SATCOM For Net-Centric Warfare January 2014

MilsatMagazine

ISR + Cybersecurity

AFSC's General Shelton, Future Of Air Force Cyber

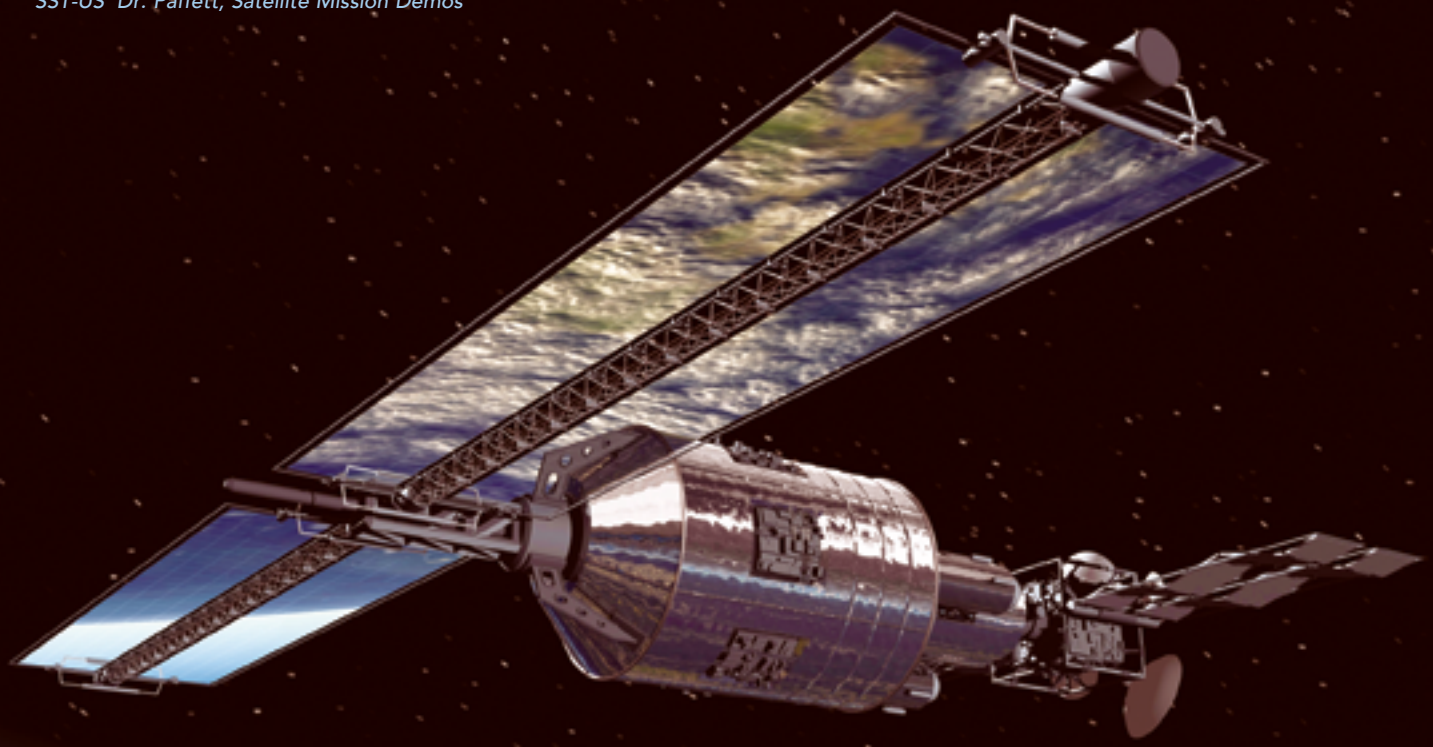
General Skinner, AFCYBER, Cyberspace Weapon Systems

iGT's Fuchs on ISR Challenges for Airborne

Integraph's Blues on Activities-Based Intelligence

Globalstar's Navarra, COMMAND CENTER interview

SST-US' Dr. Paffett, Satellite Mission Demos



When You Really Need It To Work... When You Really Need It To Be There...

Type Approved
AvL Antennas
85cm, 1.0M,
1.2M

Professional

Developed by satellite antenna engineers with over 300 years total experience

Reliable

Over 18 years of production and 18,000+ units in the field

Versatile & Affordable

FlyAway or Fly&Drive

AvL TECHNOLOGIES

designs for ultimate performance

www.avltech.com

WALTON DE-ICE

Original De-Icing Systems
- Industry leading hot air de-icing systems.

Snow Shield

Snow Shields
- Passive and heated
- .6 to 6.3m

Ice Quake

The Ultimate Power-Efficient Vibrating De-Icer

New Innovation!

Protecting Networks From Rain, Snow and Ice For Over 30 Years

- The leader in quality and reliability - 30 years of field-proven experience.
- Superior customer service - bar none. Accept no substitutes.
- Turnkey integration, installation, maintenance and tech support.
- Proudly designed and built in the USA.

Walton Enterprises, Inc.
P.O. Box 1328
Riverside, CA 92502 USA

WALTON DE-ICE

+1 (951) 683-0930
sales@de-ice.com
www.de-ice.com

MilsatMagazine

JANUARY 2014

THIS ISSUE'S AUTHORS

Captain Zachary Anderson
Sven Bues
Corporal Corey Dabney
Sergeant Sarah Fiocco
Karl Fuchs
Jim Garamone
Hartley Lesser
Dr. John Paffet
Brigadier General Robert J. Skinner
Senior Airman Michelle Vickers
Pattie Waldt

DISPATCHES

FEATURES

ADVERTISER INDEX

Published 11 times a year by
SatNews Publishers
800 Siesta Way
Sonoma, CA 95476 USA
Phone: (707) 939-9306
Fax: (707) 838-9235

A satellite doesn't run by itself.

It needs the right telemetry, tracking, and control system to do its job, and the right team of professionals to manage that system. With Harris Corporation's OS/COMET®, your mission gets a COTS scalable, customizable, and extensible TT&C solution and Harris people with unparalleled technical expertise to support you.

The OS/COMET® team has more than 30 years' experience in the satellite TT&C business. Put that experience and know-how to work for you, no matter what your satellite mission is.

OS/COMET®: BRINGING RESULTS DOWN TO EARTH.

www.oscomet.com

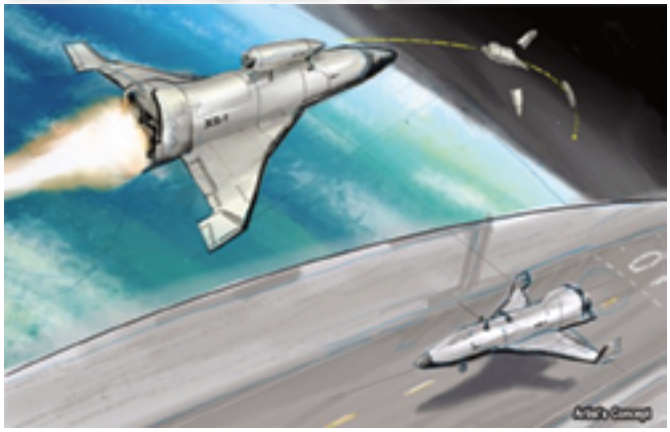
HARRIS®

assuredcommunications®

harris.com

DISPATCHES

DARPA—One Day Access To Space



DARPA's new Experimental Spaceplane (XS-1) program seeks to lower satellite launch costs by developing a reusable hypersonic unmanned vehicle with costs, operation and reliability similar to traditional aircraft.
Artistic rendition is courtesy of DARPA.

Commercial, civilian and military satellites provide crucial real-time information essential to providing strategic national security advantages to the United States.

The current generation of satellite launch vehicles, however, is expensive to operate, often costing hundreds of millions of dollars per flight. Moreover, U.S. launch vehicles fly only a few times each year and normally require scheduling years in advance, making it extremely difficult to deploy satellites without lengthy pre-planning.

Quick, affordable and routine access to space is increasingly critical for U.S. Defense Department operations.

To help address these challenges, DARPA has established the Experimental Spaceplane (XS-1) program.

The program aims to develop a fully reusable unmanned vehicle that would provide aircraft-like access to space. The vehicle is envisioned to operate from a "clean pad" with a small ground crew and no need for expensive specialized infrastructure.

This setup would enable routine daily operations and flights from a wide range of locations.

XS-1 seeks to deploy small satellites faster and more affordably, while demonstrating technology for next-generation space and hypersonic flight for both government and commercial users.

"We want to build off of proven technologies to create a reliable, cost-effective space delivery system with one-day turnaround," said Jess Sponable, DARPA program manager heading XS-1. "How it's configured, how it gets up and how it gets back are pretty much all on the table—we're looking for the most creative yet practical solutions possible."

XS-1 envisions that a reusable first stage would fly to hypersonic speeds at a suborbital altitude. At that point, one or more expendable upper stages would separate and deploy a satellite into Low Earth Orbit.

The reusable hypersonic aircraft would then return to Earth, land and be prepared for the next flight.

Modular components, durable thermal protection systems and automatic launch, flight, and recovery systems should significantly reduce logistical needs, enabling rapid turnaround between flights.

Key XS-1 technical goals include flying 10 times in 10 days, achieving speeds of Mach 10+ at least once and launching a representative payload to orbit.

The program also seeks to reduce the cost of access to space for small (3,000- to 5,000-pound) payloads by at least a factor of 10, to less than $5 million per flight.

XS-1 would complement a current DARPA program already researching satellite launch systems that aim to be faster, more convenient and more affordable: Airborne Launch Assist Space Access (ALASA). ALASA seeks to propel 100-pound satellites into orbit for less than $1 million per launch using low-cost, expendable upper stages launched from conventional aircraft.

Advantech Wireless—A Real Gem

Advantech Wireless Inc. has debuted their new SapphireBlu™ Series 6.6kW C-Band Rackmount UltraLinear™ GaN SSPA/BUC, the ultimate solution for wide bandwidth, ultra high power satellite teleport uplinks.

The new SapphireBlu Series of UltraLinear GaN technology based SSPAs and BUCs from Advantech Wireless are designed for Multi Carrier Operations and offer the highest linear power available in the market.

These new systems are designed in a compact indoor modular package with Built in Redundancy for maximum link availability.

"Our new high power density, GaN based SSPA concept, offers the maximum power/bandwidth combination. We have already started shipping and completed initial orders," said Cristi Damian, VP Business Development at Advantech Wireless.

"We can now saturate all transponders of an entire satellite and obtain maximum bandwidth/power efficiency. Our customers realize great savings in energy cost, Satellite Bandwidth, CAPEX and OPEX."

The New SapphireBlu Series of UltraLinear GaN technology based SSPAs and BUCs from Advantech Wireless, exceed all barriers between Klystrons, TWTs and SSPAs, backed by over 25 years of Outdoor SSPA design and manufacturing, combined with the traditional Advantech Wireless features.

The Advantech Wireless infosite is located at:
http://www.advantechwireless.com/

Advantech Wireless accredited products and advanced technologies have provided leading-edge innovations for over 20 years. We provide diverse and extensive technologies and products for video and data transmission and proven flexibility for specialized solutions.

The Raptor series of transportable DVB-RCS hubs are turn-key systems which can be deployed in less than 1 hour, to enable a wide range of public and/or private network topologies with satellite interactive terminals.

The AMT 73L was the World's first deployed modem with certified compliance to the MIL-STD-188-165A standard, designed to fulfill two way satellite communication requirements in Defence Satellite Communications Systems (DSCS).

The 25W GaN X-Band BUC is perfectly suited for harsh environments such as man-pack terminal deployments. Constructed in a compact cooling enclosure for outdoor operation is the smallest fully integrated unit on the market today.

Advantech Wireless' S5920M Ruggedized VSAT Terminal is a complete DVB-RCS modem that can be used in very harsh environment as in military and desert operations. The RAR9160 Ruggedized Router is designed to provide best in class performance for critical applications under harsh environments.

Advantech Wireless KR Series products empower system integrators to address US and allied defense departments and government agencies with rapid, reliable, secure, global satellite & wireless communications networks abilities.

X-Band 25W GaN BUC
for man-pack terminals

X-Band 300W / 600W
GaN BUC G-Series

Raptor - DVB-RCS
Compact Transportable Hub

S5920M Ruggedized
DVB-RCS VSAT Terminal

KR Series - WBR-2000
Mobile Wireless WAN or LAN

Ruggedized Router
RAR9160

Solid State
Pulse Amplifier

AMT 73L Modem
DISA CERTIFIED

Advantech
Wireless

www.AdvantechWireless.com/gov

DISPATCHES

KVH Industries—Cutter Completion

KVH Industries, Inc., has surpassed the 100-vessel mark in its 10-year contract to supply the next-generation satellite communications solution for the U.S. Coast Guard's fleet of small cutters.

To date, KVH's TracPhone V7 systems have been deployed on 105 USCG vessels across eight different classes of cutters, and KVH's mini-VSAT Broadband service has provided 29.2 terabytes of data and more than 835,000 Voice over Internet Protocol (VoIP) minutes.

The contract for hardware, airtime, and support was first announced in September 2010. KVH systems are now in use on cutters in all U.S. Coast Guard districts in the continental U.S., as well as overseas in the Persian Gulf, Guam, and Puerto Rico.

A cutter is a USCG designation or any vessel over 65 feet in length, including coastal patrol boats, seagoing buoy tenders, and fast-response cutters.

This diverse range of platforms supports a variety of critical USCG operations including drug interdiction, maritime border security, anti-piracy tasks, search and rescue operations, and humanitarian efforts.

The low latency of the KVH service is particularly important to the fast and efficient processing of biometric information from vessel to shore, a key to immigration and law enforcement activities.

The 24/7 nature of USCG operations and the extreme sea and weather conditions in which these relatively small vessels operate are proof of the durability and reliability of the TracPhone V7 and mini-VSAT Broadband service.

"In the face of rapidly expanding data communications requirements, including real-time use of biometric technology, homeland security efforts, and extended worldwide operations, the U.S. Coast Guard needed a global communications solution robust enough to support these demands and rugged enough for even the most demanding maritime conditions," said Martin Kits van Heyningen, KVH's chief executive officer. "Affordability was a critical factor for the U.S. Coast Guard as well, and our mini-VSAT Broadband network offers a cost-effective solution to replace expensive legacy services and still provide global coverage."

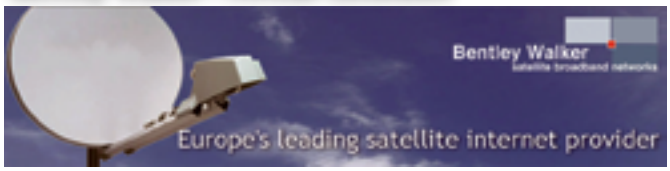
In announcing the 10-year Indefinite Delivery/Indefinite Quantity (IDIQ) contract, valued at approximately $42 million, in September 2010, the U.S. Coast Guard Telecommunications and Information Systems Command (TISCOM) named KVH's TracPhone V7 and mini-VSAT Broadband service as the U.S. Coast Guard's Small Cutter Connectivity (SCC) Ku-band System and Air Time Support Services solution.

The SCC program is part of the U.S. Coast Guard's initiative to upgrade the legacy cutter fleet's commercial satellite systems in order to provide improved communication capabilities for voice and data transmission and reception, as well as improving interoperability with Department of Homeland Security and Department of Defense partners. Supporting KVH in this multi-year effort are network partner ViaSat, Inc., and logistics partner Mackay Communications.

In addition to the deployment of TracPhone V7 on the U.S. Coast Guard cutters, KVH's mini-VSAT Broadband solution is fielded aboard vessels of the U.S. Navy, joint forces, foreign coalition navies, state emergency service organizations, and commercial fleets operating worldwide.

KVH infosite:
http://www.kvh.com/

Bentley Walker—African Extension



United Kingdom-based satellite service provider, Bentley Walker, has extended its reach across Africa and the Middle East using Avanti's HYLAS 2 satellite, signing a multimillion dollar contract extension.

