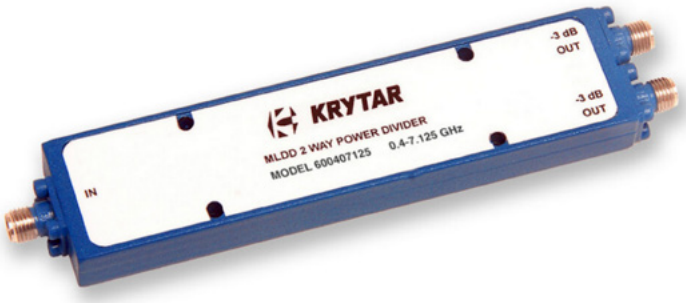
The company's ISO 9001-2015 approved manufacturing workshops and test facilities are deep underground in a series of tunnels excavated in solid chalk.

This provides an environment where temperature is naturally thermally stable, and vibration is extremely low.

With such stable conditions testing of all beam collimators becomes quantifiable and dependable

In addition to these natural advantages, Optical Surfaces Ltd. has invested in an extensive range of test equipment and uses trusted methods to ensure accurate and reliable testing of surface accuracy, quality, and slope errors.

> *Dr. Aris Kouris, Sales Director of Optical Surfaces Ltd., said, "MTF is a technique, trusted by optical designers, for objectively evaluating the image-forming capability of military optical systems. We were chosen as a partner for this project because of our track record in supplying affordable, high performance beam collimators tailored to enable precise MTF testing of military optical systems."*
>
> *He added "The high stability and performance of our reflective beam collimators is achieved using a zero expansion off-axis parabolic mirror, manufactured to better than lambda/10 p-v surface accuracy. The all-reflecting design of our beam collimators is achromatic and with aluminium / magnesium fluoride coatings can operate from the UV to the infrared without adjustment. The optics within each beam collimator are secured using stress-free mounts and come pre-aligned for optimum performance. The off-axis design of our beam collimators produces no central obscuration thereby ensuring highly efficient transmission is obtained."*



KRYTAR intros a compact matched-line directional divider

***KRYTAR, Inc*. has introduced an *MLDD 2-way Power Divider* that excellent performance over the frequency range of 0.4 to 7.125 GHz (L- through C-bands) in a compact package — this new power divider offers the ultimate solution for emerging designs and test and measurement applications including SATCOM, mmWave, 5G, radar and more.**

KRYTAR's technological advances provide excellent operating performance of this new 2-way matched-line directional divider (MLDD). *Model 600407125* covers the full frequency range from 0.4 to 7.125 GHz with >15.0 dB Isolation and ±0.2 dB of maximum Amplitude Tracking, with maximum Phase Tracking of ±3 degrees.

The 2-way divider exhibits Insertion Loss of <1.0 dB across the full frequency range. Maximum VSWR is 1.6. Input power rating is 10 watts with 2:1 load VSWRs. Units with tighter Amplitude and Phase Tracking specifications can be supplied.

This new Power Divider is a compact package measuring just 7.75 inches (L) x 1.00 inches (W) x 0.52 inches (H), weighs only 7-ounces, and comes with standard 3.5-mm coaxial female connectors.

Specifications for the full line of KRYTAR 2-Way Power Dividers can be found on the company's website: Power Dividers

KRYTAR's new Model 600407125 Power Divider offers full frequency coverage in a single package and provides superior performance targeting broadband ***electronic warfare*** (**EW**) systems and complex ***switch-matrix applications***.

KRYTAR has used its proprietary design to produce a wide assortment of matched-line directional dividers (MLDD) with excellent performance over ultra-broadband frequencies. KRYTAR MLDD 2-way Power Dividers are a new class of patented directional devices. These directional dividers can be manufactured to meet ridged military specifications.

KRYTAR also offers complete engineering services for custom designs that meet or exceed critical performance and/or packaging specifications. A data sheet with specifications and package outline drawing is available via KRYTAR's website.

GMV to supply the new space surveillance system for Spain's Ministry of Defense

***Spain's Ministry of Defense*, through its Directorate General of Weapons and Material, has awarded a €2.7 million contract to the multinational technology firm *GMV*, for development, implementation, and support and maintenance of the Space Situational Awareness and Control System (CCSE) that will be used at the Space Surveillance Operations Center (COVE).**

That center, which is operated by the ***Ministry of Defense*** (**MINISDEF**) as part of the ***Space Command*** (**MESPA**) of the ***Spanish Air and Space Force*** (**EA**), was created on November 28, 2019, by Ministerial Resolution 702/18699/19 (*Official MoD Gazette no. 233*).

Since then, the center's capabilities have been in a state of ongoing development, to achieve its space surveillance and situational awareness mission, and to provide operational support services for the Spanish Armed Forces. The center reached its ***initial operational capability*** (**IOC**) on July 14, 2021.

GMV has been providing support to this center from the beginning, which has in turn been assisting the ***U.S. Space Command*** with its ***Global Sentinel*** exercises. As part of its support, GMV has supplied its operational orbit determination tool known as Sstod, for processing space surveillance radar measurements at the Morón Air Base near the Spanish city of Seville.

To help the center achieve ***full operational capability*** (**FOC**), the Spanish Ministry of Defense's ***Sub-Directorate General of Procurement***, which is part of its Directorate General of Weapons and Material, announced a competitive tendering process at the end of 2023 for a ***Space Situational Awareness and Control System*** (**CCSE**), and GMV has been awarded the contract.

The functionalities covered by this contract include orbit calculation and propagation, generation, and maintenance of a space object catalog (with open and classified versions), prediction of atmospheric reentry, calculation of flyby events, planning of observation and sensor calibration campaigns, calculation of ***Global Navigation Satellite System*** signal degradation, and integration and processing of space weather data.

This system is expected to go into service at the end of 2024. To comply with this timeline, the system will be based on GMV's *Commercial Off-The-Shelf* (**COTS**) system known as ***Ecosstm***, which is already being used in other operational environments such as the ***German Armed Forces Space Situational Awareness Center*** (Weltraumlagezentrum), the civilian space surveillance systems of various other countries such as Greece, and GMV's commercial space surveillance center known as Focusoc.

With this new contract, GMV is further solidifying its position as a European leader in the development of space surveillance and command and control systems, which is an area where the company already has experience in both civilian (institutional and commercial) and military applications.