By using their Ka-band services across Afghanistan, Iraq, Libya and Zimbabwe, the company has further enhanced its position as one of the most successful satellite service providers in the World.

Anthony Walker, CEO of the company, said, "The flexibility of Avanti's network has given us the opportunity to develop a range of both niche and mass market services at affordable prices. Avanti satellites also provide 100 percent coverage of the key countries that we want to target."

Matthew O'Connor, Chief Operating Office of Avanti, commented: "By being an early mover in both technology adoption and market entry, Bentley Walker is now an established leader within the satellite industry. Avanti's market changing approach has provided the ultimate flexibility and quality to help them address the demands of their multiple markets."

The Bentley Walker infosite is located at:
http://www.bentley-walker.com/

DISPATCHES

ViaSat—Patriot's Outpost Support

ViaSat Inc. will be hosting active duty military men and women at the Farmers Insurance Open as the Presenting Sponsor of the Patriots' Outpost, one of the premier locations for watching the PGA tournament.

The Century Club of San Diego will also be using ViaSat Exede® Enterprise satellite services—technology also used by U.S. military personnel—for networking tournament operations.

The Patriots' Outpost is a private chalet both dedicated to and exclusively available for Active Duty military and their dependents. The Outpost is located on the 14th hole at Torrey Pines Golf Course with beautiful views of the Pacific Ocean. Local heroes are provided complimentary food and beverages as well as a great vantage point to watch the action unfold on one of the closing holes of the tournament.

"Our company's roots are in military satellite communications and network security so we have a deep appreciation of the extraordinary job that our service men and women perform every day," said Rick Baldridge, president and COO of ViaSat. "We're looking forward to showing our gratitude for their service at one of the signature San Diego events of the year."

Exede® Enterprise is a turnkey business networking service with the capacity and flexibility to support anything from a large network to a single user. Powered by ViaSat-1, the most powerful communications satellite ever launched, it delivers high-speed IP access instantly, even in locations without terrestrial networks.

Virtually any location can be connected with service available on-demand anywhere within the nationwide Exede service footprint. The Century Club will use a number of the small, portable Exede terminals—similar in size to a home satellite TV dish—to provide wireless Internet and other communications networking during the PGA TOUR event.

"In the past, wireless networks were costly and not always reliable across property for our communications. Dropping temporary cable is costly and inefficient. Exede service has already provided us with cost-effective connections and no downtime. The mobility of the system allows us to expand its use on-course throughout the PGA TOUR event," said Peter Ripa, Farmers Insurance Open CEO.

The Patriots' Outpost is reserved to Active Duty military and their dependents. However, Retired and Reserve military are provided complimentary General Admission to the Farmers Insurance Open. Please log onto ***http://www.govx.com/e/80*** for more information.

For additional Exede information, access: ***http://www.exede.com/***

DISPATCHES

ViaSat + Harris—Extended Range Ops Demos

ViaSat Inc. and Harris Corp. have completed demonstrations of the upgraded Small Tactical Terminal (STT) KOR-24A in combination with the Harris high-band power amplifier for extended air to ground range operation of both Soldier Radio Waveform (SRW) and Adaptive Networking Wideband Waveform C (ANW2C).

The demonstrations were held in San Diego at the ViaSat facility in Carlsbad and in Huntsville at Redstone Arsenal in early December.

The two-channel STT provides simultaneous 63-watt Link 16 and 50-watt SRW communications in a software-defined radio.

The STT, the first and only fully-certified, two-channel, Link 16 and VHF/UHF radio, includes a range of software-defined VHF/UHF military radio and Link 16 functions.

The terminal is available now to meet program needs for quick turnaround and delivery of units and was recently selected for Apache AH64E Lots 4 and 5. At only 16 pounds, the STT/KOR-24A terminal reduces the size, weight, and power of tactical data link equipment.

Applications include rotary wing and light aircraft, small boats, UAVs, and for ground forces including vehicles and a wide variety of "shelterized" communication nodes.

Additional STT information is available at this direct infopage link: ***http://www.viasat.com/government-communications/data-links/small-tactical-terminal***

Comtech Teleco

Comtech Telecommunications Corp. has announced that its Orlando, Florida-based subsidiary, Comtech Systems, Inc., has received a $4.4 million contract from the Brazilian Military for an upgrade to its satellite network.

In commenting on this important award, Fred Kornberg, President and Chief Executive Officer of Comtech Telecommunications Corp., said, "Our long-standing leadership positions in all facets of communications have firmly established Comtech as the choice for advanced satellite communication solutions. We look forward to continuing to work with the Brazilian Military on this and future opportunities."

Comtech Systems specializes in system design, integration, supply and commissioning of turnkey communication systems including over-the-horizon microwave, line-of-sight microwave and satellite.

Comtech Systems infosite is located at: ***http://www.comtechsystems.com/***

Russia Signs Over Baikonur Ownership For 2016

Baikonur Cosmodrome in Kazakhstan. Photo courtesy of RIA Novosti.

Kazakhstan wants a permanent Russian presence at the Baikonur space center, the head of its space program said on Thursday, after years of argument between Moscow and Astana over Russia's use of the site.

"Neither I nor any sane person in Kazakhstan wants Russia to leave Baikonur. We are partners and allies and at this level of international cooperation it's normal to have joint strategic projects," Talgat Musabaev said in an interview published Thursday by the Izvestia newspaper.

Russian President Vladimir Putin announced last month that the leaders of the two countries had signed a three-year roadmap on the cooperative use of Baikonur.

Musabaev, a former cosmonaut, said if Russia was to leave Baikonur, Kazakhstan would "do everything possible to ensure Baikonur remains a gateway to space."

He claimed Russian resistance to launches of Ukrainian-made Dnepr and Zenit rockets from Baikonur by Kazakhstan and its partners had relaxed following the appointment of Oleg Ostapenko as head of the Russian space agency Roscomos in October.

The newly-signed roadmap with Russia will hand ownership of the new Baiterek launch pad for the Zenit rocket to Kazakhstan, and requires recommendations be made to reduce the ecological impact of Russian heavy-lift Proton rocket launches beginning in 2016, he added.

Proton launches were suspended for three months following the explosion of one of the rockets shortly after liftoff in July that rained blazing, highly toxic propellants on the Kazakh countryside.

Russia is currently building the Vostochny space center in the Far Eastern Amur region, expected to open in 2018, to reduce its dependence on the Baikonur facility, which it leases from Kazakhstan for $115 million annually.

DISPATCHES

US Army—Comms Training In Honduras

U.S. Army Spc. Luis Mitchell practices setting up a satellite communication antenna during a communication exercise (COMMEX) conducted by Joint Task Force-Bravo, Jan. 6, 2014. During the exercise, members of the task force were instructed on the operation of several types of communication equipment, and practiced using the equipment so they will be prepared to use it in a real-world scenario.
U.S. Air Force photo by Capt. Zach Anderson

Several members of Joint Task Force-Bravo received training on the operation of critical communication equipment during a communication exercise (COMMEX) conducted at Sotoa Cano Air Base in Honduras from January 6th through the 7th, 2014.

"The purpose of the exercise was really two-fold," said U.S. Army 1st Lt. Joseph Ramaglia, a communications officer assigned to Joint Task Force-Bravo. "First, we are able to bring up all our equipment and test our communication capabilities on the installation to ensure we are prepared for any operations in the future. The second part was to train communications personnel within each of the MSCs on the functionality of the equipment to ensure they are prepared for future operations as well."

Throughout the exercise, service members received training and familiarization on the operation of the AN/PRC-148 radio, the AN/PRC 152 radio, Broadband Global Area Network (BGAN) system, Land Mobile Radio System (LMR) and Iridium satellite phones.

According to Ramaglia, this type of training is critical for members of the Task Force.

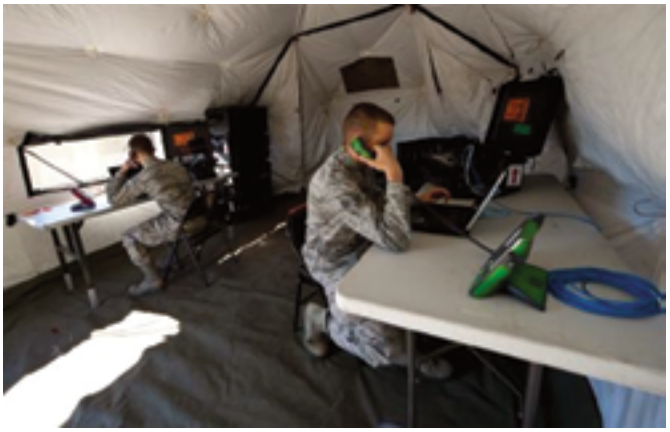
"Everyone on this installation is going to utilize some form of communication equipment at some point during their tour here," said Ramaglia. "It's beneficial for us to ensure we have service members trained and that they are ready to operate and use this equipment when it's required, whether that be during an exercise or in a real-world scenario."

Story by Capt. Zachary Anderson, 931st Air Refueling Group, Joint Task Force Bravo, USAF

DISPATCHES

USAF—No Comm, No Bomb

Senior Airman Brandon Seyl, 1st Special Operations Communications Squadron radio frequency transmissions systems journeyman, adjusts satellite communication systems at Hurlburt Field, Fla., Dec. 12, 2013. The tactical communications flight creates channels so command and control can be conducted. U.S. Air Force photo/Senior Airman Michelle Vickers



Senior Airmen Brandon Seyl, 1st Special Operations Communications Squadron radio frequency transmissions systems journeyman, and Derek Giesbrecht, 1st SOCS cyber transport technician, check phone lines at Hurlburt Field, Fla., Dec. 12, 2013. The tactical communications flight contains everything necessary to establish communications at a remote location for up to 30 days. U.S. Air Force photo/Senior Airman Michelle Vickers

Silence. Picking up the phone or transmitting over a radio to get no response on the other end can be an eerie feeling, especially when airmen deployed to a remote location seek directions on what they need to do, where they need to go, and how to get there.

The 1st Special Operations Communications Squadron's tactical communications flight keeps the lines of communication open in remote locations, whether it's by phone, radio or computer.

"Everything necessary to support deployed communications is self-contained in the flight," said Staff Sgt. Christopher Wessels, 1st SOCS power production craftsman. "We have all the tactical satellites to mobilize quickly out the door to remote locations. We can pretty much operate anywhere."

The tactical communications flight focuses strongly on providing communication support in the deployed environment, while other elements of 1st SOCS focus on base communication infrastructure.

"The three core missions we do here at [the tactical communications] flight are advanced echelon (ADVON) pallet, deploying, and training the younger airmen so they can step up and be in our boots," said Senior Airman Brandon Seyl, 1st SOCS radio frequency transmissions journeyman.

ADVON pallets contain everything airmen need equipment-wise to set up initial communication in a place where there hasn't been time for a site survey.

"Here at the work center, our biggest package is ADVON," Seyl said. "We constantly keep building the pallet up, and if a hurricane or a typhoon hits, we would be able to respond and sustain 30 days out in a remote environment."

To ensure airmen are ready to deploy at a moment's notice, the tactical communications flight performs necessary routine maintenance to their equipment, which ranges from quiet generators to a variety of antennas.

"For the home environment, we're doing preventative maintenance inspections just to make sure the equipment is running properly," Wessels said.

Communication in deployed environments aid commanders in executing missions by enabling them to provide orders. Aircrews also use tactical communication systems to relay messages back to the ground.

"We use radio frequencies to transmit voice and data for commanders in deployed environments, setting up the systems from the ground up," Seyl said. "While deployed, communications are everything. If commanders and aircrew don't have communications, missions can't happen."

Once tactical communications airmen deploy, they can see the vital role they play in a larger mission.

"When you actually go out in the field and you see the operational side, it opens your view to what you're really here for, why you're doing it, and the people you get to help, especially if it's a humanitarian mission," Seyl said.

While the flight places strong emphasis on the deployed mission, training at home station is necessary to equip Airmen for their deployments.

"If you don't know what you're doing, you're not able to set up and maintain networks out in the field," said Senior Airman Derek Geisbert, 1st SOCS cyber transport technician. "Then, people can't get the phone calls they need or intelligence, surveillance and reconnaissance feeds. They can't do any type of command and control if they're basically in a blackout."

Even though Seyl and Geisbert are trainers for their specialties, they both said one of their favorite aspects of their job is the constant hands-on learning.

"I think as new troops come in, it can be challenging to learn to be a trainer," said Tech. Sgt. Scott Fischer, 1st SOCS noncommissioned officer in charge of tactical communication training. "We get new people in and we spin them up, that's a vital part of our culture."

For Wessels, who previously worked at a base civil engineer squadron, the tactical communications flight mission is rewarding and unique in its focus.

"Just knowing we're ready to go at a moment's notice and able to do our job is [the flight's] biggest accomplishment," he said.

Story by Senior Airman Michelle Vickers, Hurlbert Field, USAF

DISPATCHES

USAF—45th Space Wing Ensures Thaicom 6's Launch Success

The Air Force's 45th Space Wing provided support to the successful launch of the Thaicom 6 communications satellite from Space Launch Complex 40 at 5:06 p.m. on January 6th at Cape Canaveral Air Force Station in Florida.

The 45th Space Wing team consists of military personnel, government civilians and contractors provided launch support to the Space Exploration Technologies, or SpaceX, mission, including weather forecasts, launch and range operations, security, safety, and public affairs. (Courtesy photo)

"I am immensely proud of the work of the wing and our mission partners," said Col. Robert Pavelko, the vice commander of the 45th Space Wing, who also served as the launch decision authority.

"This is a tremendous way to open 2014, and we look forward to an exciting launch manifest in the year ahead."

The launch of the Thaicom 6 satellite is the second commercial launch by SpaceX. The satellite will provide C-band and Ku-band communications services across Southeast Asia and Africa.

The satellite will fly in a geostationary orbit approximately 22,000 miles above the Earth's equator.

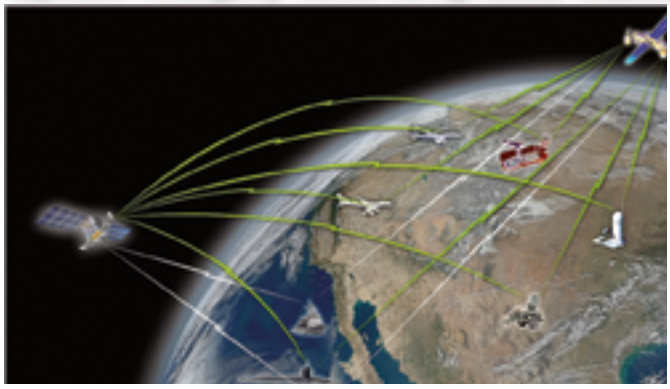
The Falcon 9 launch vehicle flew in the v1.1 configuration with upgraded Merlin 1D engines, stretched fuel tanks, and a payload fairing.

The Thaicom 6 mission was the second launch of the Falcon 9 v.1.1 from Cape Canaveral Air Force Station.

The mission was also SpaceX's second launch of a payload to geostationary orbit.

DISPATCHES

Raytheon—Emergency Comms During Nuclear Missions



Raytheon Company has as new $183 million contract that will find the firm designing and building terminals that are designed to transmit emergency messages to aircrews during nuclear missions.

Raytheon Company is the only provider of fielded Advanced Extremely High Frequency (AEHF) satellite terminals to protect the military's most sensitive information.

The Global Aircrew Strategic Network Terminal (Global ASNT) is part of the nuclear command and control system that allows the President of the United States to direct and manage U.S. forces.

The terminals will be installed at fixed sites, including wing command posts, nuclear task forces and munitions support squadrons, and forward deployed mobile support teams. Fielding is expected to begin in fiscal 2017.

"Our satellite terminals offer strong connectivity and reliability in the harshest of environments," said Scott Whatmough, vice president of Integrated Communication Systems in Raytheon's Space and Airborne Systems business. "Thirty years after we built our first terminal, we're still the only company that provides protected satellite communication terminals at the highest levels."

Raytheon is actively producing AEHF terminals for the U.S. Army, Navy and Air Force.