High Throughput Tactical FlyAway & Gateway

2.4m Full Hemispherical Tracking Terminal
GEO / MEO / LEO Multi-Orbit
X, Ku & Ka Bands
SATCOM / SIGINT / EW / EO

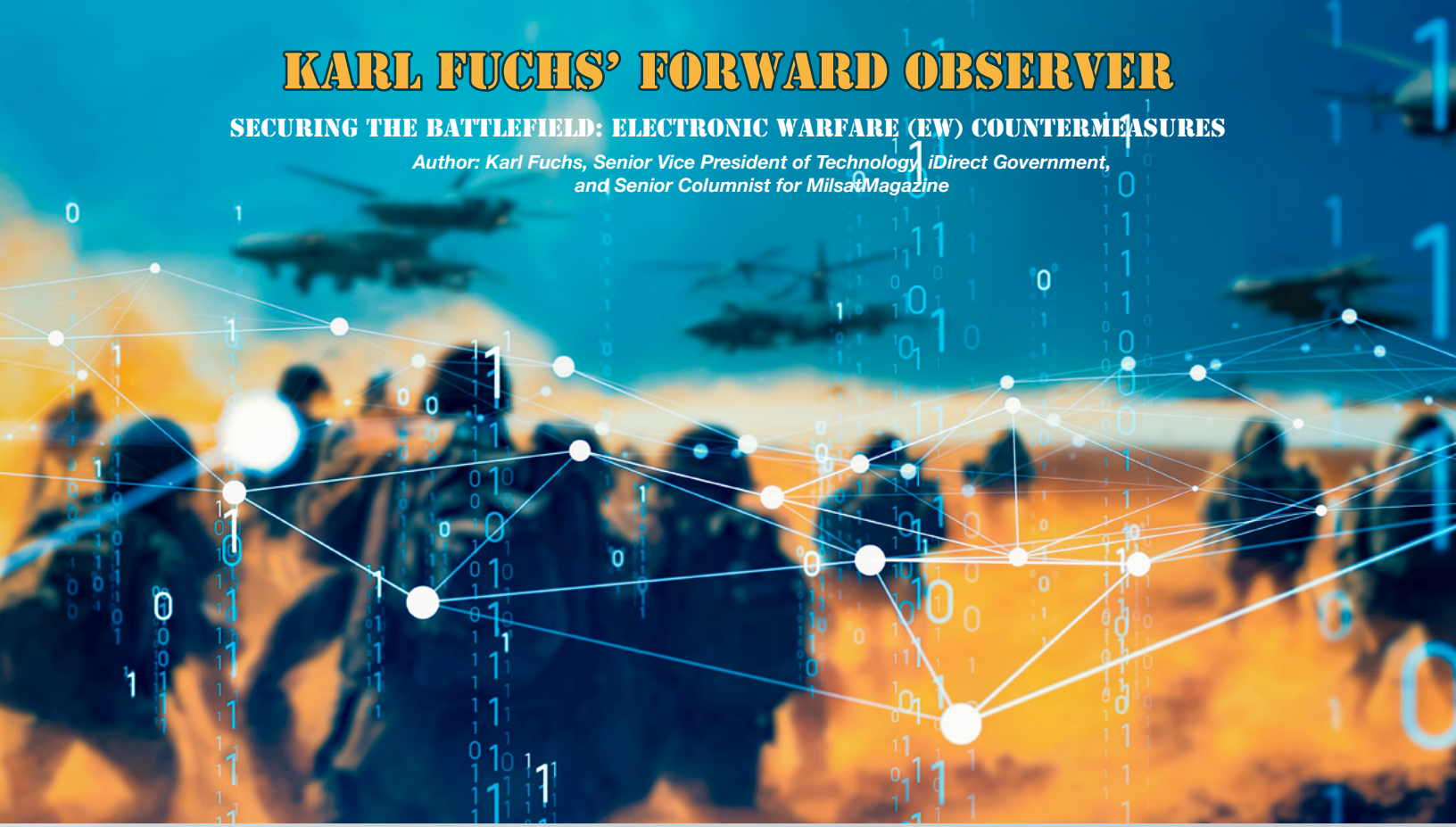
AvL TECHNOLOGIES
avltech.com

Let's Talk Multi-Orbit

KARL FUCHS' FORWARD OBSERVER

SECURING THE BATTLEFIELD: ELECTRONIC WARFARE (EW) COUNTERMEASURES

Author: Karl Fuchs, Senior Vice President of Technology, iDirect Government, and Senior Columnist for MilsatMagazine



The fusion of electronic warfare (EW) tactics and satellite communications stands as a critical cornerstone in modern military strategies.

The escalating reliance on cutting-edge technologies to gain strategic advantages has accentuated the intricate interplay between EW tactics and the safeguarding of satellite communication systems.

This article delves deeper into the multifaceted dimensions of EW, evolving jamming technologies, countermeasures, and the escalating role of anti-jamming technologies in fortifying satellite communications on the dynamic battlefield.

ELECTRONIC WARFARE DYNAMICS JAMMING, DETECTION AND SPOOFING

EW encompasses diverse tactics, with jamming technology serving as a prominent method employed by adversaries to disrupt or interfere with desired signals.

These threats exhibit a spectrum of sophistication, ranging from overt transmission blocks to elusive and subtle interference patterns, posing significant challenges to signal integrity and reliability.

Moreover, EW maneuvers encompass signal detection, geolocation for targeting and the intricate art of signal spoofing, encompassing pivotal systems such as GPS and communication devices.

HISTORICAL COUNTERMEASURES AND CONTEMPORARY TECHNOLOGICAL ADVANCEMENTS

Historically, countering jamming threats primarily relied upon spread spectrum technology, notably ***Frequency Hop Spread Spectrum*** (**FHSS**). However, contemporary advancements have propelled anti-jamming capabilities into the digital realm, primarily through the use of ***Direct Sequence Spread Spectrum*** (**DSSS**).

Additionally, signal excision technologies, exemplified by ***Communication Signal Interference Removal*** (**CSIR**™), have emerged as formidable tools in neutralizing interference without being reliant on traditional spread spectrum techniques. The amalgamation of DSSS with CSIR technology epitomizes a robust anti-jamming solution, amplifying data throughput capacities beyond the constraints of conventional FHSS methods.

Low Probability of Interception/Low Probability of Detection (***LPI/LPD***) mechanisms constitute pivotal countermeasures against geolocation-based jamming threats. Leveraging DSSS, these techniques effectively diminish the power spectral density of carriers to levels below discernible thresholds amidst background noise.

The integration of DSSS with CSIR technology enhances the effectiveness of LPI/LPD measures and also elevates the data transmission rates of these signals, crucial in scenarios with inherently low user data rates.

Spoofing, a highly sophisticated EW threat, necessitates intricate countermeasures. The integration of x.509 digital certificates, a cornerstone of ***transmission security*** (**TRANSEC**) solutions, represents a robust defense mechanism against spoofing attempts. However, in scenarios where bidirectional certificate exchanges prove unfeasible, such as broadcast signals including ***Position Navigation and Timing*** (**PNT**), simpler encryption methods stand as effective anti-spoofing measures for safeguarding PNT signals.

THE PROLIFERATION OF EXCISION TECHNOLOGY AND ITS ROLE IN MITIGATING EW THREATS

The prowess of excision technology lies in its ability to effectively mitigate diverse forms of interference, ranging from carrier waves to intermittent and fastmoving threats, all without necessitating prior knowledge or additional hardware.

This capability assumes particular significance as adversaries increasingly employ ***signal intelligence*** (**SIGINT**) strategies to disrupt military and governmental spectrum use.

In the pursuit of secure and dependable communications infrastructure, the evolution of anti-jamming technologies remains instrumental in fortifying satellite transmissions across dynamic and adversarial landscapes. These advancements play a pivotal role in mitigating threats, fortifying troop safety across varied terrains — land, air and sea — and ensuring the integrity of sensitive data and SATCOM networks against hostile incursions.

The symbiotic relationship between EW strategies and the protection of satellite communications epitomizes a critical nexus in contemporary military operations. As technology continues to evolve, the perpetual arms race between EW tactics and countermeasures underscores the need for robust, adaptable and innovative approaches to fortify satellite communication systems against emerging threats in the ever-evolving battlefield environment.

www.idirectgov.com

Karl Fuchs is the Senior Vice President of Technology at iDirect Government (iDirectGov), a U.S. corporation that is a trusted partner of the U.S. government and has been for more than 18 years. All its employees are U.S. citizens, with a third being U.S. military veterans. Fuchs leads iDirectGov's team of federal systems engineers and serves as chief architect for new product integration and specialized technology including transmission security (TRANSEC), Communication Signal Interference Removal (CSIR™) anti-jam technology and Open Antenna Modem Interface Protocol (OpenAMIP). All Defense-grade products sold by iDirectGov are designed, developed, assembled, programmed and verified within the United States. Fuchs has more than 20 years of experience in the areas of technology and the federal government and is a Senior Contributor to MilsatMagazine.
kfuchs@idirectgov.com.

SATCOM'S CRITICAL ROLE IN DISASTER RECOVERY

Author: Nimrod Kapon, Founder and Chief Executive Officer, OASIS Networks

In the aftermath of disasters, whether natural disasters or as the result of conflict, effective communication can be the difference between life and death. In these situations, it's vital that lines of communication are quickly established. This enables agencies to get a clear picture of the situation on the ground, and also allows for coordinated response and recovery efforts to happen so that the necessary aid and resources reaches the right places as soon as possible.

However, communication in these situations is often challenging. Terrestrial infrastructure may be lacking or become overloaded as a result of the disaster, and additionally, there might also be damage to infrastructure that disrupts existing wired and cellular communication networks.

Satellite connectivity on the other hand has several distinctive features that make it very well suited for use in disaster situations, yet NGOs and other organisations are not always using it to its full potential. Why is that and what can we do about it?

SATELLITE IS A CRITICAL ENABLER IN DISASTERS

Let's begin by looking at why satellite connectivity is so important in a disaster. First, its global reach means that it can be used to provide immediate and reliable communication networks anywhere in the world. And with the ability to operate independently of other communication networks, satellite terminals can be used without the need for infrastructure to already be in place.

This means that a communication channel can be easily established regardless of the conditions in the area, even when infrastructure is completely lacking or has been damaged. With the correct expertise and equipment, satellite terminals are generally easy to install and set up.

Additionally, satellite terminals can be configured to get the service from a teleport located in another country so that there is no dependency on local personnel who may also be affected by the disaster.

Given these characteristics, it's clear that satellite connectivity is a key enabler and should be incorporated into disaster planning and recovery.

BARRIERS TO MAXIMIZING SATCOM'S POTENTIAL

The satellite industry is highly dynamic, and innovations and technological developments are happening all the time, which could enormously benefit regions experiencing disaster events.

However, many regions are still reliant on older equipment, and are not benefiting from these technological innovations. This comes largely down to complex political and indeed financial reasons, although challenges around logistics and resource management also play a part, particularly when dealing with geographically remote locations.

And even if the latest SATCOM equipment is available, without the right expertise to hand, there's always a possibility that it may not be used correctly, or fully used.

It's true that SATCOM technology has improved a lot in the recent years, to the point where there are some satellite terminals that can be easily installed even by people with very limited technical skills. However, not all equipment is quite so easy to use, and so it's not unusual for organisations to view the technology as technically complex and even intimidating.

This creates a real barrier to its use. To overcome this, and to make satellite technology much more inclusive, it's important that NGOs are educated and trained about satcom systems and available resources. It's important that as an industry, we raise awareness among NGOs about the available resources that can support them to leverage satcom in both disaster planning and recovery situations.

There are many resources available in different countries that are not being used efficiently, in terms of both available satcom equipment and qualified engineers. If organizations operating in disaster scenarios are aware of all available resources, they may be able to deploy a communication channel much faster than they can currently.

EXPERTISE WHERE NEEDED

Of course, it's important that field engineers are well-equipped and trained to install and maintain satellite terminals effectively. This is why ***Oasis*** is a proud member of ***GVF/GSOA*** and indeed invest lot of effort and energy into on-going training and equipping of field engineers.

But aside of this, situations will also arise when qualified field engineers are not readily available on site to establish the satellite link. In these scenarios, there is a need to guide local staff, who are not certified VSAT engineers, to bring the satellite link up. In these circumstances, the set up just needs to be good enough to work for a limited time, at least until someone qualified can reach the site and fix things up.

We have teams that are spread all over the world, so can usually dispatch someone fairly local, fast enough to provide a second line of support, if not a first one. We have constant access to local engineers with whom we work all the time, not only when there is a crisis. And crucially, we have access to wide inventory of equipment located in many countries around the globe, which helps to ensure that equipment can quickly be delivered to the affected area.

EDUCATION + TRAINING IS KEY

Although we're an established VSAT company, we haven't previously been involved with deploying satellite technology in emergency or disaster situations. However, we're quite familiar with emergency situations that require swift response as well as dealing with difficult logistics challenges such as inaccessible roads, poor weather and security concerns.

For example, some years ago, there was a highly unusual satellite failure that suddenly affected thousands of Earth stations, some of which were providing critical infrastructure, such as GSM connectivity. All of a sudden, we were inundated with urgent requests to send engineers in several countries to migrate services to other satellites.

In the **Democratic Republic of Congo** alone, we dispatched more than 40 engineers to some of the most extreme locations in the country. To access some locations, we had to convoy with the army, and in other areas we had to get to sites on motorbikes, or even navigate with canoes or hike by foot.

Experiences such as this makes us well placed to help guide NGOs, agencies and field engineers to deploy satellite technology in emergency situations. We're thrilled to be involved in a wonderful training project in **Ghana** that is being run in partnership with a local university, the **UENR** in Sunyani, and funded by the **World Bank**.