The terminals have demonstrated interoperable communications using the AEHF satellite's Extended Data Rate (XDR) waveform, one of the military's most complex, low probability of detection, low probability of interception, anti-jam waveforms. XDR moves data more than five times faster than legacy satellite systems.

Raytheon's terminals currently support military operations on older Milstar satellites, and are deployed and ready to operate with the newest AEHF satellites as soon as they are declared operational.

USAF—The Need To Refine Funding Priorities

Budget battles in Washington DC are causing tectonic shifts in the Air Force, the service's leaders said during a Pentagon news conference held in December of 2013.

Acting Air Force Secretary Eric Fanning and Gen. Mark A. Welsh III, Air Force chief of staff, said that even with some relief from sequestration, the service will pay the bills via force structure, modernization and readiness.

How this occurs will affect what the service will look like in 2023, when sequestration ends, they said.

The proposed budget deal making its way through Congress would mitigate some near-term readiness problems, Welsh said, and Air Force leaders will put any money Congress approves beyond sequestration into training and maintenance accounts.

Still, he said, this doesn't change the long-term picture, noting that sequestration poses a "Sophie's Choice" dilemma for the Air Force. Does the service choose to keep near-term readiness high at the expense of force modernization, or vice versa? "That's the balance we're trying to walk," the general said.

One example of this conundrum is the close air support mission. The Air Force is studying proposals on how best to carry out this core mission, the general said. One proposal would eliminate the A-10 Thunderbolt II close air support aircraft—the aircraft Welsh flew as a young pilot.

If money were no object, the A-10 would be a great platform to retain, the general said. But money is tight, he noted, and will be tighter.

"To pay our $12 billion-a-year bill toward sequestration, we have got to find savings in big chunks," Welsh said. "That's the problem. And that's what all these discussions are based on. It's not about a specific platform. It's about balancing the mission sets."

The Air Force ultimately will replace the A-10 with the F-35 Lightning II joint strike fighter, Welsh said. "That plan hasn't changed," he added.

The general said other aircraft—F-16s, B-1s and B-52s—provide roughly 75 percent of the close air support in Afghanistan today. "We have a lot of airplanes that can perform that mission and perform it well," he said. "Those other aircraft do other things for us."

Saving money also is important, he said. "To do that, you have to start talking about fleet divestitures, because you have to get rid of the infrastructure behind the aircraft—the logistics tail, the supply systems, the facilities that do all the logistical support and depot maintenance, et cetera," he said. "That's where you create big savings."

Changing force structure also will change the service, and this is inevitable, Welsh said.

"We will have to draw down people—both the tooth and the tail that comes with that force structure," he added.

Gen. Mark A. Welsh III is Chief of Staff of the U.S. Air Force, Washington, D.C. As Chief, he serves as the senior uniformed Air Force officer responsible for the organization, training and equipping of 690,000 active-duty, Guard, Reserve and civilian forces serving in the United States and overseas. As a member of the Joint Chiefs of Staff, he and other service chiefs function as military advisers to the Secretary of Defense, National Security Council and the President.

Personnel policies will be used to shape the force, and the service is getting these policies out to airmen now so they can make informed decisions, Welsh said.

"We'd love to get all this done with voluntary force-shaping measures over a period of time," he said. "If we ... have to take involuntary measures, I would like everyone to have at least six months of time to talk to their family [and] to think about the impact this could have on them."

Story by Jim Garamone, American Forces Press Service

DISPATCHES

USMC—Working Together To Gain Services During ITX

Most Marines use the Internet and radio frequencies for multiple purposes each day.

In combat situations, Marines use different types of radios to call medical evacuations, logistical resupplies or just get a simple radio check before stepping out on a patrol.

What is often over-looked, are the full capabilities of the radio systems they carry and the Marines who ensure that day-to-day communication is possible.

The Marines serving with the Communication Platoon, 3rd Battalion, 7th Marine Regiment, brought a new array of capabilities to the unit by using both the ANPRC-117G, a wideband tactical radio and the Support Wide Area Network program.

The systems provide the unit with advanced forms of communication while conducting an integrated training exercise. Individually the AN/PRC-117G can attach to a laptop to send data and pictures to one another, and it allows the Marines to chat with one another, said Cpl. Grant Moulden, a field radio operator serving with Headquarters and Service Company, 3rd Battalion, 7th Marine Regiment.

"If a scout sniper is deployed and he comes across someone doing something wrong like burying an improvised explosive device he can connect this lightweight radio unit to a laptop and send photos and data back to his command," said Moulden, 22, a native of Muscoutah, Kan. "Then the sniper can talk to his command about how to deal with the hostile target."

The AN/PRC-117G also has a second capability that uses the Adaptive Networking Wideband Waveform, commonly known as ANW2, to supply the Marines with Internet capabilities, Moulden added. While the AN/PRC-117G is impressive, the (SWAN) adds even more capabilities to the unit.

The (SWAN) is an integrated, IP-based communications system that uses commercial satellite terminals, network baseband equipment, wireless systems and various software to provide deployed Marines with robust communications capabilities.

"Alone. the (SWAN) pulls Internet access from our communications headquarters through specific pre-determined satellites and into our computer," said Cpl. Steven Rice, a data network specialist, serving with the battalion. "Then we add a switch that allows us to push the Internet to our other computers near us using CAT 5 cables (category 5 unshielded twisted pair cables).

Both types of gear working together allows the Marines to do even more. When hooked to the (SWAN), this radio pulls the Internet connection from the satellite through the (SWAN) and into the AN/PRC-117G, Moulden said. Then it distributes the non-classified Internet protocol network (NIPR) and secret classified Internet protocol network (SIPR) to neighboring computers in the network.

Story by Cpl. Corey Dabney, 1st Marine Division, Regional Command Southwest, USMC

DISPATCHES

Northrop Grumman—Cyber Threat Competition

Holding the number one spot in the world for the second consecutive year, a Northrop Grumman Corporation (NYSE:NOC) team of cyber engineers won the overall "grand champion" title in the Defense Cyber Crime Center's (DC3's) eighth annual Digital Forensics Challenge.

The global challenge is a call to the digital forensics community to pioneer new investigative tools, techniques and methodologies to address the dynamic cyber threat.

The challenge encourages innovation from a broad range of individuals, teams and institutions, and recognizes winners in various categories including military, government, commercial, civilian and academia.

In addition to earning the top spot as grand champion, the Northrop Grumman team once again took first prize in the U.S. and commercial categories.

The company's team is also the only U.S. team to have taken first place in the overall competition since it was opened to international participants in 2009.

The 2013 competition exceeded 2012's submissions by 235 percent with 3,182 exercise submissions compared to 1,356 in 2012. Overall, there were 1,254 registered teams from 49 US states and 49 countries.

"We are very proud of our world-class team of cyber professionals who have proven the importance of rapid innovation to address the ever-changing cyber threat," said Jim Myers, vice president and general manager, cyber solutions division, Northrop Grumman Information Systems. "This competition validates the breadth and depth of talent we have at Northrop Grumman and reconfirms our continued commitment to cyber workforce development."

The 10-½ month contest started in December 2012. The challenge consisted of 41 individual scenario-based exercises organized into five levels of difficulty. They ranged from basic digital forensics, or "novice-level," to "developer-level," where advanced tool development was required to solve the exercise and earn points.

Teams were free to select which of the exercises to work on and submit for grading. The following is a link to DC3 challenge leaderboard: ***http://www.dc3.mil/challenge/2013/stats/leaderboard.php***.

Team members researched solutions and, in some cases, developed new techniques to solve specific problems. This year, the team focused on forensics tool development exercises, Windows system forensics, as well as encryption.

The DC3 sets standards for digital evidence processing, analysis and diagnostics for any Department of Defense (DOD) investigation that requires computer forensic support to detect enhance or recover digital media, including audio and video.

The center assists in criminal, counterintelligence, counterterrorism and fraud investigations of the Defense Criminal Investigative Organizations and DOD counterintelligence activities. It also supports safety investigations and inspector general and commander-directed inquiries. For more on DC3 and the challenge, go to ***www.dc3.mil***.

Northrop Grumman is committed to building a world-class cyber workforce. Among the company's numerous cyber initiatives related to science, technology, engineering and math, the Northrop Grumman Foundation supports CyberPatriot, the national youth cyber education competition and the University of Maryland Baltimore County (UMBC) CyberScholars program.

The corporation supports the University of Maryland Advanced Cybersecurity Experience for Students program, leads the Cybersecurity Research Consortium, is partnered with the UMBC Research Park Corporation on the Cync incubator program, and operates its own Cyber Academy.

USMC—Comms Flow During Steel Knight

Lance Cpl. Jacob Turnage, data network specialist, Headquarters Company, Combat Logistics Regiment 1, 1st Marine Logistics Group, secures the cords connected to the Support Wide Area Network transmitter aboard Marine Corps Air Ground Combat Center Twentynine Palms, Calif., during Exercise Steel Knight 2014. The SWAN transmitter connects to a satellite for comms services.

A radio check as a unit heads out on a mission, scheduling a convoy by phone or sending an email to confirm a supply drop in the field might seem like easily accomplished communication, but there is more to it than meets the eye.

Telecommunication, data and radio operator Marines worked quickly to get these communications up and running in time for the start of Exercise Steel Knight 2014 aboard Marine Corps Air Ground Combat Center Twentynine Palms, Calif., and accomplished that mission in only one day, supporting more than 500 Marines and sailors.

"We've set up different phone lines within the command operations center, the forward operating bases and the headquarters tent," said Sgt. Ebony Tatum, telecommunications supervisor, Headquarters Company, Combat Logistics Regiment 1, 1st Marine Logistics Group, and a Fort Washington, Md., native. "We also set up fiber lines with 1st Marine Division, so we can communicate with them as well as other 1st MLG units."

The ability to make phone calls is just one of the capabilities these communications Marines provide in the field. Data Marines set up the Support Wide Area Network in order to get other services, such as email, up and working.

"First we have to get the [transmitter] up that connects to the satellite in the sky," said Lance Cpl. Brenden Salinas, data network specialist, HQ Co., CLR-1, 1st MLG. "After that, we can turn on our servers and communicate with other units."

Salinas' job goes further than just making sure the network is up and running in a timely fashion. When he's not ensuring the overall communication abilities of CLR-1 are working in the field, he's troubleshooting computer issues for individual Marines and sailors.

"I'm working the help desk," said Salinas, of Westbend, Wis. "When someone's computer doesn't work or they can't send emails, I find a way to fix the problem."

While the telecommunication and data Marines are setting up transmitters and phone lines, the radio Marines already have the initial form of communication operating.

"We set up the first line of communication," said Lance Cpl. James Biggs, radio operator, HQ Co., CLR-1, 1st MLG. "We just put our antennas up really quickly, and we're ready to go. We connect those antennas to the COC, so that they can hear everything that's going on."

Not only do radio Marines provide the COC with another communication outlet, they also set up an electronic tracker that allows the COC to see exactly what is happening on convoys.

"We track the vehicles on a GPS, so we can see where they are. We can't really coordinate anything unless we know where they're at," said Biggs, of Atlanta, Ga. "We also make sure convoys do not go near any live-fire areas during the exercise."

Combined, the MAGTF is able to deploy and respond in a timely manner to any situation across the globe.

Story by Sgt. Sarah Fiocco, 1st Marines Logistics Group, USMC

DEFINING THE FUTURE OF AIR FORCE CYBER

By General William L. Shelton, Commander, Air Force Space Command

In December of 2013, General Shelton spoke before the AFCEA NOVA Chapter on Air Force IT Day. Our thanks to AFSPC/PA Operations and Captain Chris Sukach and Anthony Roarke for forwarding to MilsatMagazine the transcription of his presentation.

"It's always challenging to speak to such a diverse audience, one that understands implicitly how important our space and cyber capabilities are for joint warfighting and for our economic well-being.

And I think this audience will agree, space and cyber capabilities have changed the form of modern warfare... and they will become more important over the long-haul... as such, we have to ensure they are preserved."

"As Secretary of Defense Chuck Hagel recently acknowledged, '*As our potential adversaries invest in more sophisticated capabilities and seek to frustrate our military's traditional advantages, including our freedom of action and access, it will be important to maintain our decisive technological edge.*'

"I completely agree with the SecDef…we must maintain our edge... our Nation can't afford to surrender our lead in space and cyber.

"But I don't want to focus my comments today on the budget issues. Quite frankly, I'm tired of thinking about it, tired of losing sleep over it, and tired of living it.

Gen. William L. Shelton is Commander, Air Force Space Command, Peterson Air Force Base, Colorado. He is responsible for organizing, equipping, training and maintaining mission-ready space and cyberspace forces and capabilities for North American Aerospace Defense Command, U.S. Strategic Command and other combatant commands around the world.

General Shelton oversees Air Force network operations; manages a global network of satellite command and control, communications, missile warning and space launch facilities; and is responsible for space system development and acquisition. He leads more than 42,000 professionals assigned to 134 locations worldwide.

General Shelton entered the Air Force in 1976 as a graduate of the U.S. Air Force Academy. He has served in various assignments, including research and development testing, space operations and staff work.

The general has commanded at the squadron, group, wing and numbered air force levels, and served on the staffs at major command headquarters, Air Force headquarters and the Office of the Secretary of Defense.

Prior to assuming his current position, General Shelton was the Assistant Vice Chief of Staff and Director, Air Staff, U.S. Air Force, the Pentagon, Washington, D.C.

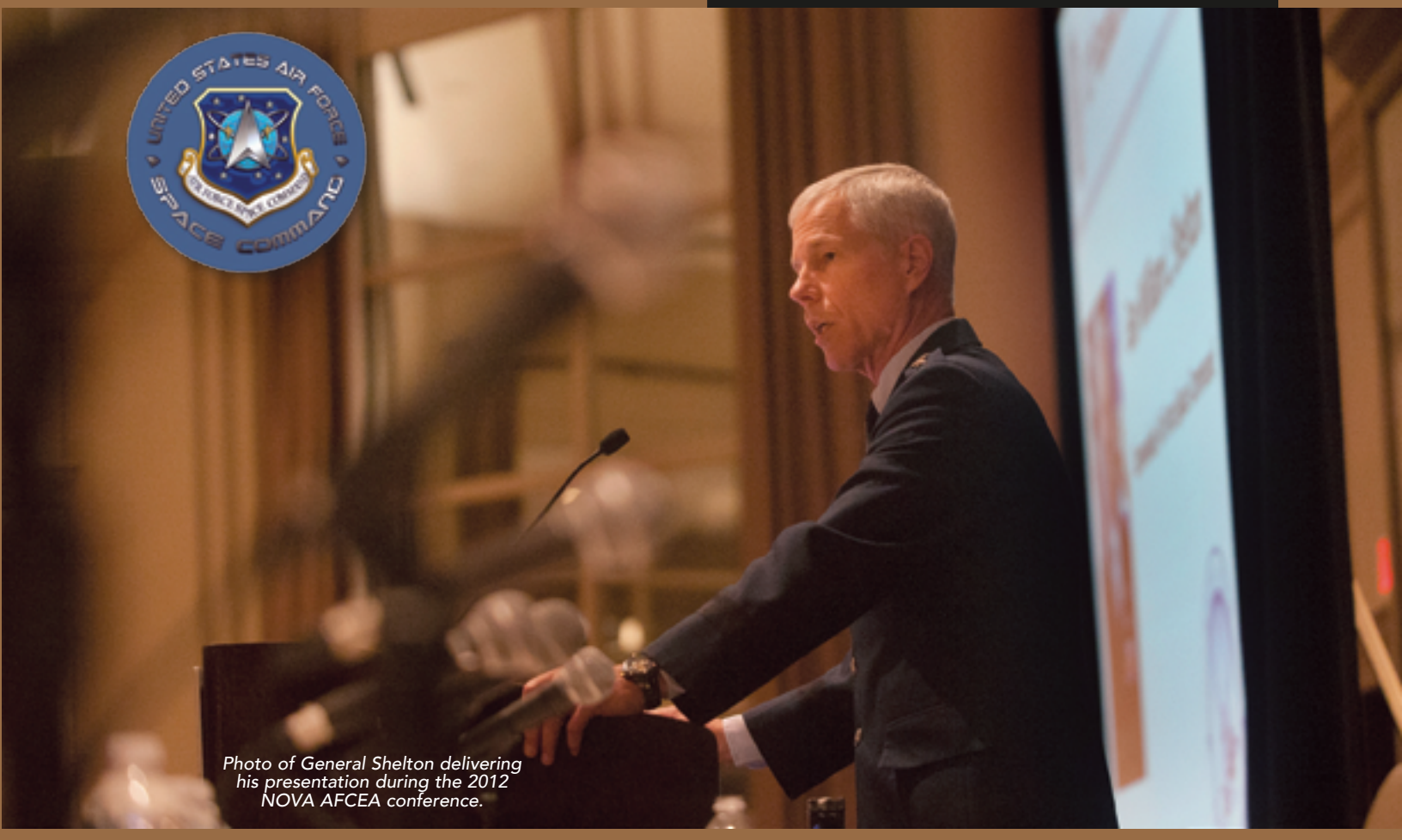


Photo of General Shelton delivering his presentation during the 2012 NOVA AFCEA conference.