Under the project, we'll be providing training to future field engineers under a structured curriculum of academic courses, which will cover both theoretical and practical aspects of satcom. The trainees will obtain both certifications that are recognized by the industry, and academic points that will be counted in their academic degree.

We've recently developed and launched the curriculum, and the first course is planned for June of 2024, with 25 subscribed participants. There is an expectation that the center will train at least 50 field engineers each year and will be hub for young students from neighboring countries as well.

Initiatives such as this are an important part of ensuring that SATCOM technology is being fully used by NGOs and other organizations. Alongside the training project in Ghana taking place this year, we also organize training sessions each year in different parts of this world. Last year, we trained people in Southeast Asia and, this year, we're focusing on West Africa at the center in Ghana and have also delivered some small-scale training in Latin America.

In addition to the main training events, we also hold sporadic training activities as and when needed. Our model of boots on the ground and equipment on the ground is highly relevant to the disaster response industry. While we are new to the field of disaster preparedness and recovery, we are eager to learn and to work with new partners.

ROLE OF PLANNING + COORDINATION

SATCOM clearly has a vital role to play in disaster recovery by facilitating emergency communication in affected areas. However, it is essential that it's use is planned for when governments, NGOs and organizations develop disaster preparedness strategies. This will help to ensure that adequate funding and expertise is in place for fast roll out of satellite communication networks in the event of a disaster.

Short-term and mid-term contingency plans are crucial for successful disaster response, as is access to a network of experts responsible for coordinating recovery efforts. Only with such coordination can regions fully harness the potential of satellite connectivity to support disaster response and recovery.

Getting this right is a critical part of ensuring that the people affected by disasters can access the help and support they need, so that they can stay safe and start to recover from the disaster event.

www.oasisnetworks.net

GA-ASI contracted to build + field 1st Gray Eagle 25M for Army National Guard

General Atomics Aeronautical Systems, Inc. (GA-ASI) has announced that the Army National Guard (ARNG) has ordered 12 Gray Eagle 25M (GE 25M) Unmanned Aircraft Systems (UAS) paid for as part of 2023 congressional funding.

The funding comes after ARNG leaders, which make up 45 percent of the U.S. Army's combat divisions, requested GE 25Ms to make ARNG Divisions mirror the active component in being ***Multi-Domain Operations (MDO)*** capable, deployable, and better able to team with newly formed ***Division Artillery Brigades (DIVARTY)***. They will also be available to support domestic missions, such as homeland defense and disaster response, as needed.

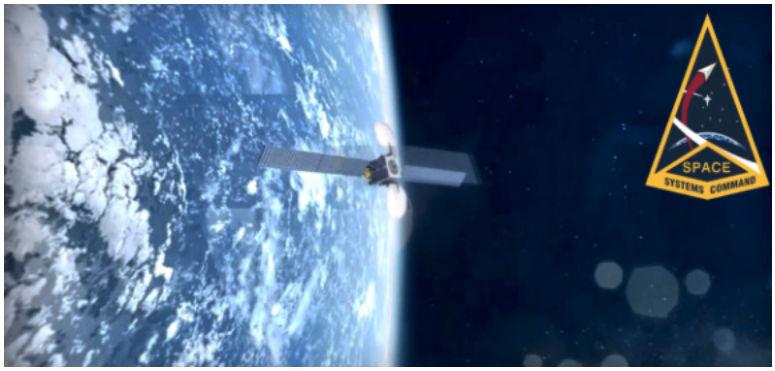
GE 25M is a modernized model of the Gray Eagle designed to meet the U.S. Army's needs for MDO capability for both active duty and National Guard units. GE 25M is equipped with the new **EagleEye** multi-mode radar and electro-optical/infrared sensors, and can host a wide range of additional kinetic and non-kinetic payloads.

Equipping ARNG Divisions with organic GE 25Ms makes possible the necessary mission planning, targeting, communications, detailed coordination, and realistic training needed to employ the systems successfully in combat. GE 25M will allow ARNG Divisions to have ***Divisional Reconnaissance, Surveillance, and Target Acquisition (RSTA)*** for the first time. GE 25M flew its maiden flight on December 5, 2023, following the award of an undefinitized contract award announced on Dec. 1, 2023, for the Gray Eagle 25M Production Representative Test Aircraft.

> *"The Gray Eagle platform has a proven record of performance with over a million hours of safe operations, including automatic takeoff and landing capability," said GA-ASI Vice President of DoD Strategic Development Patrick Shortsleeve. "The aircraft excels as an enabler for Fires, Maneuver, Network, and Intelligence operations. It is also an integral part of the Army Aviation team, working closely with manned rotary-wing systems to achieve overmatch against pacing threats."*

Space Systems Command awards million$$ to Starfish Space Inc.

Space Systems Command (SSC) recently awarded Starfish Space a $37.5 million Strategic Funding Increase (STRATFI) contract to build, launch, and operate an Otter satellite vehicle for a first-of-its-kind docking mission designed to provide two years of augmented maneuver for National Security Space assets.



Through partnership with ***Air Force Research Laboratory's (AFRL) SpaceWERX Program***, Starfish Space, Space Safari, and SSC Commercial Space Office, SSC's Assured Access to Space organization has expanded efforts to improve responsiveness, resilience and strategic flexibility of U.S. assets on-orbit; game-changing innovation and capabilities to win in today's Great Power Competition

The Otter spacecraft will be capable of performing ***autonomous rendezvous, proximity operations, and docking*** (**RPOD**), compatible with a wide range of clients, including those that were never designed or configured for docking. This capability gives the U.S. Space Force a range of options to support existing assets and allow future assets to be supported without imposing additional configuration requirements.

Advancing flexible RPOD capabilities with scalable architectures such as the Otter is critical to the development of various Space Mobility and Logistics missions in support of the warfighter. This effort builds on previous Small Business Innovative Research (SBIR) efforts, advancing early Research & Development efforts to viable capabilities.

Unique to the Department of the Air Force, the STRATFI (Strategic Funding Increase) program provides additional funds to scale Phase II SBIR efforts to achieve better technology transfer. STRATFI is structured to leverage private capital investment as a matching source of funds, with periods of performance up to four years, in order to de-risk development of emerging technology and transition research and development work into operational capabilities.

"This project is another step forward in delivering what our warfighters require in sustained space maneuver," said Col. Joyce Bulson, Director, Servicing, Mobility, and Logistics within AATS. "For a particular class of spacecraft with particular mission sets in GEO, refueling may be the answer to sustaining maneuver; for other systems, augmented maneuver options may be the solution. There is a wide range of applications for Starfish Space's Otter in addition to augmented maneuver, such as station-keeping or life extension, orbital transfer, and ultimately orbital disposal which assures access to key orbital slots while demonstrating responsible norms in space."

DISPATCHES

Iridium Communications Inc. ***(Nasdaq: IRDM) has announced a historic development for uncrewed aerial systems (UAS) operations Beyond Visual Line Of Sight (BVLOS).***

Iridium partner ***American Aerospace Technologies, Inc.*** (**AATI**) was granted a first-of-its-kind waiver from the ***U.S. Federal Aviation Administration*** (**FAA**) to conduct UAS surveillance of critical infrastructure in the San Joaquin Valley on behalf of a multinational oil and gas company. This waiver may serve as a tipping point for wider adoption of safe and scalable UAS operations in the ***National Airspace System*** (**NAS**).

Enabled by Iridium's L-band satellite connectivity, ***AATI's AiRanger*** is supporting remote aerial surveillance for the energy corporation's pipeline and production facilities. Iridium's low-latency network is providing reliable and cost-effective BVLOS connectivity, including remote ***Command and Control*** (**C2**) and ***Detect and Avoid*** (**DAA**) capabilities.

SkyLink 7100 (Aviation)

Flying over a pipeline network, the large drones (*more than 200 lbs*.) will send information via Iridium® satellites to quickly perform routine oil and gas pipeline inspections. Iridium partner ***Blue Sky Network*** customized the development and integration of its global, dual-mode ***SkyLink 7100*** voice, data, and BVLOS terminal installed on the aircraft. The Iridium Connected™ Skylink 7100 enables continuous tracking and C2 capabilities for aviation and UAV operations.

The Iridium Connected AiRanger is the first UAS to demonstrate compliance with industry consensus standards for the DAA system and meet FAA requirements for aircraft right of way BVLOS operations. This milestone helps pave the way for companies to deploy BVLOS UAS to support operations and achieve higher situational awareness, lowering inspection costs and maximizing value. The waiver demonstrates that Iridium satellite C2 capabilities can meet large drone BVLOS waiver requirements with the FAA.

Iridium continues to collaborate with the drone industry in establishing safe separation using ***Commercial Off-the-Shelf*** (**COTS**) avionics. Last year, Iridium published a whitepaper that addresses challenges faced in enabling a safe, scalable, and efficient adoption of UAS in the NAS, including how to maintain safe separation between aircraft and what supportive COTS avionics are readily available today. This whitepaper provides a recommended equipment list and highlights capabilities enabled by the Iridium network that support safe and scalable UAS operations in the NAS.

> *"This certification shows innovation through the fusion of technology, partnership, and practical application," said* ***John Peterson, Executive Director of Aviation, Iridium****. "When aircraft manufacturers and communications providers get together, scalable business solutions can become a reality. Iridium and our partners AATI and Blue Sky Network are proud to lay the groundwork for scalable BVLOS operations and show what's possible with reliable satellite communications."*

DISPATCHES

Reticulate Micro named exclusive supplier of Himera taccom radios in U.S.

Reticulate Micro, Inc. **and *Himera* have entered into an exclusive distribution agreement — Reticulate will serve as the exclusive supplier of Himera's battle-proven *Electronic Warfare* (EW)-protected tactical communication systems in the U.S. and with key global government customers.**

Himera was founded in Ukraine in 2022 after Russian's full-scale invasion of the country and has evolved to quickly meet the tactical radio needs of frontline soldiers, leapfrogging traditionally long procurement cycles to quickly develop and deploy its mission-critical equipment.

Himera has fielded thousands of secure tactical radios to the Ukrainian defense forces, with the number continuing to grow.

The radio functionality ensures both ***Low Probability of Intercept*** (**LPI**) and ***Low Probability of Detection*** (**LPD**). The ***Frequency-Hopping Spread Spectrum*** (**FHSS**) technology allows the radio to switch frequencies, making it challenging to target.

The Himera G1 Pro

Built from ***Commercial Off-the-Shelf Components*** (**COTS**), the ***Himera G1 Pro*** employs FHSS technology, which has been proven resistant to EW, according to published reports by the **Ukraine Minister of Digital Transformation**. The G1 Pro will incorporate both **AES 256** and **Post-Quantum** symmetric encryption for added performance and security.

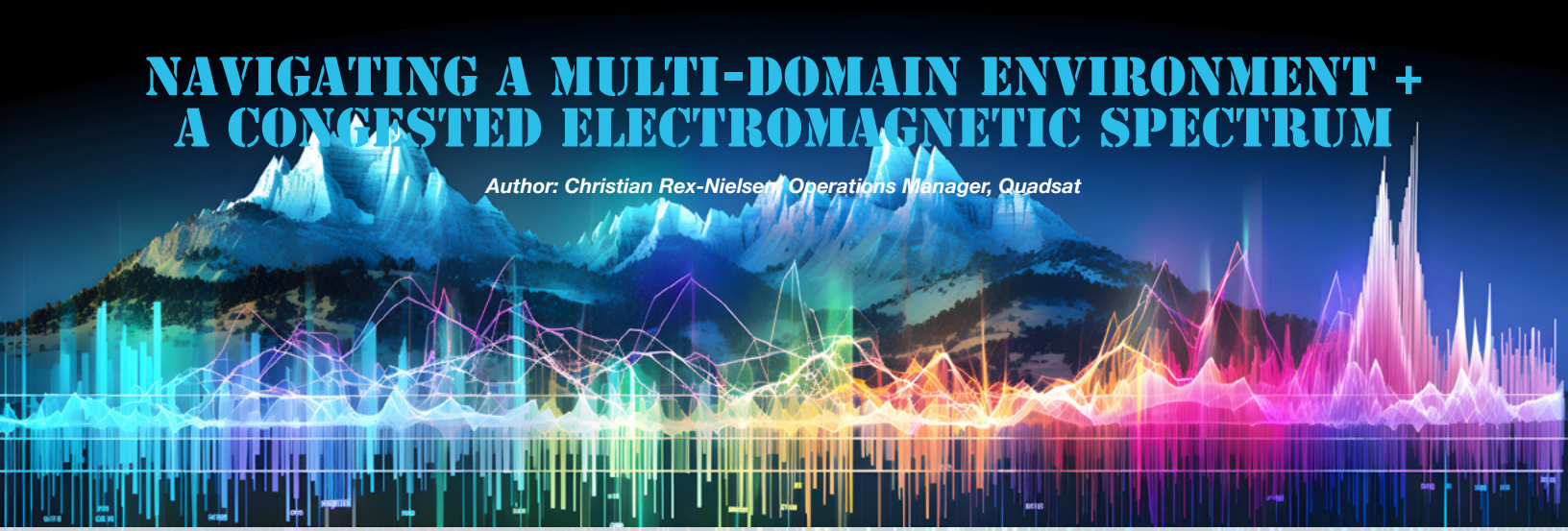
*"Our This battle-proven technology fills the gap between inexpensive radios that are unsecured, and those that are sophisticated with premium features and correlated prices," said **Joshua Cryer, president and CEO of Reticulate Micro**. "We are not looking to compete with larger program of record tactical MESH radios, and in fact, believe the Himera technology is complementary to many of the radios that are currently fielded by U.S. and coalition forces."*

Misha Rudominski, co-founder of Himera, said, "We are excited to work closely with Reticulate to get our products much faster to clients who need them most. Partnering with Reticulate Micro is an opportunity to aggregate a lot of knowledge and expertise from the global defense market and merge it with what we've learned in Ukraine to create even better products. We built our products with users in mind – to make them easy to use and to resolve specific issues met by those on the front lines of the battlefield."