"So, instead, I'd rather talk about a much happier subject: What our AFSPC Airmen are doing to lead the way, helping to ensure our Air Force remains the greatest air, space and cyberspace force in the world.

"I'll talk about cyber, what my command is working on today and into the future. I'll be jumping around on several different subjects, so please hang with me.

"Let's start with what I assert as a given—space and cyber capabilities are absolutely foundational to America's future... our military, our industry, our freedom of action... you name it... they touch everything. Militarily, space and cyber capabilities enable seamless command and control, global surveillance and precision targeting, among many other things. If you think about it, our Air Force has been at war for nearly 23 years, starting with Northern and Southern Watch, right through Desert Storm.

"During that time we've stitched space and cyber into the fabric of joint operations and created a synergy that has changed modern warfare. Our own mental model has shifted, as planners now actively consider the full space and cyber toolkit.

"Our potential adversaries have been watching us these 23 years, and they have gone to school on our space- and cyber-enabled modern warfare. And our dependence on these domains yields a corresponding vulnerability for adversaries to exploit.

"I think it's fair to say that without a doubt, they will challenge us in space and cyberspace.

"As our dependence has grown, both domains have become increasingly contested. And in cyberspace the threats have grown both in quantity and sophistication—denial of service attacks, malicious code, direct attack on critical infrastructure, and theft of intellectual capital... these are all serious problems we face.

"And as many of you have heard me say before, the price of admission to be a contender in the cyber domain is very cheap…literally a computer, an Internet connection and some software savvy and you're in.

"The adversaries we face in cyber come from a troubling mixture of backgrounds and agendas—state sponsored hackers, actors with an ideological agenda, criminals and probably most troubling to patriots… insiders.

"The threats are sometimes very obvious and discoverable, and sometimes very insidious and difficult to detect…and we have to be ready for both. Which is why conferences like this are so important--we must be able to operate in, defend, and fight through the challenges in the cyber domain.

"To be successful, we'll all need to think very deliberately on how to counter these threats and how to ensure cyber mission accomplishment, even in the face of attacks.

"Let me say that a different way: Even when challenged, our data MUST get through, it must be timely, and it must be valid. True for C2 data, intel products, TPFDDs, Air Tasking Orders—you name it.

"While denial of service is scary, so would be discovery of manipulated data in our networks during conflict. The corresponding lack of trust that would follow would result in much confusion and at minimum, delays in our ability to prosecute the fight.

"The Airmen in my command are leading the charge in these areas and working through sophisticated defense methodologies. We're using the standard approach to defense, which starts with Defended Asset Lists provided to us by our users.

"And, by the way, we can all agree that the cyber domain is a very different animal, but we're increasingly finding that application of tried and true military processes pay dividends in the cyber domain as well.

"So, let me shift gears and talk about some things we're doing to try to normalize cyber ops in our AF.

"Normalizing cyber operations has been a challenge because as some of you have experienced first-hand, cyber's genesis was disparate networks with inconsistent resourcing and very disparate roles and responsibilities.

"Networks grew up base by base with an eye mainly to each base's mission. Eventually, as MAJCOMs took ownership, there was a beginning to enterprise oversight, but it stopped at MAJCOM boundaries. We still had no enterprise, a lack of standards, configuration control and most importantly: Zero enterprise-wide situational awareness.

"This changed somewhat with the standup of the Air Force Network Operations and Security Center, at Barksdale AFB in 2004…at this point we began to see some centralized vulnerability management and enterprise security.

"A great start…but we still had the issue of numerous distinct networks, gateways and program office networks…and we didn't have a good handle on the activities writ large.

"Fast forward to today: AFSPC, 24th Air Force and the Air Force Network Integration Center (AFNIC) have worked hard to consolidate all of these networks into a single Air Force Network…the AFNet.

"We've collapsed 120 different network entry points into 16 gateways and already improved our ability to secure the AFNet, monitor traffic and provide defense-in-depth. So far we've migrated approximately 90 percent of our 275 targeted sites, which equates to just over 580K users.

"We'll be fully consolidated by the spring of next year, and when finished, we'll have a single enterprise network with consistent standards... one that we can defend.

"The user experience will be greatly improved: once migrated, the CAC card allows you to access the AFNet from any AF location—just as if you were at your home base machine. And we can begin to think about enterprise solutions for our users to simplify account management and gain efficiencies.

"What if: When you got your CAC card at BMT or your commissioning source, your account was created and you didn't have to reapply for an account upon every PCS move? Instead, we would provide a website that would allow you to update your account as needed, but no need to spend extra quality time establishing accounts every time you move or go TDY.

"This is but a small sample of what our folks in 24th AF are thinking about, enabled by an enterprise capability and approach.

"As we go forward, there are areas where we'll continue to innovate and shape the enterprise. Our teams are looking at ways to weave in commercial and cloud solutions to meet our enterprise goals. We're looking hard at the "Next Generation Desktop"…commercially provided e-mail, data, voice and collaborative tools…unified capabilities which could save millions of dollars.

"And, we're looking at integrating technology that will make our workforce more productive…like tablets and next generation mobile computing.

"It's no secret that as we envision the future, we have to continue working the "lanes in the road" discussion. In the past, there was no MAJCOM with the lead for cyber, so things defaulted to the Air Staff.

"Now, we at Air Force Space Command have assigned responsibilities for both cyber operations and cyber programs. It's really no different from the air and space domain, if you think about it. Let me use the air domain as an example.

"If we have capability shortfalls in either the CAF or MAF, whether they be weapons systems or infrastructure, we count on ACC and AMC to define the requirements, work those up through the AFROC and JROC, then work closely with the appropriate product center to close the gap. Why would cyber be any different?

"We get a little hung up on definitions of cyber and IT, and getting those definitions clear and agreed upon is absolutely critical, but it turns out we're having a devil of a time reaching consensus.

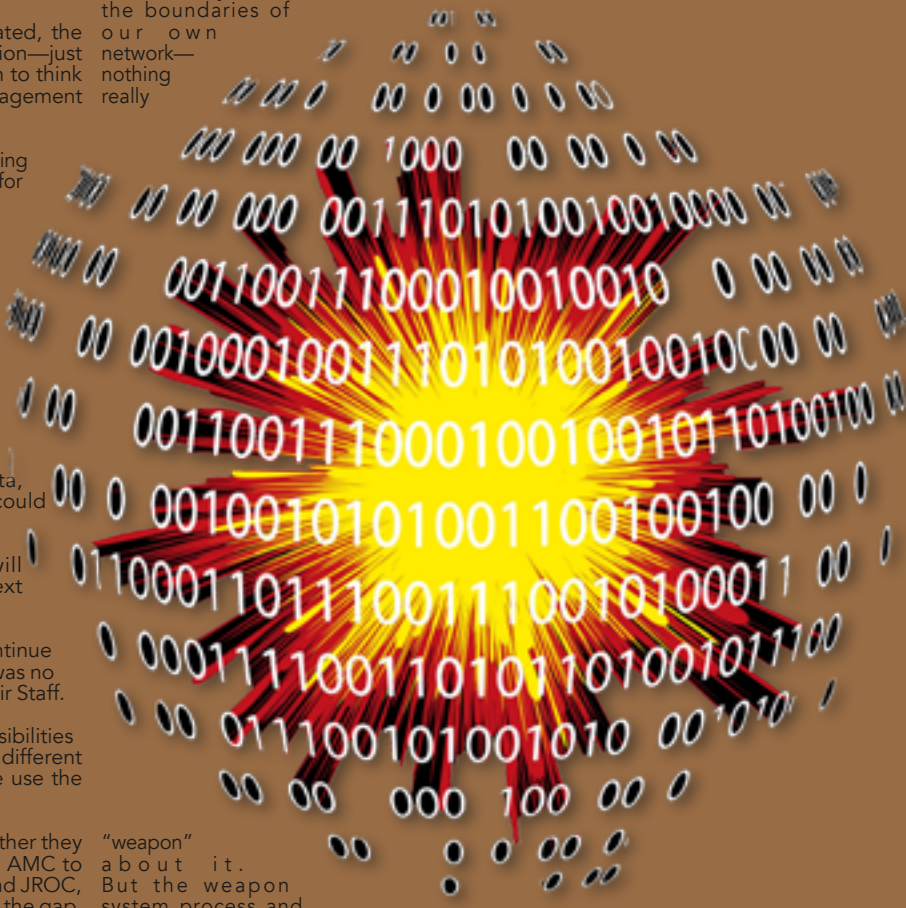
"In AFSPC, we're absolutely focused on providing joint cyber capabilities, which means we have to avoid an IT-minded approach to cyber. Certainly IT provides the great tools and platforms we use, but that is not cyber operations…no more so than the F-22 sitting on the ground is doing air superiority.

"We have to operate in a domain that's *created with IT* to accomplish cyber ops and produce joint warfighting effects. Additionally, conducting cyberspace operations includes having the tools to do the job... like we do for other capabilities in our inventory.

"Earlier this year [2013], we made a significant step when our Chief of Staff declared 6 of our cyber capabilities as weapon systems—another big step toward normalization. If that catches you slightly off guard, please understand, these are not weapons in the conventional sense… we used the proven, standard weapon system construct to establish a business process to drive our investments in this domain.

"Just as the Air Force must invest in, maintain and sustain our air assets, we're using the standard weapon system framework to source our cyber capabilities. For example, for two years now our Airmen have conducted defensive cyberspace operations for Air Mobility Command (AMC) using the CVA/Hunter system, one of those "weapons systems," that's an active cyber-capability that we've invested in.

"It's purely defensive in nature, and it stays within the boundaries of our own network—nothing really "weapon" about it. But the weapon system process and the sustainment discipline and funding protocols that go with it, will help normalize this business.



"Now let me shift gears again on you and talk about our contribution to the Joint Cyber Force. And Cyber Mission Teams are where the rubber meets the road in cyberspace.

"USCYBERCOM recently established a Cyber Mission Force requirement to conduct full spectrum cyberspace operations…this is where our Airmen will provide vital capability for joint cyberspace operations.

"Over the next three years, the Air Force will provide 39 distinct teams to CYBERCOM as our share of the CMF. These cyber mission teams will include National Mission Teams, which defend our nation from strategic cyber-attack; Combat Mission Teams, which support mission execution for combatant commanders, fully integrated with operations in all other domains; and Cyber Protection Teams that provide mission assurance and defend missions in cyberspace.

"I mentioned a few moments ago that our Airmen are conducting defensive cyberspace operations for Air Mobility Command (AMC)… going forward we will extend DCO capabilities to Transportation Command (TRANSCOM) prioritized missions, meeting the needs of General Fraser and his Command.

"When fully operational, we'll have over 2,200 Airmen in 24th Air Force/AFCYBER committed to the Cyber Mission Force. We've already re-cast some of our folks conducting these joint missions.

"Next let me talk briefly about some exciting work we're doing with the Army and DISA on the Joint Information Environment.

"Honestly, we've spent several months doing some important due diligence on JIE implementation. While our commitment to the JIE vision is unwavering, as the AF lead for cyber, I felt it was important to look before we leapt—and it was some good discovery work by a host of people.

"We've now formed a very strong and productive partnership with the Army and DISA and we will begin implementing our Joint Regional Security Stacks early next year….our operational success with our AFNet Gateways has been instrumental to this effort.

"We will also provide enclave control nodes for JIE at 10 of our Air Force bases, integrating the Air Force into the JIE enterprise. And the Air Force has leaned forward with classified Defense Enterprise E-mail…or DEE, and while DEE is not part of the JIE architecture per se, it is a step toward the JIE vision of a single DoD enterprise with centralized services.

"We're still in a due diligence mode on unclassified DEE, working through the cost estimates with DISA. So we're tapped into JIE and partnering to define the single joint enterprise. As with everything else these days, we are looking hard at every aspect of this transition to ensure we gain the resource efficiencies predicted.

"Clearly, combatant commander and warfighting priorities remain the primary focus for all our space and cyber capabilities. And while the United States remains the leading global military power, that status is being challenged every day.

"It's imperative the warfighter trusts the data they receive from our space and cyber systems…anywhere around the globe, 24/7. And as I've said, we need to ensure the data gets from Point A to Point B, through any contested environment.

"Our adversaries will also use cyber to inject themselves in space, wherever they can, particularly at the seams in our capabilities. Cyber-attacks—to deny command and control of our satellites and by interfering with the Air Force Satellite Control Network…let me assure you, we are very concerned about such threats. Our adversaries are looking for accessible single points of failure, and we must harden our systems.

"A watchword in my headquarters is *resiliency*... that's where we're headed with future space and cyber architecture. Resilience means that despite adversary action we still have a capability to present to the joint warfighter.

"Let me give you one example. The Iridium constellation uses 66 satellites in Low Earth Orbit to provide commercial comm and data services. The resiliency of Iridium's constellation was certainly tested when a Russian KOSMOS satellite collided with one of Iridium's satellites in 2009. Despite the loss, the constellation was still able to support users because of the overall resilience inherent in the constellation.

"In stark contrast, the national security MILSATCOM architecture is nowhere near as resilient.

"In fact, with most SATCOM systems, we're often one-deep on capability because it's expensive…we build just enough and just in time. To get to a much more fault tolerant architecture, we're working hard to find the balance between affordability, capability and resilience.

"There are a lot of good ideas on the table right now… discussions between staff in my headquarters, industry and the Space and Missile Center at Los Angeles.

"In fact, we're wrapping up a study that addresses joint warfighting requirements and resiliency in order to project what our future architecture will look like.

"This study is looking at a number of environments to paint the picture. Benign, those with some IO or jamming activity; contested, direct and purposeful kinetic/non-kinetic or IO attack on our systems; and, nuclear, aimed at protected national critical assets to support senior leaders during and after a nuclear event.

"For space and cyber, the reality is that we're facing external threats outside of DoD as well as tough budget challenges from within.

"For the long term, the ripple effects caused by continued sequestration mean uncertainty and a bow wave of bills that will someday come due. As we continue to make headway in cyberspace, the long-term effects of sequestration will challenge us on many levels. We can't continue with the status quo: business as usual...we simply don't have that kind of money.

"But the good news: We are the best Air Force in the world with the best Airmen around…and they're looking at solutions.

"We have a lot of hard work *and* opportunity ahead of us, but it requires us to find answers to some pretty tough questions. It starts with a team of Airmen, contractors, researchers and industry innovation…good ideas from all quarters.

"And speaking of industry, we know that the commercial sector is ahead of the government sector in technology in cyber…so we need to hear from industry. We're putting all ideas on the table, listening to folks from government, industry and those within our command.

"On the people part of this, a lot has also changed in how we prepare our people to conduct cyber missions. For one, we've moved to much higher training standards… there are requisite skills our cyber operators need in order to do the mission. And, we expect a level of preparedness from our cyber operators that didn't exist before…they have to be certified to fly missions in cyberspace.

"And the folks we need in the driver's seat must have the right combinations of tools to head us in the right direction.

"It never ceases to amaze me how much talent our Airmen, contractors and industry partners demonstrate every day.

"We have some challenges and opportunities ahead of us, so we'll need all the talent we can muster. Thanks for the opportunity to speak today. Space and cyber are absolute game changers for modern warfighting. And the demand clearly exceeds our resources. But that doesn't change the fact we're going to continue to lead at the edge in cyber…our Nation depends on it.

"I look forward to where we're headed as an Air Force and as a Nation."

Space—The Ultimate High Ground
General Shelton's Remarks To George Washington University Students

By Jim Garamone, American Forces Press Service

Space is fundamental to the economy, the military and the way of life in the United States and officials must continue to guard against challenges in the domain from adversaries, the commander of Air Force Space Command said on January 8th, 2014, to students at George Washington University in Washington DC.

General William Shelton shared with students at George Washington University some of his worries and concerns regarding space defense for our nation.

In the past 60 years, space has grown from a domain with a lone satellite beeping across the heavens to a $300 billion economic engine.

"The advent of space systems has allowed citizens and governments to engage routinely in the world around them, communicate at the speed of light and to tap sources of information previously unavailable to them," Shelton said.

"Satellites are now essential parts of the 21st century way of life for all nations. Weather forecasting, precise navigation, instant communications and many other capabilities tie space to Earth.

"These are incredibly important during crises. The death tolls from Hurricane Katrina in 2005 and the Japanese tsunami in 2011 would have been even higher, had not satellite surveillance and communications been available," he said.

Space has also changed the military. "In all of recorded history, when armies met on the battle field, they fought for the coveted high ground because of the obvious advantage it gave them over the adversary," Shelton said. "Later, balloons performed that function and even later, airplanes were used as observation platforms."

"Space is the ultimate high ground," he said.

Shelton's Air Force Space Command has a global mission with global responsibilities that reach all corners of the planet and up to 23,000 miles in space and geosynchronous orbit. "We get space-derived information to all sorts of users, including the military operators of our nation's Army, Air Force, Navy and Marines—those who rely on timely and accurate data," he said.

Intelligence, logistics and other operationally relevant data flow seamlessly to the front lines in Afghanistan as well as to other parts of the world where U.S. forces are operating.

"I can't think of a single military operation across the full spectrum, from humanitarian relief operations all the way to major combat operations, that doesn't somehow depend on space for mission success," Shelton said. "But frankly, this dependence on space has also become quite a bit of a double-edged sword. Our potential adversaries have been going to school on us during these many years of combat operations."

Adversaries are mimicking American procedures and looking for chinks in American armor," the general said. "More concerning, as they've watched us, we've watched them develop systems to challenge our advantages in space," he said.

"Because space launch is so expensive, we loaded as much as we could onto our satellites—multiple missions, multiple payloads, " Shelton said. "After all, we were operating in a relatively peaceful sanctuary in space."

Not today.

"As I look at the next 20 years in space, we have a difficult, up-hill climb ahead of us," he said. "I equate this to the difficulty of turning the Queen Mary. You send the rudder a command and the delayed response tries your patience."

To sustain space services, the United States must consider architectural alternatives for future satellite constellations.

"These alternatives must balance required capability, affordability and resilience," he said. "There are many options that we're actively studying right now. The notion of disaggregation is one. And what we mean by this is moving away from the multiple payload, big satellite construct into a less complex satellite architecture with multiple components."

Distributing space payloads across multiple satellite platforms increases U.S. resiliency. "At a minimum, it complicates our adversaries' targeting calculus," he said.

A United Launch Alliance Atlas V rocket carrying a National Reconnaissance Office payload launches from Vandenberg Air Force Base on December 5, 2013, from Space Launch Complex-3 by Team Vandenberg. U.S. Air Force photo/Michael Peterson.

Satnews Publishers readers save £300

SMi Group - The Organisers of Global MilSatCom present the 2nd Annual

MilSatCom Middle East & Africa

24 - 25 February 2014

AMWAJ ROTANA, JUMEIRAH BEACH RESIDENCE, DUBAI

"The leading MilSatCom Middle East Event bringing you in contact with key decision-makers in the MilSatCom Industry"

WHY ATTEND THIS EVENT:

- **Hear** direct from the United Arab Emirates Space Reconnaissance Centre about their projects and benefit from their expertise
- **Learn** about new SatCom projects in the Middle East and where you can invest in the future of satellite technology in this region
- **Get** an insight into the issues faced by the MilSatCom industry including space debris and how to combat it
- **Explore** new developments in SatCom in Africa and network with the Nigerian Navy
- **Investigate** how MilSatCom evolves along the chain from the academic research into the finished working product and how academics can help design the best products
- **Hear** about the future of MilSatCom - Telehealth capability and the benefits for the defence forces

KEYNOTE ADDRESSES FROM:

Brigadier Syed Zulfiqar Ali, Commander, **Strategic Command of Pakistan**

Lieutenant Colonel Ali Alshehhi, Manager, Space Reconnaissance Centre, **UAE Armed Forces**

Colonel Katala, Tanzanian People's Defence Forces

OTHER CONFERENCE SPEAKERS INCLUDE:

Omran Sharaf, Director of Space Image Processing & Analysis, **EIAST**

Nico Stephan, Director and General Manager, **LSE Space ME**

Speaker to be Confirmed, **UK MoD***

Group Captain Lanre Oluwatoyin, Director, Directorate of Space Technology, **Armed Forces of Nigeria**

Sethu Menon, Researcher, **Space Policy Institute**

Dr Mohamed Mahmoud, Researcher, Integrated Systems Engineering Department, **National Authority for Remote Sensing and Space Sciences**

Riaz Lamak, International Director Benchmarking & Validation, **GVF**

Christopher Baugh, President, **Northern Sky Research**

Hannes Potgieter, Product Manager, **VASTech**

Anthony J. Colucci, Vice President Marketing & Sales, **Space Systems Loral**

*Subject to final confirmation

POST CONFERENCE WORKSHOP - 26 FEBRUARY 2014

Flexible, Cost Effective, Multi-Mission Commercial Solutions for Military Forces

Hosted by: **Shady Ahmed Ali,** Business Development Director for MEA at **SatCom Direct** and **Nathan Andrews,** Business Development Manager, **SatCom Direct International**

09.00 - 13.30

SPONSORED BY:

HARRIS CAPROCK · SSL · THALES · VASTech · vocality

REGISTER ONLINE & SAVE £300 - QUOTE SMI6U8P

www.milsatcom-mea.com

Alternatively call us on +44 (0) 20 7827 6000

CPD CERTIFIED

COMMAND CENTER
TONY NAVARRA, GLOBALSTAR SATELLITE COMMUNICATIONS, LLC

MilsatMagazine (MSM)

Mr. Navarra, how did you decide upon a career within the SATCOM industry and, secondly, what drew you to Globalstar?

Tony Navarra

I 'decided' on a SATCOM industry career having been the U.S. Army Officer in charge of providing satellite service to the White House Communication Agency for the President of the United States from 1970 to 1972. Upon leaving the service, I went to work for a major supplier of ground-based satellite communications equipment, Magnavox. From there, I developed space based processors for satellites and ground stations at TRW and, finally, Loral Space and Communications, where I assisted in the formation of Globalstar and have been the President since 2000.

MSM

Please discuss the importance of Globalstar's second generation satellite constellation and how it can be used by the MAG (Military, Aerospace and Government) to ensure mission success, all the while saving lives?

Tony Navarra

The second generation satellite constellation was developed to enhance all the first generation satellite capabilities, services and product features that were used by our military and commercial customers. The second generation satellites and ground infrastructure are significantly increasing the number of features available to MAG users as well as offering the ability to fine tune special features and capabilities for end-users. Increasing the power from the satellites provides significantly higher data rates, going from tens of kilobits to thousands of kilobits, instantly. This really makes a difference operationally and the ability to meet many more applications.

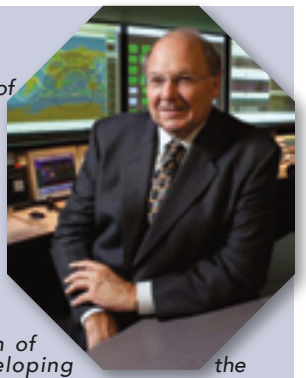
MSM

What are your plans to further introduce Globalstar product into the U.S. military and agency acquisition process? What steps must be taken to ensure you are "heard" by the purchasing authorities?

Tony Navarra

Our plans include working directly with the various services and research laboratories to develop specific software and hardware solutions to meet the needs of the government and the armed forces. We have learned that the best approach in communicating with MAG customers is to develop commercially proven products, and during the commercial launch process, to demonstrate their range of capabilities at the same time sharing sales and service terms with the procurement bodies, such as the U.S. General Services Administration.

The final second generation Globalstar satellite completing its launch preparatons. Photo courtesy of Arianespace.



Anthony J. Navarra is President of Space Operations and Special Projects at Globalstar and has been working with Globalstar for nearly 22 years. Prior to his appointment to his current position in September 1999, Mr. Navarra was executive vice president of strategic development and acting chief operating officer for Globalstar. In this position, Mr. Navarra was responsible for the acquisition of partners for Globalstar, developing the business plan and marketing the company's satellite mobile services. He also oversaw functions of all corporate departments including international business development, marketing, engineering, corporate development and production, finance and administration, regulatory affairs and system applications.

He is currently responsible for the design, development and management of the $ 1.1 billion second generation 48-satellite production and launch contracts with Thales Alenia Space and Arianespace. He continues to manage the control and operations of the first generation satellite constellation which provides SIMPLEX messaging, position location service and voice and data service to the Globalstar ground stations and subscribers.

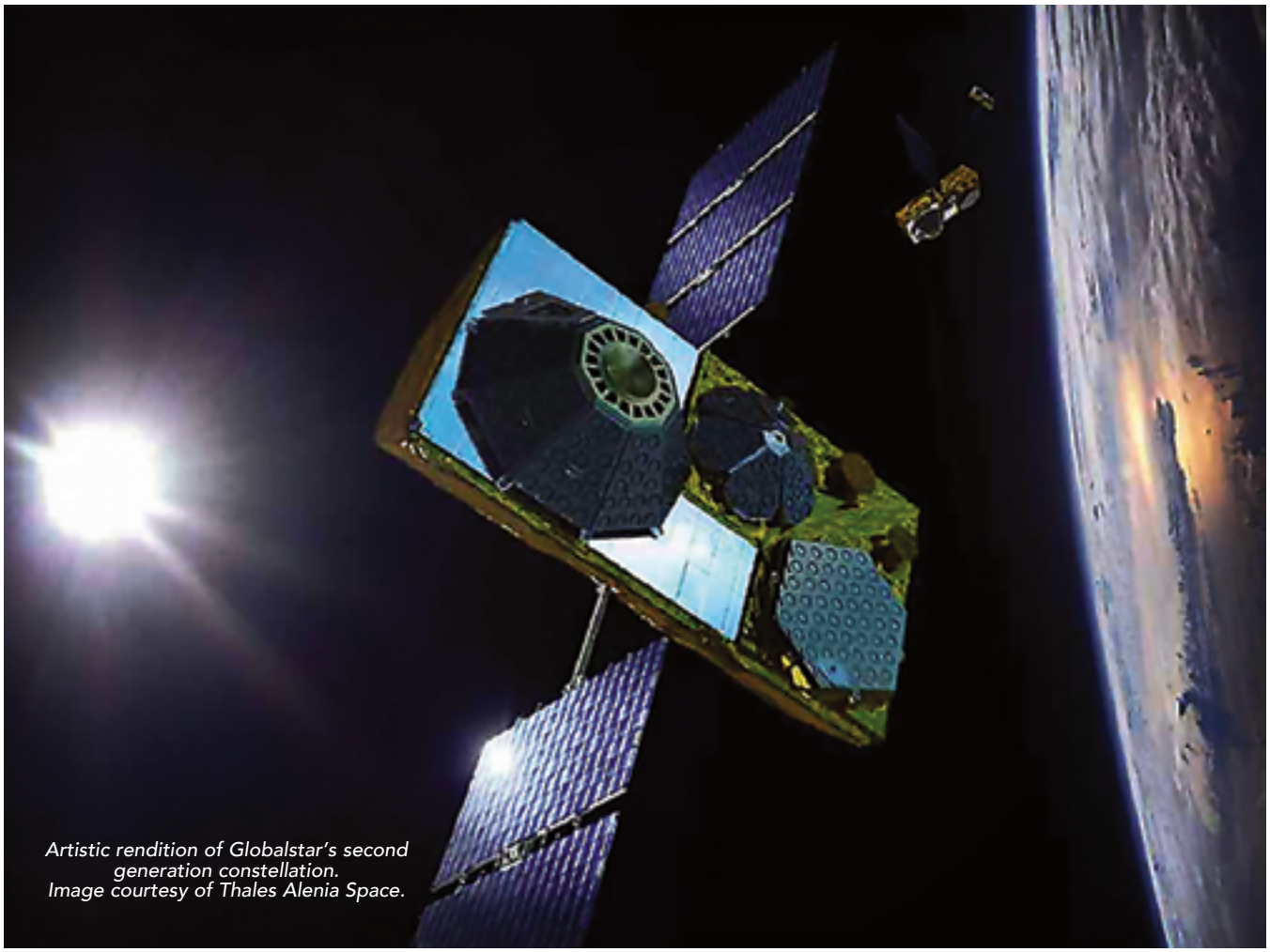
Prior to joining Globalstar in 1987, Mr. Navarra served as marketing vice president at the Rolm MilSpec Computer Division of Loral Corporation, responsible for managing the product development of military computers, high speed mass storage device and satellite communication processors. He developed and manufactured the embedded computers and signal processor for the U.S. Department of Defense advanced data processing program on the Airborne National Command Post for the President of the United States, Air Force One, and various fixed, mobile and airborne satellite terminals.

From 1984 to 1987, Mr. Navarra worked for TRW in Redondo Beach, California, as Business Area Director of satellite terminal development responsible for the antenna technology and development of submarine systems, VHSIC technology based modems for the MILSTAR program and satellite signal processor for the Department of Defense. Prior to that time, Mr. Navarra worked for Magnavox Research Laboratories and Government Electronics Company in Torrance, California from 1972 to 1984.

Mr. Navarra holds a Bachelor of Science degree in Physics from the University of San Francisco and Master of Science degree in Systems Management from the University of Southern California. He received post degree work experience in the theory of Satellite Communications while attending the U.S. Army Signal Corps at Ft. Monmouth, New Jersey. Mr. Navarra has continued post-graduate work at Stanford University in business and management. He continues to provide guest telecommunications courses at the University of San Francisco McClaren Business School and is a member of the USF Telecom Board.

His current responsibilities include the operations of the Globalstar first generation satellite constellation and the delivery and launch of the second generation satellite constellation which was completed in August 2013. Additionally Mr. Navarra continues to grow the telecommunications and special applications for Globalstar in the government and commercial sectors.

He was key in the placement of both Globalstar IPOs in 1993 and 2006 and has participated in many road shows raising 4 billion since 1993. He most recently was instrumental in establishing a French government, CoFace, backed, $504 million loan, from a consortium of French banks in July of 2009.



Artistic rendition of Globalstar's second generation constellation. Image courtesy of Thales Alenia Space.

MSM

Additionally, given the crucial role of NGOs and first responders during horrific disasters (natural and man-made), what can they leverage from the Globalstar constellation to help them with their good works?

Tony Navarra

Globalstar has already successfully demonstrated and sold multiple configurations of our handheld voice and data phones, SPOT (safety and security messaging devices) to hospitals, federal and state governments, first responders and MAG customer groups in emergency and remote configurations that provide satellite and cellular network services at critical facilities worldwide during emergencies.