*"The Himera G1 Pro has proven very effective on the battlefield in the Ukraine, supporting voice, GPS and data for a squad radio at a very low price," said **Louis Sutherland, Reticulate Micro's senior director of Business Development and the company's lead on tactical markets**. "There aren't any suppliers out there that can provide this capability at this cost. On top of that, we are leapfrogging current radio technologies with Post-Quantum symmetric encryption."*

NAVIGATING A MULTI-DOMAIN ENVIRONMENT + A CONGESTED ELECTROMAGNETIC SPECTRUM

Author: Christian Rex-Nielsen, Operations Manager, Quadsat



Ensuring seamless and consistent use of the Electromagnetic Spectrum is fundamental to enabling the military to communicate with confidence, navigate with certainty, perceive an operational area with lucidity, and engage with accuracy during peace, crisis, or conflict.

However, the increasingly complex multi-domain environment, coupled with recent and ongoing conflicts, is making that more challenging than ever before experienced. This is having a knock-on effect for communications — this is making all of the fundamentals of warfare extremely challenging and even changes the skillsets required for military personnel in the field.

Navigating this evolving landscape requires the military to effectively make the invisible, well, visible, in order to easily gain insight and knowledge of the available spectrum and any threats to keeping the spectrum 'clean.' But what is the invisible and exactly how can it be made visible?

OPERATING IN A MULTI-DOMAIN ENVIRONMENT

Warfare is no longer limited to one, or even just a couple, of domains. Land, sea, and air warfare remain critical; however, military operations now encompass cyber and space as well. Coordinating those operations across all domains can be extremely challenging and requires an enormous amount of planning and resources to ensure such is managed in a cohesive and efficient fashion. Add to that the fact that all of these environments are using the same electromagnetic spectrum, and the task at hand is not insignificant.

Since the onset of the war in the Ukraine, that spectrum has been under even more strain. Historically owned and managed by NATO, it is now highly congested ***and*** contested. It is no longer a simple question of adding a new service when needed. The congested spectrum means that it is almost impossible to ensure a high quality and safe transmission. This is making it challenging for military operations to be effective and ensure the reliability of fundamental communication, navigation, and perception needs as set out above.

THE INVISIBLE

As mentioned, part of the problem with the ***Electromagnetic Environment*** (**EME**) is that much is invisible, yet it remains extremely important, even vital, for all military operations. When a unit is setting out into a particular region, it is impossible to know what the EM spectrum will be like once they arrive as there are so many factors that impact the region. There are no google maps equivalent for seeing the current status of the spectrum in a given area.

There could, for example be solar storms... even wet woods... in the area, or power lines, all of which could interfere with the signal. Also challenging is determining the precise and up-to-the-minute regional weather conditions, and those conditions can have a huge, adverse impact on the radio signal. And, of course, the other big unknown is the presence of someone who may be deliberately jamming the signal.

In a conflict situation, there will most likely be other units in the same area, whether friend or foe, all using the identical spectrum. As EM spectrum becomes more and more congested, additional challenges with interference can be derived from a plethora of different sources. Not only is this difficult to predict, it is also complex to have a solid oversight of the cause in order to resolve it. And yet, in a military setting, it is more important than ever that any of these issues are resolved... and quickly.

TRAINING THE NEXT GENERATION OF SOLDIERS

These complex EM issues require a different skillset within military teams to manage them. In every part of the world, soldiers undergo extensive training which, for the most part, is centered around combat and some technology basics for use in the field.

As the environment becomes more complex, those same soldiers need to be equipped with enough knowledge to troubleshoot communications issues as they arise and to open lines back open as quickly as possible. In an envionment where there is likely little infrastructure, and often hostile conditions, and imminent threats, it can be extremely difficult to determine whether equipment is jammed, broken, or an operating error has been made.

For example, how many soldiers would know the best way to confirm if your **dagger** (***military GPS device***) is being jammed? Jamming requires line of sight. By placing the unit on the floor, or even in a hole in the ground, it might regain signal. If that action does not improve the signal condition, the problem is not jamming but something else.

It is clear that the military needs to look at adapting training to approach this new environment. As with most military training exercises, the most effective way to do this is by creating an in-field test scenario, giving soldiers as close to a real-life experience as is possible.

Using drone technology is the best way to create multiple different test scenarios for training and be able to deliver that condition elsewhere. It is then possible to simulate a connection with the satellite and a number of different scenarios, such as a how the equipment would react if there were a jammer, or how to react when the equipment itself is faulty.

By enabling that type of test scenario, teams could learn how they could quickly troubleshoot and resolve communications and navigation problems in short order, making them much better equipped once they are active in the field.

MAKING THE INVISIBLE VISIBLE

Tools exist to make the invisible visible; however, the real key to being able to do that effectively is to ensure teams know exactly how to react and troubleshoot, no matter what adversity is thrown at them. Being able to easily simulate real-life scenarios for troops on the ground will make it much easier to deliver targeted training across multiple soldiers and equip the military to deal with the complexities of a multi-domain environment and an increasingly congested Electromagnetic Spectrum.

www.quadsat.com

QUADSAT

Hera Testing

The rectangular, radar-bearing Juventas CubeSat seen part-deployed from the top of its Hera mission mothership, inside ESA's space-like Maxwell chamber for electromagnetic compatibility testing.

The foam pyramids seen around Hera absorb radio signals, while the 9 meter high metal walls of the Maxwell chamber keep out all external radio interference. The result is a space that mimics the infinite void of space. This allows the Hera team to validate how the spacecraft will interact with its two CubeSats through its ***Low Gain Antenna*** (*projecting top left*), while simultaneously maintaining contact back with Earth through its large, dish-shaped ***High Gain Antenna*** (*lower left*).

"We're testing that Hera can communicate with its CubeSats while also talking to Earth, without unexpected interference," said Hera systems engineer Franco Perez Lissi. "Accordingly Hera's mission control team at ESA's European Space Operations Centre, ESOC, in Darmstadt, Germany, is also talking directly with the spacecraft for the first time, through the High Gain Antenna, just as they will when the mission is in space."