These products assure that these organizations and facilities remain in contact, linking their network, employees, service personnel and headquarters. More importantly Globalstar's products, service and satellites provide interoperability across many organizations, federal and state, first responders and military services via ground stations which are 1) redundant geographically and 2) located well outside the natural disaster, emergency or area of operations. All of this is aimed at ensuring uninterrupted satellite based communication services.

MSM

What do you recall as the company's—and your—major accomplishments over the 18 years you have been with the firm?

Tony Navarra

The major accomplishments for Globalstar, include the introduction of ground-breaking industrial, commercial and consumer products worldwide as well as products specifically for consumers that deliver affordable voice and data communications and messaging for the safety and security of individuals as well as their property, including buildings, cars, boats and motorcycles. Additionally, launching our second generation of satellites—securing Globalstar services with backward compatible second generation products through at least 2025—this is a major accomplishment for the business and myself personally.

MSM

Why is SIMPLEX an important technology for the company? Please explain some of the products Globalstar offers to support SIMPLEX and what communication challenges this technology solves.

Tony Navarra

Simplex products include SmartOne, SPOT Personal Tracker, SPOT Satellite GPS Messenger, SPOT Gen3 and now, the recently introduced SPOT Trace product. All of these represent a highly reliable, worldwide signaling capability, providing position location and short messages combined with a long battery life, ensuring the safety and security of personnel as well as property.

These products provide real-time messaging to designated computers, cellular phones and smart phones. They help users by swiftly reporting position information, and help get emergency services back to the user. All of this is provided without a cellular or ground network. Rather, Globalstar's unique service is a high quality, CDMA-based, redundant messaging system that assures real-time communications from the Simplex device to the designated user terminal or mobile device, with optimum reliability.

MSM

What are SIMPLEX' capabilities that would, or could, be of interest to militaries and agencies?

Tony Navarra

Our Simplex products, SPOT and Trace products are capable of providing remote status, location and sensor information as

programmed by the MAG. Today, many government organizations are using these devices for important assets that need to be tracked, obtaining real time location information of moving assets.

Additionally, sensor information such as fluid levels is readily available, as well as temperature, and pressure, fire and intrusion alarms. We assist in keeping individuals safe and provide very quick medical assistance or support to individuals, company's employees and provide the basic position location and messaging service to security organizations.

Police, military police, fire fighters and first responders all rely on the capabilities of our network.

MSM

Globalstar offers what the company calls "Extreme Systems." Please explain what these systems are and what roles these products could play in the MAG environment.

Tony Navarra

Our products operate in extreme temperatures and in wet environments, both in water and in inclement weather. Also our solutions perform in environments where there are potential fire or explosive hazards, for example, during the manufacturing, moving and storage of volatile chemicals, munitions and hazardous materials. The MAG will find these products useful in providing personnel safety, facility security and rapid emergency response capabilities.

MSM

You have had a presence in most of the major Globalstar efforts, from its reorganization in 2001 to the launch of the second generation satellite constellation. What will comprise the company's next major efforts during 2014?

Tony Navarra

Globalstar's next major effort will be the completion of our second generation ground station and infrastructure enhancements. Globalstar will continue to provide high quality mobile and fixed voice and data along with our family of Simplex products using the second generation network. In addition to growing our sales in 2014 our focus will be the completion of our second generation products for our customers, delivering more features and at higher data rates.

MSM

As many are aware, there is a "talent" crisis forthcoming for our industry, that being the lack of trained applicants for the various technical positions within companies who need such resources to drive their projects forward. How does Globalstar cope with this need and how can the industry further STEM education within middle and high schools and at the college level? Is Globalstar involved directly in such efforts?

Tony Navarra

Globalstar recruits specialized engineering talent from the Silicon Valley, and also benefits from the universities in the San Francisco Bay Area. We also benefit from our alumni in our offices in California and Louisiana to recruit from their colleges and universities near San Francisco and New Orleans.

MSM

How do we, as an industry, market the potential within SATCOM to students as a career worthy of consideration?

Tony Navarra

In addition to state-of-the-art engineering, we speak with students by sharing our exciting sales and management opportunities in a worldwide business focused upon delivering voice and data communication and navigation services via low Earth orbiting satellites. We emphasize these messages by explaining the personal growth opportunities and career potential of being a part of an organization that has engineering and operations challenges at ground stations and control centers as well as sales and administrative offices around the world.

Globalstar provides many options for upward mobility to corporate headquarters, as well as all of the relationships you make within the industry, working with really talented people and the broad array of experiences that are possible in working with large corporate customers and suppliers. In addition, there are opportunities in related industries using satellite delivered services, *e.g.*, communications, navigation and reconnaissance solutions. The satellite communications industry is populated with people who are technologically and commercially creative, so it's intrinsically interesting. We communicate this whenever we can.

MSM

Given your years of experience in this industry, when you look back over your career, what project or projects truly bring a sense of satisfaction to you?

Tony Navarra

Looking back over the years the most rewarding projects have been the commercial and military upgrades in installations for major customers where early satellite technologies from the 1980s were updated with higher power satellites, ground station equipment and mobile or portable handheld products that even 10 years earlier were not feasible.

We provided a major petrochemical company with a real time position-navigation device with batteries lasting two years to support its worldwide operations. High data rate satcoms equipment was once the size of a refrigerator and now it's the size of a small suitcase or a single drawer. And a satellite phone is now the same size as a cell phone—all of this is remarkable and incredibly satisfying to me.

MSM

What has been the most unexpected change in the MILSATCOM sector in the last year?

Tony Navarra

I am most intrigued by how MAG customers have come to use commercial solutions and to explore hosted payload solutions from commercial satellite operators. They have shown real pragmatism in the use of the rapidly developing capabilities of our satellite technologies as well as our ground stations and terminal equipment.

MSM

What sector developments will be making the headlines in 2014?

Tony Navarra

New satellite technology, higher bandwidth, innovative signal processing along with additional spectrum allocations in 2014 will improve and increase services to the general public, the industry and the military.

MSM

What developments seen in the U.S. market might be seen in other territories around the world?

Tony Navarra

Multi-signal processing by ground infrastructure, gateways and switches will continue to enable U.S. and overseas customers to have multifunctional, navigation, text messaging, web surfing, voice telephony and local hotspot (Wi-Fi and Bluetooth) communications in a single portable device. Competitive pressures will lead to more devices and service providers will provide more products and services with new network capabilities.

MSM

As governments continue to cut military budgets, buyers of communication services need to be ever-more savvy in spending these diminishing funds. What new paradigms, commercial models do you foresee coming into play?

Tony Navarra

Successful deployment of hosted payload solutions and the enhancements of signal compression, increased use of software defined radios and encryption will allow governments to use commercial satellite services through local ground stations. These may become more prevalent. The availability of fiber and wireless broadband will also be a technology driver in the interconnection between the satellite operators and governments' termination points. Also the MAG's need for mobile vs. fixed and/or requiring both services may result in the business model requiring a change in satellite designs and potentially, satellite industry consolidation to meet the needs of commercial customers and governments.

Second generation satellites launch via a Soyuz rocket. Photo courtesy of Globalstar.

ACTIVITIES-BASED INTELLIGENCE + THE NATIONAL SECURITY MISSION

By Sven Bues, Vice President, EMEA Defense & Intelligence Sales, Intergraph

For more than a decade now, the demands of two wars, regional unrest and natural disasters around the world have driven the Intelligence Community (IC) to develop better information pieces to apply to the intelligence puzzle: More useful signals information, satellite imagery, Unmanned Aerial Systems, aerial and satellite full-motion video, multi-camera generation, three-dimensional images, human intelligence and on it goes.

Analysts at fusion desks in Distributed Common Ground Stations assemble these pieces, often in time-consuming processes, to create a Geospatial Intelligence picture. However, Big Data threatens to swamp the process and its practitioners, generating a need for dynamic tools that automate and enhance data preparation, allowing the specialists to apply more of their time to analysis.

The Activity-Based Intelligence (ABI) paradigm has emerged to solve this problem. Built on the geospatial intelligence foundation, ABI can take today's picture of the enemy over the hill or around the urban corner and combine it with yesterday's picture and another from last week. It adds other puzzle pieces to better predict if the hostiles will be there tomorrow, and what the enemy is capable of doing in that location, as well as what any associates are doing 10 miles away.

An exciting advancement, ABI exploits improvements in sensor development, information management, analysis, sharing, and enhancing intelligence activities. Rather than focusing collection and analysis efforts on a single target, the approach assesses a wider variety of data – both conventional and unconventional—over a period of time and, in doing so, provides better insight into patterns of behavior and future activities.

The technology's grounding in multi-intelligence fusion makes ABI even more exciting and demanding, as it involves uniting data from disparate geospatial sources with unstructured and seemingly mundane information—such as documents, business system data and business intelligence, along with archives—into an integrated analytical environment for detecting trends that offer context: The what, when and where, and even the how and why, elements of a comprehensive geospatial story that can drive smarter decision-making.

Modeling input can clarify that decision, and the fused elements can be subsequently recombined by others for their own uses. Those supporting the decision makers have to work with data across time, and to do so they must connect through an Enterprise Information Management foundation, one that also integrates with capture platforms and sensors to automate and speed the processing of their inputs.

To accomplish these tasks, ABI solutions establish real-time connections to as many raw intelligence collections as possible. The ability to bring imagery intelligence (IMINT), signals intelligence (SIGINT), human intelligence (HUMINT), Measures and Signatures (MASINT), and other sources into an integrated analytical environment provides a powerful setting to assist analysts in detecting trends they might not otherwise see.

Feeds from one source of intelligence can also provide cues to specific segments of data from other sources, leading to a more meaningful analysis. One segment also can help to validate or discount another.

The modern command operations center.

The mission requires doing all of this quickly, extracting from stovepipes a meaningful array of information. With the Middle East wars winding down, there is also a demand for increased flexibility in intelligence gathering and exploitation to meet needs as varied as those of U.S. Special Operations, which is present in as many as 100 countries at any one time; of disaster relief agencies working in places such as Southeast Asia in the aftermath of Typhoon Haiyan; and with military and civilian agencies monitoring ongoing tensions in Syria and elsewhere among Arab Spring nations.

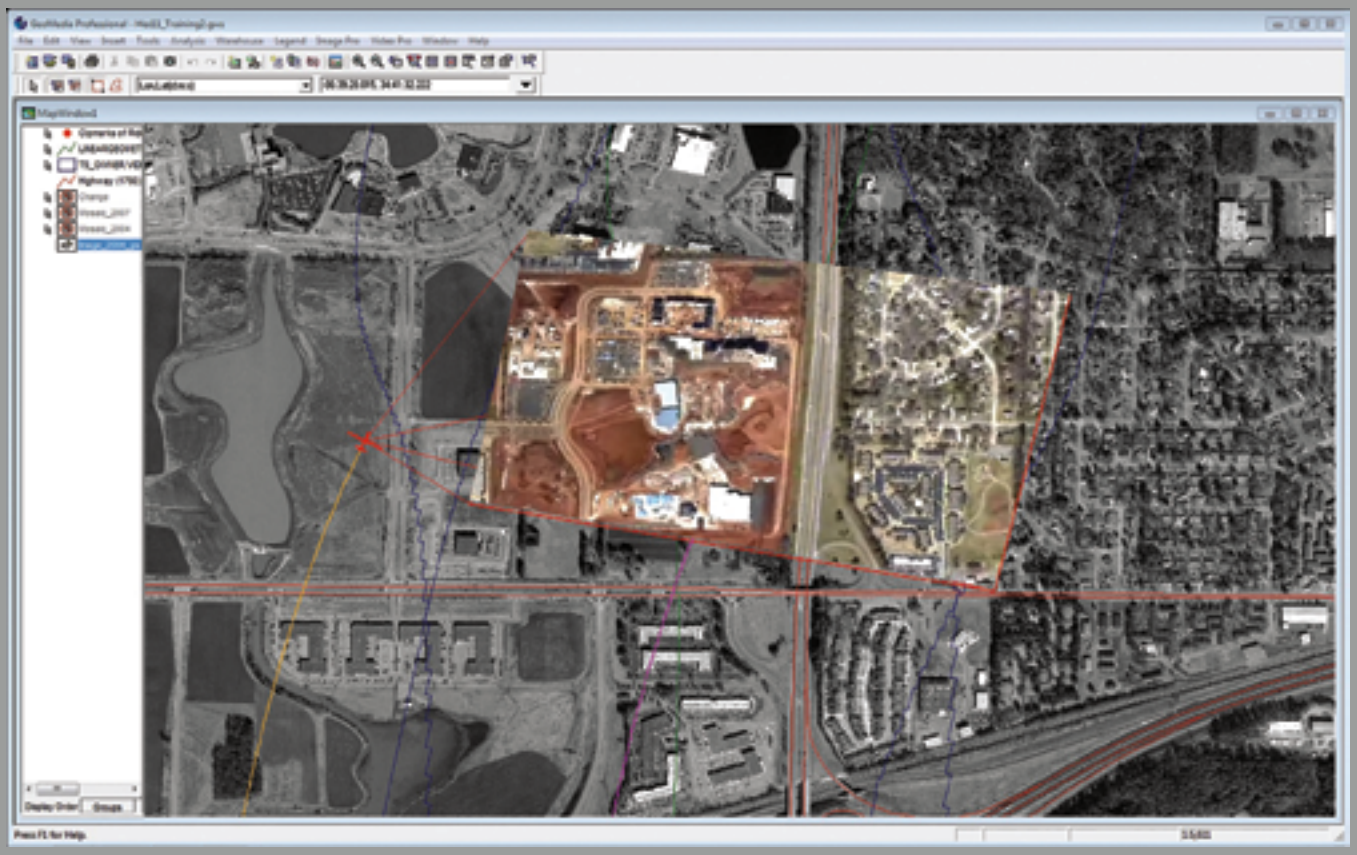
To meet this goal, intelligence, defense, national security and disaster assistance agencies require a portfolio that provides best-in-class data capture, GIS, remote sensing and photogrammetry capabilities, as well as the synthesis of these technologies in server-based products specializing in data management, spatial data infrastructure, workflow optimization, web editing and web mapping.

As exciting as ABI has become, its development and improvement has to be accomplished in the constraining environment of fiscal austerity in which it competes with other defense, security and disaster relief elements for funding. Fortunately, it is now possible to tie all of these components together cost effectively to achieve a complete end-to-end capability that advances security efforts on a global scale.

For example, tying together sensor-based data capture of geo-referenced position and terrain information with data processing, including orientation and triangulation, creates a cross portfolio capability that benefits border security, police forces, defence and intelligence and more. This also includes 3D feature collection and editing, as well as digital terrain model collection, editing and enhanced visualization.

In terms of sensor integration, this could also include Radar Operational Surveillance Systems in which technology integrates satellite-based AIS data from exactEarth and other satellite-based radar systems.

A comparison of two images shows how automatic dehazing improves the quality and usability of imagery, allowing the analyst to make better decisions



Displaying real-time UAV video feeds and other geospatial data over a satellite image provides improved context an understanding of unfolding activities in the area of interest.

New industry solutions also play a key role in helping large systems integrators meet their government customers' challenges. Aligning with customer requirements, a fully customizable geospatial SDK can help these organizations seamlessly embrace the solutions' capabilities.

These tools meet the needs of a dynamic geospatial approach to intelligence gathering and exploitation, as does the implementation of the open Web Processing Service (WPS) standard, which greatly extends the reach and value of the models analysts develop. By using a simple, standards-based web interface, non-domain experts can apply powerful modeling, analysis and data manipulation without the need of extensive training or specialist hardware.

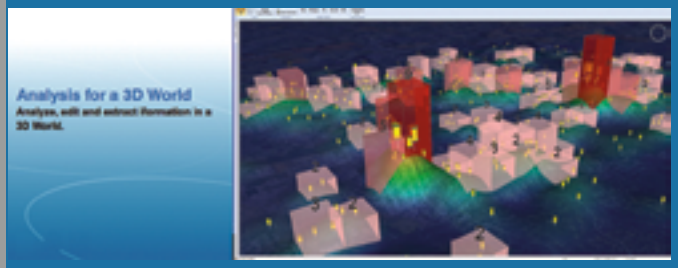
With more capability, and more users for that capability, the IC can call on an ever-developing array of tools to exploit more and different intelligence pieces to generate a clearer picture that is the product of decades of evolution in the field. And those pictures can be used in ways that are more numerous, diverse and powerful than ever.