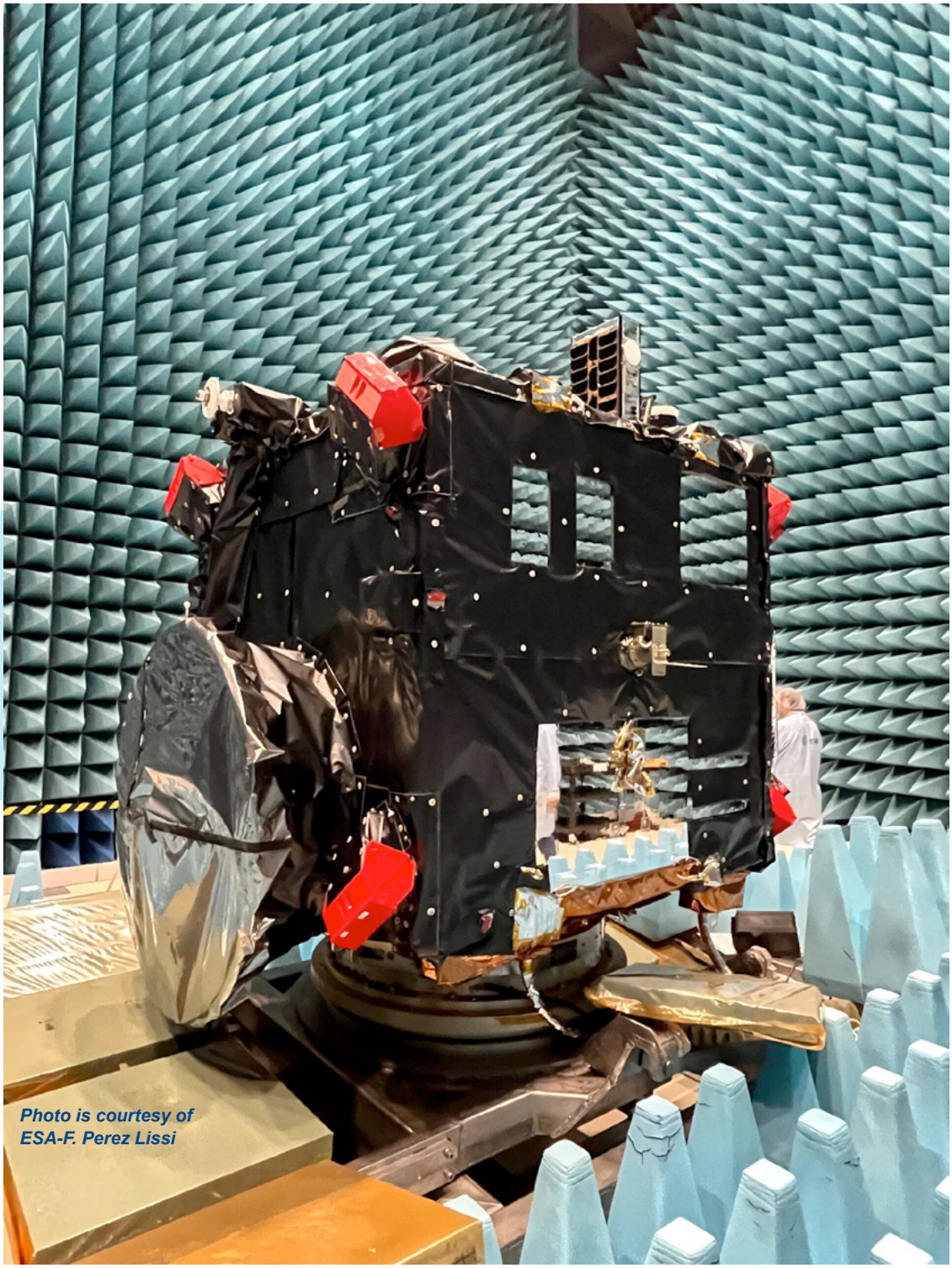


Photo is courtesy of ESA-F. Perez Lissi

Hera is ESA's first mission for planetary defence. Due for launch in October this year, Hera will fly to the ***Didymos*** binary asteroid system in deep space to perform a close-up survey of the Dimorphos moonlet in orbit around the primary body. The Great-Pyramid-sized Dimorphos is already historic, as the first Solar System object to have its orbit changed by human activity, by the 2022 impact of ***NASA's DART*** mission.

Hera is intended to gather crucial missing data about Dimorphos for scientists, to turn DART's grand-scale experiment into a well-understood and potentially repeatable planetary defence technique. To increase its yield of data, Hera carries with it ESA's first deep space CubeSats, carrying additional instruments and planned to fly closer to the asteroid's surface than the main spacecraft, beforeeventually landing.

The ***Juventas CubeSat*** carries a radar instrument, to perform the first radar probe of an asteroid's internal structure, along with a gravity-detecting gravimeter. Its ***Milani*** counterpart hosts a multispectral imager to survey surface mineralogy as well as a dust surveyor.

In addition, the inter-satellite links connecting both CubeSats with Hera will enable greater accuracy in Hera's measurement of Dimorphos's mass, by analysing gravity-driven Doppler shifts occurring between the trio.

"Our testing of how Hera works with its CubeSats starts with the initial deployment process, which occurs differently from that of any standard CubeSat," said Franco. "The Deep Space Deployer on Hera's topside 'Asteroid Deck' part releases each CubeSat, so it emerges from the spacecraft but still has power and data tethers connecting it. This will allow us to check the CubeSat is fully operational, and its radio link with Hera works as needed, before each one is fully deployed into space around a day later, to begin its own mission."

Once this initial phase is completed, the testing will proceed to simulate the communications of the CubeSats in free flight back with Hera.

Defense Threat Reduction Agency contracts for combating weapons of mass destruction

Applied Research Associates Inc., Albuquerque, New Mexico (HDTRA124D0002); Booz Allen Hamilton Inc., McLean, Virginia (HDTRA124D0003); Leidos Inc., Reston, Virginia (HDTRA124D0004) + (HDTRA124D0008 ; Peraton Inc., Herndon, Virginia (HDTRA124D0005); SRC Inc., North Syracuse, New York (HDTRA124D0006); Two Six Labs LLC (*doing business as Two Six Technologies****), Arlington, Virginia (HDTRA124D0007); Parsons Government Services Inc., Centreville, Virginia (HDTRA124D0010); and Signalscape Inc., Cary, North Carolina (HDTRA124D0011), all were awarded a multiple award, indefinite-delivery/indefinite-quantity contract with a maximum cumulative ceiling of $4,000,000,000 for the Defense Threat Reduction Agency's (DTRA) Research and Development Directorate.***

This contract provides for performing research, development, test and evaluation, procurement, maintenance, support, systems engineering and/or sustainment to provide scientific and technological solutions to meet the Department of Defense's priority Combating Weapons of Mass Destruction objectives.