About the author

Sven Bues is the Vice President, EMEA Defense & Intelligence Sales, at Intergraph. Sven served in the German Armed Forces until 1996 and studied mechanical engineering during his military service. In the last position of his military career, he served as an army officer for the drone reconnaissance system CL-289.

For 40 years, Intergraph has been a trusted partner of defense and intelligence agencies. Drawing from the firm's solid engineering heritage and open standards architecture, brought together are people, data, and systems for faster, more accurate decision making. Their geospatially powered solutions transform vast amounts of complex data into actionable intelligence, protecting U.S. and global interests and supporting the warfighter. The company's solutions and IT services help clients build and manage geospatial databases, produce operational maps, manage critical enterprise content, analyze and fuse geospatial intelligence, manage weapon support systems, and ensure the security of military bases and installations worldwide.

GeoMedia 3D is the latest addition to the Intergraph GeoMedia product suite, a set of well-integrated applications that offer a wide range of geospatial processing capabilities. GeoMedia 3D is a GeoMedia add-on product that extends the functionality of Intergraph's geospatial solutions through an integrated 3D visualization and analysis environment.



Satnews Publishers readers save £200

"A very interesting and reliable conference...It was inspiring and it will help me hugely in the future."
Armed forces of the Slovak Republic

SMi
LINKING BUSINESS and INFORMATION

SMi present their 7th Annual Conference...

Mobile Deployable Communications

Mövenpick City Centre Hotel, Amsterdam

6th - 7th FEBRUARY 2014

Top-Ranked Speaker Faculty Includes...

- **Colonel Horst Treiblmaier,** Chief of Communication, **Ministry of Defence, Austria**
- **Colonel (BG-A) Krasimir Yordanov,** IT & Security Branch Chief, CIS Directorate, EUMS, **European External Action Service**
- **Aurel SABO,** Deputy Commander of Mobile CIS Base, HQ Mobile CIS Base, **Mobile CIS Base of Slovak Armed Forces**
- **Karl Thurnhofer,** Director Communication Section, Command Support Centre ICT Engineering Division, **Federal Ministry of Defence and Sports, Republic of Austria**
- **WO2 (YofS) RM Stephen Scott MBE,** COMUKAMPHIBFOR Yeoman of Signals, J6, **Royal Marines**
- **Martin Jarrold,** Chief, **International Programme Development at Global VSAT Forum**

Event's Highlights Include:

- **Hear the UK MOD most recent update on UK Land Environment Tactical CIS**
- **Join the discussion on EU militaries working towards a truly mobile communications system during an interactive panel discussion**
- **Learn about the Italian view point on Network Centric Warfare**
- **Listen to a focused energy supply presentation from the Ministry of Defence, Austria**
- **Hear how the challenges of SOA - based communications in the tactical domain will effect ongoing operations from the Polish Institute of Military Communications Institute**

PLUS AN INTERACTIVE HALF-DAY PRE-CONFERENCE WORKSHOP

Wednesday 5th February 2014, Mövenpick City Centre Hotel, Amsterdam

Sponsored by

HARRIS CAPROCK · iOra · Together ahead. RUAG

Mobility & Deployability for Emergency & Post-Disaster Recovery Communications

Hosted by: **Martin Jarrold,** Chief, **International Programme Development at Global VSAT Forum**

12.30 - 17.30

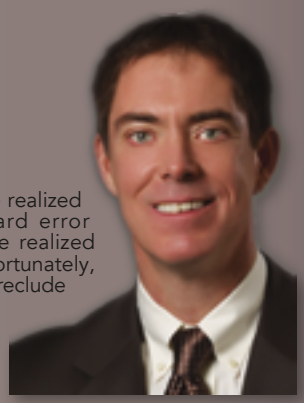
REGISTER ONLINE & SAVE £200 - QUOTE SMI7T6P

www.mobiledeployable.com

Register online or contact James Hitchen on +44 (0) 20 7827 6054
or email jhitchen@smi-online.co.uk

CPD CERTIFIED

Airborne ISR Challenges



By Karl Fuchs, Vice President of Technology, iDirect Government Technologies (iGT)

Intelligence, Surveillance and Reconnaissance (ISR) is by far the most prevalent application for Unmanned Aerial Systems (UASs).

Currently, the majority of ISR data from a UAS is transmitted by Common Data Link (CDL), line-of-sight directly to ground. There are, however, a number of missions where ISR transmission, beyond line-of-site over satellite, is most advantageous. As with most network designs, there is no one size fits all solution. There are pluses and minuses to both line-of-sight and beyond line-of-sight transmission of ISR traffic.

Line-of-site data transmission allows for very high data rates with relatively inexpensive and low-power transmission equipment on board. In fact, line-of-site, CDL video links can exceed 250Mb/s. Satellite links at such high speeds would be impractical on UAS platforms.

Of course, the drawback to line-of-sight communications is the need for line-of-sight. In many cases, to receive the video link a vehicle is deployed in theater. This practice has a number of obvious drawbacks not the least of which is the safety and security of the personnel manning the ground infrastructure.

The reliance of a ground infrastructure for CDL systems is very acceptable for certain applications. CDL links are widely deployed in battlefield operations and are very well suited to border patrol and first responder applications. CDL links, however, are limited if the mission is global or extends over a very wide geographic area.

Beyond line-of-sight data exfiltration systems using geosynchronous satellites require sophisticated tracking antennas and modems with Doppler-compensating modems. Furthermore, due to antenna size restrictions, the data rates available to transmit video off the aircraft are limited to about 15Mb/s. A number of new technologies being introduced are increasing theses data rates.

Some improvements in data rates are realized through new waveform and forward error correction techniques, and some are realized through new antenna technologies. Fortunately, the current limit in data rate does not preclude satellite communications for high-definition ISR missions.

Some high-definition codex can operate with as little as 2Mb/s with 6Mb/s being the most typical for HD video. Of course, the two things that make beyond line-of-sight communications most attractive are its independence from a terrestrial infrastructure and the global coverage available.

Certainly, exfiltrating ISR data is only half the story. In order for the video to be of any use, it has to be received by the people who need the information and in a very timely manner.

For missions with troops on the ground and an ISR covering a limited geographic region, CDL is an excellent solution. In the case where ISR data needs to be backhauled for further analysis, high-speed, ground-based, single channel per carrier satellite or even terrestrial links can be utilized. In some instances, the Global Broadcast Service (GBS) is used to bring ISR video to the field.

Currently, GBS is a one-way only system, but the desire and plan is to enable two-way communications. New satellite terminals are being developed with the ability to receive two independent DVB-S2 feeds. One DVB-S2 out-route would be used for the GBS service with the other as the out-bound for a two-way communications system.

Keeping the two systems independent is important for ease of transition and to maintain separate transmission security (TRANSEC) security domains. Integrating the GBS receive and the two-way communication in a single platform is vital in lowering the size, weight and power (SWAP) requirements of a communications package.

As airborne communications on the move (COTM) becomes more mainstream and technological advances continue to increase the data rates available off an airborne platform, direct to satellite ISR links will become more prevalent. The advent of High Throughput Satellites (HTS) with their global spot beam architecture will only speed the adoption rate.

The adoption of direct-to-satellite ISR will be driven by ISR platforms with a global mission. Existing terrorist networks are not limited to national boundaries or geographic regions. Furthermore, conflicts can quickly arise halfway around the world. UAS platforms which can operate on a global scale are ideal for these quick response ISR missions.

Security becomes increasingly complex in a system which is global in nature and utilizes a broadcast technology such as satellite as its transmission medium. Seamless hand-off of a UAS from one satellite coverage area to another is one thing. Seamless hand-off of a UAS under TRANSEC cover is another.

For global networks in which one operator controls the entire ground infrastructure, a solution for global TRANSEC cover has been designed and implemented. The challenge now is to extend that TRANSEC capability to include the global footprint of HTS secure, commercial service.

Although line-of-site backhaul will continue to play a dominant role in ISR missions with the pieces quickly coming into place, the use of direct to satellite exfiltration will grow dramatically. The flexible, ubiquitous coverage, and the independence from a terrestrial infrastructure that satellite communications offers, bring too many compelling reasons not to move many ISR missions to satellite. Enhancements in waveform, security and antenna technologies are rapidly dispelling objections against satellite. These are fundamentally the same driving factors which have brought satellite COTM to commercial aircraft.

About the author
Karl Fuchs serves as Vice President of Technology for iDirect Government Technologies (iGT); ***kfuchs@idirectgt.com****.*

Editors note
Images for this article were provided by iGT.

iGT AiMS High

Airborne In-flight Monitoring System (AIMS) is iGT's solution for customers to view satellite information with respect to a moving aircraft while in flight.

The software, which is loaded onto a PC, communicates with the iDirect modem, as well as the Antenna Control Unit (ACU) to display the real-time position of the aircraft and allows a user to quickly see when the aircraft will leave one satellite coverage footprint and enter another.

With AIMS, an operator is able to quickly determine the position of the aircraft and whether or not a communications interruption might occur due to switching satellite footprints.

The operator has the ability to manually switch to an available network, or view a countdown timer before the automatic beam switch occurs.

Through the Graphical User Interface (GUI), a beam information window is provided that displays information on all the beams for the configured modem.

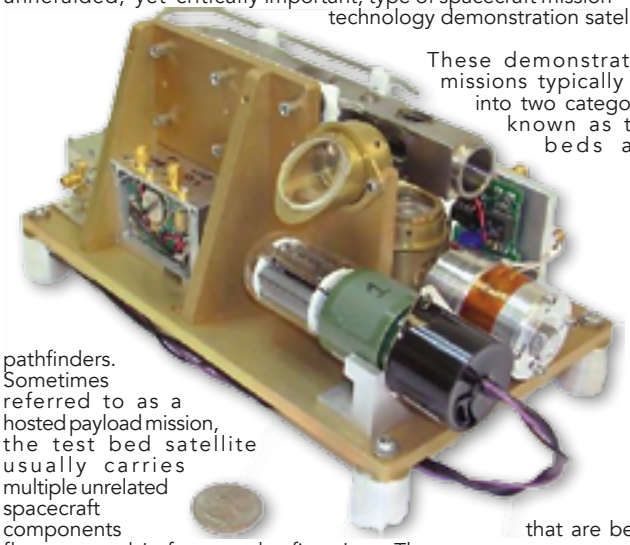
AIMS provides the option for a user to log flight statistics into a KML file format for future analysis. These flight statistics are logged every two minutes and include iDirect Modem and ACU parameters.

The Value Of Demo Satellite Missions

By Dr. John Paffett, Chief Executive Officer, Surrey Satellite Technology US LLC

In June, NASA's Space Technology Mission Directorate announced that the Jet Propulsion Laboratory (JPL) would fly the Deep Space Atomic Clock payload aboard the commercial Orbital Test Bed satellite that is being developed by Surrey Satellite Technology US (SST-US) at the firm's new Colorado assembly facility.

The announcement focused a much-deserved spotlight on an unheralded, yet critically important, type of spacecraft mission—the technology demonstration satellite.



These demonstration missions typically fall into two categories known as test beds and pathfinders. Sometimes referred to as a hosted payload mission, the test bed satellite usually carries multiple unrelated spacecraft components that are being flown on orbit for the first time. These components may be entirely new subsystems or improved engineering designs of traditional equipment that must prove their performance in the rigors of space before integration into large operational missions.

The Deep Space Atomic Clock (DSAC) is a prime example of a test bed mission. Atomic clocks are crucial for spacecraft navigation, and JPL is designing DSAC as a much smaller and more precise replacement for existing devices.

NASA's objective is to test DSAC on orbit with a relatively inexpensive mission before installing another on a far more costly flight to outer space.

DSAC will be launched in 2015, along with eight other payloads, aboard the commercial Orbital Test Bed (OTB), which will be owned and operated by SST-US. As is often the case with test bed missions, the OTB satellite will use a flight-proven design, the SSTL-150, developed by SST-US' parent company in the United Kingdom, Surrey Satellite Technology Ltd.

While the Surrey name is most often associated with operational satellite missions, 33 of its 41 launches have involved demonstrations of remote sensing, navigation, and communications technologies.

The other type of demonstration mission, the pathfinder, is usually more technically complex, often involving multiple new or redesigned components that must be tested together as an integrated subsystem. These components may relate to the operation of the satellite or to its mission, such as a new imaging sensor on a remote sensing satellite. In some cases, a pathfinder may be a scaled-down version of a multifunction satellite that meets the minimum requirements of the proposed larger mission.

Whether the demonstration mission is a test bed or pathfinder, the goal is the same—to reduce risk in the development of new aerospace technology.

Demonstration missions are becoming increasingly important in the U.S. defense/intelligence community for two reasons.

First, this community is under constant pressure to develop new space-based solutions in response to continually evolving world situations. Solutions must be developed quickly.

Second, the costs of engineering, building, and launching large complex satellites are climbing steeply at a time when budgets across the board are being cut. The risk of launching an untested sensor aboard a billion-dollar satellite is simply too great.

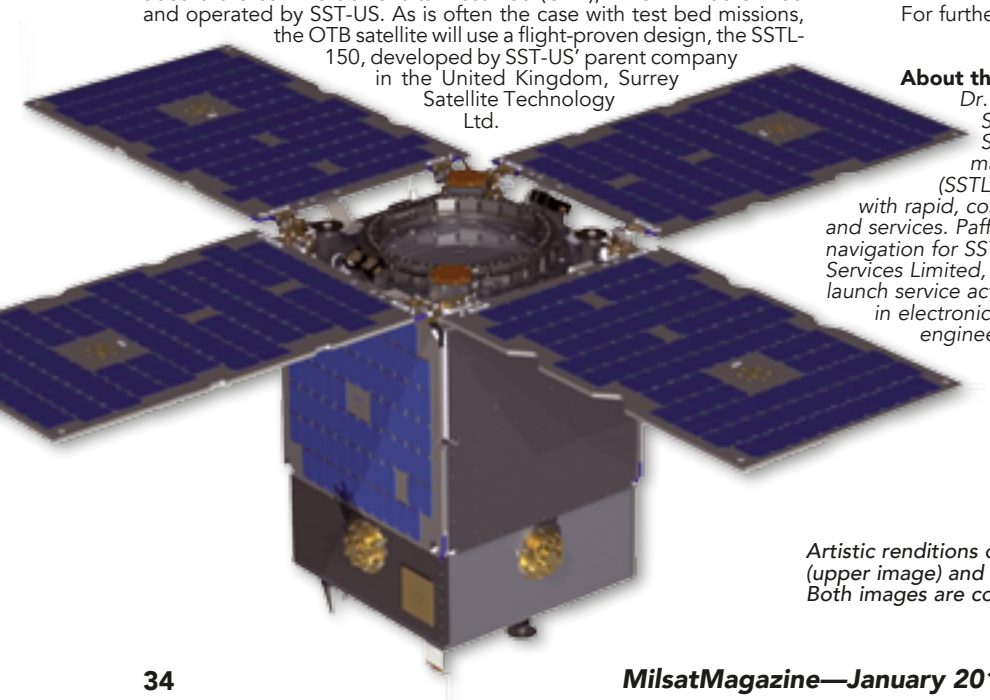
Test beds and pathfinders address these issues. As is the case with the OTB, the new clock is being flown on a space-proven satellite design, minimizing the chance of a bus failure. Moreover, existing satellite designs in the commercial sector are often selected because they are built with off-the-shelf components, which means they can be assembled and launched quickly, allowing new engineering concepts to go from the drawing board to orbit in as little as 12 to 24 months.

Increasingly, organizations in the defense/intelligence sector are tapping satellites in the 100- to 600-kilogram class for their demonstration missions. Much less complex than their larger multi-function counterparts, these satellites have price tags ideally suited for experimentation. Depending on the cost of sensors or subsystems being tested, a complete pathfinder mission could be launched for less than one-tenth the cost of an operational satellite.