Work under this program is divided into three pools: artificial intelligence, machine learning, data science, and software development…

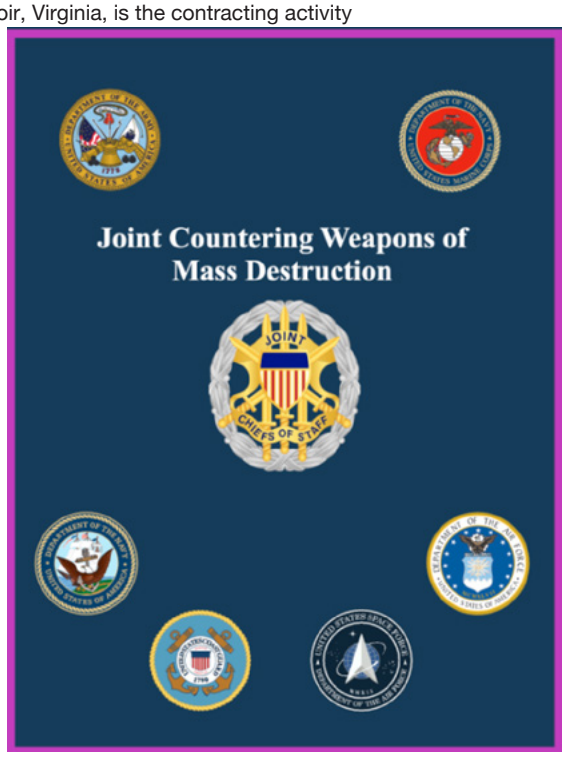
1. ***Pool 1: artificial intelligence, machine learning, data science, and software development***
2. ***Pool 2: operations and countermeasures in a chemical, biological, radiological, and nuclear environment***
3. ***Pool 3: targeting, information operations and irregular warfare***

The maximum ceiling value applies to all awards issued under all three pools. Fiscal 2024 research, development, test and evaluation funding in the amount of $500,000 ($50,000 minimum guarantee per contract) will be obligated at the time of award and will expire at the end of fiscal 2025.

All other funding will be obligated as task orders are issued using research, development, test and evaluation; operations and maintenance; procurement; and other funding. Work locations will be determined at the task order level.

The contract will include a five-year base ordering period and a five-year optional ordering period. The ordering period will go through May 2029; if all options are exercised, the ordering period will go through May 2034. This award is the result of a full and open competitive acquisition.

Proposals were solicited through SAM.gov and 27 offers were received. DTRA, Fort Belvoir, Virginia, is the contracting activity



The U.S. Army continues to invest in CIRCM's always on technology, pictured above the rear wheels of the CH-47. (Photo Credit: U.S. Army)

Northrop Grumman delivers 500th Common Infrared Countermeasures (CIRCM) shipset to the Army

Knowing your team "has your back" is reassuring on any level, but it carries even more significance for warfighters embarking on a mission.

For pilots flying through contested airspace, where hidden enemy missiles below are designed to destroy what's flying above, a well-established, advanced survivability system silently protects warfighters.

> *"I saw the plume, the corkscrew trail, and then [an incoming enemy missile] took a sharp turn and crashed into the ground."*

That is what *Kyle Freundl* recalls from a conversation he had with one pilot telling him about how a product within ***Northrop Grumman's Infrared Countermeasures (IRCM)*** suite protected against an incoming missile fired at his aircraft during a combat mission. Prior to his current role at Northrop Grumman, Freundl served in the U.S. Air Force as an aircraft survivability and systems engineer. His mission then and now covers the same vital key points.

> *"Our job is to save lives and bring our warfighters home. Their mission success is our success," said Freundl.*

COMMON INFRARED COUNTERMEASURES SYSTEM

IRCM refers to a variety of systems designed to protect aircraft from ***infrared homing*** (IR) missiles. These missiles are designed to lock onto heat, such as emissions from aircraft engines, and steer the missile toward that energy. IR missiles are increasingly abundant and dangerous, posing a major threat to military aircraft.

Northrop Grumman has yielded five generations of IRCM protection, including today's CIRCM system — the lightweight, next-generation aircraft survivability system that's a trusted technology of the U.S. Army and approved for export.

Northrop Grumman recently received a $174 million production order — its fourth yearly CIRCM award from the U.S. Army —and has delivered on each commitment by providing all systems on time. After delivering the 500th CIRCM

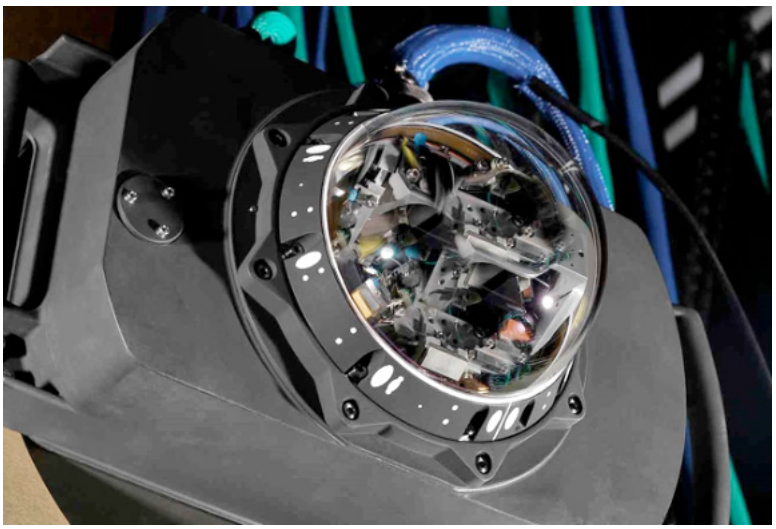


Photo of Northrop Grumman's CIRCM shipset.

shipset, Northrop Grumman has another 336 on order – bringing this always on, mostly unseen technology to more than 800 aircraft in total.

Where CIRCM excels is meeting the challenging size, weight and power restrictions of smaller airframes — specifically rotary wing, tiltrotor and small fixed-wing aircraft. CIRCM technology has provided more than 30,000 operational flight hours of safe passage across the U.S. Army's AH-64, CH-47 and UH-60 aircraft.

SILICON VALLEY

SPACE WEEK

OCTOBER 21-24, 2024

SATELLITE INNOVATION

October 21 - 22, 2024
SATINNOVATION.COM

&

MILSAT SYMPOSIUM

October 23 - 24, 2024
MILSATSHOW.COM

Hosted back-to-back, two premier satellite industry events maximize output from your valuable time.

Focused on analyzing next-generation satellite technologies and the current business environment, **Satellite Innovation** runs October 21-22, 2024.

Providing deep insight into dynamic solutions in space defense the **MilSat Symposium** constitutes the latter half of **Silicon Valley Space Week (SVSW)**. Join the MilSat Symposium October 23-24 2024.

SVSW.EVENTS