For further information, access the SST-US infosite at:
http://www.sst-us.com/

About the author

Dr. John Paffettt is chief executive officer for Surrey Satellite Technology US LLC (SST-US), the United States subsidiary of world-leading small satellite manufacturer Surrey Satellite Technology Limited (SSTL). SST-US was created to serve the U.S. market with rapid, cost-effective small satellite systems, applications, and services. Paffett is also director of telecommunications and navigation for SSTL and chief executive officer of Surrey Satellite Services Limited, the SSTL subsidiary responsible for provision of launch service activities. He holds a bachelor's degree (honors) in electronic engineering and a doctorate in electronic engineering from the University of Surrey.



Artistic renditions of the Deep Space Atomic Clock (upper image) and the Orbital Test Bed satellite (lower image). Both images are courtesy of NASA + JPL.

Where can you find the satellite industry under one roof?

sspi gala

March 11, 2014
Walter E. Washington Convention Center
Washington, DC

The Gala offers a unique opportunity to network and visit with clients, customers, suppliers, colleagues and industry friends. From the champagne reception to a gourmet meal to the presentation of the Industry Innovator Awards, the Gala is the talk of the industry.

For the first time, SSPI will offer a reception only ticket, allowing guests to participate in the networking opportunity provided by the Champagne Reception, yet still attend any offsite dinner plans they may have that evening.

For more information or to purchase tickets for the SSPI Gala, visit www.SSPI.org

Interested in supporting the mission? Sponsorship and branding opportunities are available. Contact Tamara Bond (tbond@sspi.org) for more information.

Think global, party local at SATELLITE 2014

THE IMPORTANCE OF DESIGNATING CYBERSPACE WEAPON SYSTEMS

By Brigadier General Robert J. Skinner, U.S.A.F.

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, defines weapon system as "a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency."[1]

When one thinks of the US Air Force and weapon systems, the B-2 Spirit stealth bomber, F-15E Strike Eagle fighter jet, or F-16 Fighting Falcon aircraft quickly come to mind. Even the Minuteman III missile, the Global Positioning System, or KC-135 Stratotanker air refueling aircraft could become part of the discussion because, after all, the Air Force's mission is to fly, fight, and win in air, space, and cyberspace.

These assets, which fall under the air and space umbrella, have served as tried and true weapon systems for many years. The Air Force has now added to the long line of its weapon systems that support cyberspace operations "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." These systems are unique in that they are tied to the newest domain of cyber—"a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2]

On 24 March 2013, the chief of staff of the Air Force approved the official designation of six cyberspace weapon systems under the lead of Air Force Space Command (AFSPC), which is responsible for organizing these systems, equipping units with them, and training individuals to use the systems. The Air Force's provision of global reach, power, and vigilance across the domains of air and space now applies to the cyberspace domain through the designation of the following cyberspace weapon systems:

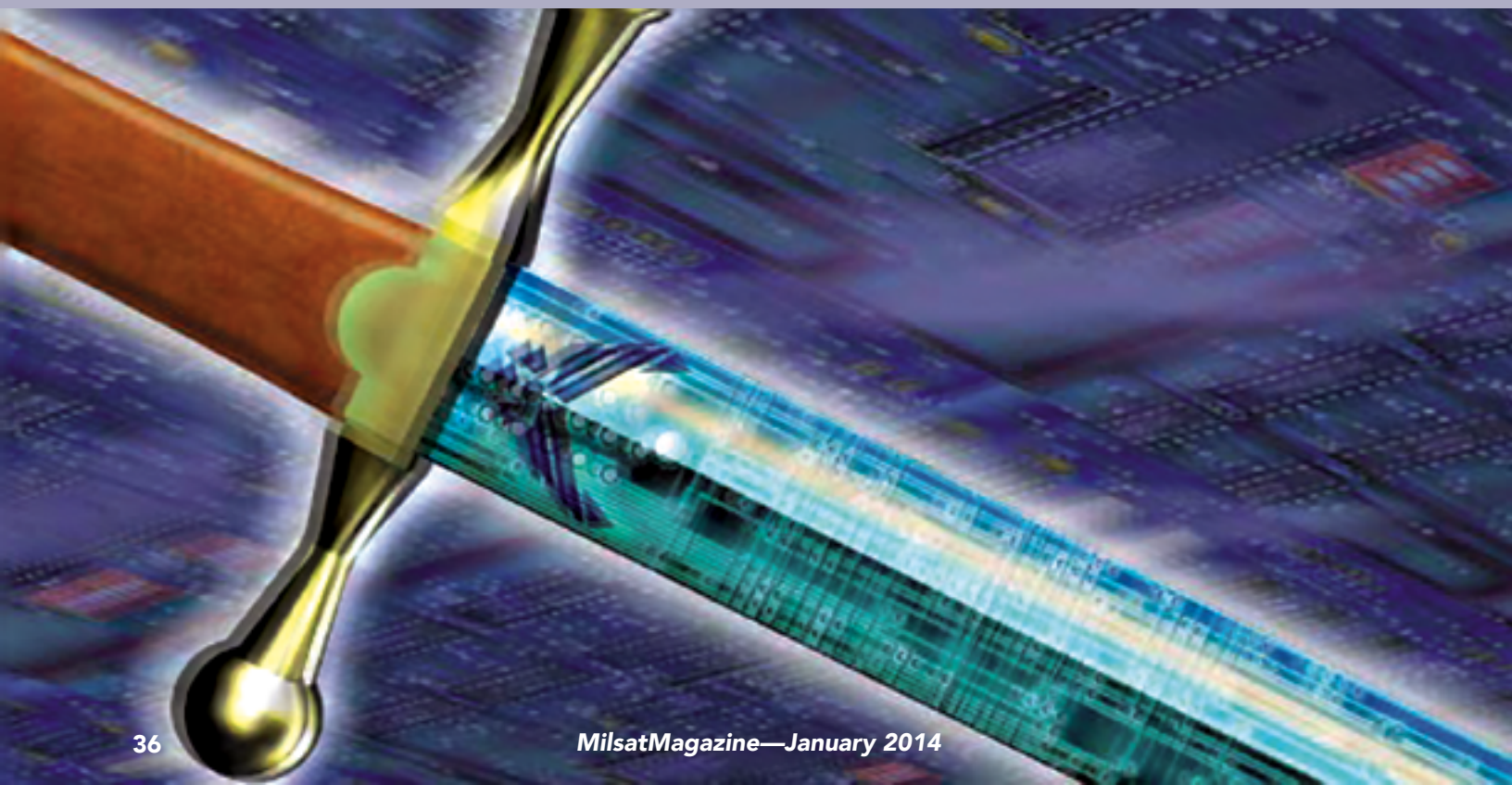
- **Air Force Cyberspace Defense**
- **Cyberspace Defense Analysis**
- **Cyberspace Vulnerability Assessment / Hunter**
- **Air Force Intranet Control**
- **Air Force Cyber Security and Control System**
- **Cyber Command and Control Mission System**

Although the names may imply some duplication of effort with respect to these capabilities, the personnel and equipment that comprise these systems perform unique missions and complement each other. All of them focus on providing and securing cyberspace as a mission enabler and protecting critical information while defending our networks from

General Skinner (BS, Park College; MS, Oklahoma City University) is the deputy commander, Air Forces Cyber (AFCYBER). He is the primary liaison and personal representative to US Cyber Command and the National Security Agency; he also supports AFCYBER's operational activities with the Office of the Secretary of Defense, Director of National Intelligence, Central Intelligence Agency, and other National Capitol Region cyber stakeholders.

Commissioned in 1989, the general is a graduate of Squadron Officer School, Command and General Staff College, Air War College, and the Industrial College of the Armed Forces. His career highlights include wing and group commands, multiple squadron commands, a variety of tactical and fixed communications assignments as well as staff assignments at the Joint Staff, Air Staff, and a numbered air force.

Prior to assuming his current position, General Skinner served as inspector general at Headquarters Air Force Space Command, Peterson AFB, Colorado. In this role, he led a 70 person, three-division directorate consisting of five branches charged with evaluating the readiness of more than 300 Air Force Space Command space and cyber units located at more than 100 worldwide locations.



attack. Any consideration of the capabilities of these weapon systems would benefit from comparing this suite of cyberspace weapon systems to the Air Force's military airlift weapon systems (the C-5, C-17, C-130, etc.), each of which contributes uniquely to September–October 2013 Air & Space Power Journal | 31 Space Focus Senior Leader Perspective the overall air mobility mission. Just as clear distinctions exist among these platforms, based upon the operational capabilities required, so do the cyberspace weapon systems differ from each other. The systems may have overlapping mission areas, but they are complementary in much the same way as our airlift platforms—they offer comprehensive capabilities.

Revelations of Chinese activities on our networks, as outlined earlier this year in the Mandiant Company's report titled *Advanced Persistent Threat (APT) 1: Exposing One of China's Cyber Espionage Units*, emphasize the urgent need for the Air Force and the nation to develop capabilities to defend this critical domain and thereby ensure information superiority. The report illustrates the persistent threat, noting that "the details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them. . . . Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors."

The Mandiant report on APT 1 highlights only one of more than 20 APT groups based in China, tracking this single group to cyber attacks on nearly 150 victims over seven years with hundreds of terabytes of data exfiltrated.[3]

Clearly, though, this discussion does not confine itself to any particular adversary. Many aggressors inhabit the cyberspace domain, and the executor of these activities ranges from an individual in the basement of his house, to groups of individuals working as teams, to nation-states. Their intentions can also cover a spectrum of activities, including espionage, theft of intellectual capital, organized crime, identity theft, military operations, and so forth.

This article examines each weapon system, highlights its history and unique capabilities, and describes the specific units that operate the system. It then discusses the importance of classifying these capabilities as "weapon systems," illustrating how they directly address the threats we face today. Before doing so, however, the article presents a stage-setting vignette to establish an understanding of weapon system capabilities and their employment against an adversary.

Assume that you are a government civilian sitting at your desk at a major command headquarters when you receive an e-mail concerning sequestration and a potential furlough. Included in the e-mail is a link to a website for more information. You attempt to open the link but receive an error message. You try again with the same result. You then resume work on your tasks. Unknown to you, the link has directed you to a malicious web server that downloaded malware enabling an adversary to take command of your desktop computer. How could this occur, and why would anyone specifically target you? Actually, it was not difficult. Remember the conference you attended a few months ago, before temporary duty became restricted? The adversary lifted your e-mail address from the conference sign-in sheet, also available to the event sponsors. Why you? Adversaries consider your unique expertise and access to valuable information a "target-rich environment." Only one person needs to click on the link to initiate a series of malicious actions. Because the adversary left no hint of a problem on your computer, he now has unfettered access to that unclassified but useful information.

How does the Air Force combat such intrusions? Actually, the best defense for phishing attacks is user education. However, these attacks are becoming more sophisticated and sometimes almost impossible to identify. All of the services have cyberspace units responsible for network defense. In this case, network traffic monitoring tips off the Air Force to the intrusion on your desktop computer. A network operations unit identifies an unusual amount of traffic leaving your base directed to addresses in another country. The unit notifies the 624th Operations Center, including Air Force Office of Special Investigations personnel, and the center begins command and control (C2) and law enforcement efforts to address the event. Cyberspace forensics experts are dispatched to review the situation, not only locating the "infected" equipment but also determining how the adversary accessed the Air Force system.

Cyberspace C2 dispatches cyber operations risk-assessment personnel to survey the situation, determine the exact data exfiltrated, and assess the damage. The Air Force computer emergency response team (AFCERT) examines your base's computers and other hardware to footprint exact infiltration methods, using them to develop (and share) defensive actions specific to the threat and glean any new tactics, techniques, and procedures. The AFCERT pushes patches to all Air Force desktop computers to combat future attempts to employ this technique; it will support your base on further network cleanup and hardening. Now that we have described an attack from 50,000 feet, let us delve deeper into the weapon systems and units that carry out these missions.

Air Force Cyberspace Defense Weapon System

The Air Force Cyberspace Defense (ACD) weapon system prevents, detects, responds to, and provides forensics of intrusions into unclassified and classified networks. Operated by the 33d Network Warfare Squadron (NWS), located at Joint Base San Antonio–Lackland, Texas, and the Air National Guard's 102d NWS, located at Quonset Air National Guard Base, Rhode Island, the ACD weapon system supports the AFCERT in fulfilling its responsibilities. The crews for this weapon system consist of one cyberspace crew commander, one deputy crew commander, one cyberspace operations controller, and 33 cyberspace analysts, all of them supported by additional mission personnel.

The ACD weapon system evolved from the AFCERT, which has primary responsibility for coordinating the former Air Force Information Warfare Center's technical resources to assess, analyze, and mitigate computer security incidents and vulnerabilities. The weapon system offers continuous monitoring and defense of the Air Force's unclassified and classified networks, operating in four subdiscipline areas:

1. Incident prevention: Protects Air Force networks (AFNet) against new and existing malicious logic; assesses and mitigates known software and hardware vulnerabilities.

2. Incident detection: Conducts monitoring of classified and unclassified AFNets; identifies and researches anomalous activity to determine problems and threats to networks; monitors real-time alerts generated from network sensors; performs in-depth research of historical traffic reported through sensors.

3. Incident response: Determines the extent of intrusions; develops courses of action required to mitigate threat(s); determines and executes response actions.

4. Computer forensics: Conducts in-depth analysis to determine threats from identified incidents and suspicious activities; assesses damage; supports the incident response process, capturing the full impact of various exploits; reverse-engineers code to determine the effect on the network/system.

Cyberspace Defense Analysis Weapon System

The Air Force Cyberspace Defense Analysis (CDA) weapon system conducts defensive cyberspace operations by monitoring, collecting, analyzing, and reporting on sensitive information released from friendly unclassified systems, such as computer networks, telephones, e-mail, and US Air Force websites. CDA is vital to identifying operations security disclosures. The weapon system is operated by three active duty units (68 NWS; 352 NWS; and 352 NWS, Detachment 1) and two Air Force Reserve units (860th Network Warfare Flight and 960th Network Warfare Flight) located at Joint Base San Antonio–Lackland, Texas; Joint Base Pearl Harbor–Hickam Field, Hawaii; Ramstein Air Base, Germany; and Offutt AFB, Nebraska. The crews for this weapon system consist of one cyberspace operations controller and three cyberspace defense analysts. All mission crews receive support from additional mission personnel.

The CDA weapon system's two variants are designed to monitor, collect, analyze, and report on official Air Force information transmitted via unsecured telecommunications systems to determine whether any of it is sensitive or classified. The system reports compromises to field commanders, operations security monitors, or others, as required, to determine potential effects and operational adjustments. The second variant provides additional functionality to conduct information damage assessment based on network intrusions, coupled with an assessment of Air Force unclassified websites. Only the 68 NWS operates the second variant.

The CDA weapon system supplies monitoring and/or assessment in six subdiscipline areas:

1. Telephony: Monitors and assesses Air Force unclassified voice networks.

2. Radio frequency: Monitors and assesses Air Force communications within the VHF, UHF, FM, HF, and SHF frequency bands (mobile phones, land mobile radios, and wireless local area networks).

3. Email: Monitors and assesses unclassified Air Force e-mail traffic traversing the AFNet.

4. Internet-based capabilities: Monitor and assess information that originates within the AFNet that is posted to publicly accessible Internet-based capabilities not owned, operated, or controlled by the Department of Defense (DOD) or the federal government.

5. Cyberspace operational risk assessment (found within the second variant operated by the 68 NWS): assesses data compromised through intrusions of AFNets with the objective of determining the associated effect on operations resulting from that data loss.

6. Web risk assessment (found within the second variant operated by the 68 NWS): Assesses information posted on unclassified public and private websites owned, leased, or operated by the Air Force in order to minimize its exploitation by an adversary, diminishing any adverse affect on Air Force and joint operations.

Cyberspace Vulnerability Assessment / Hunter Weapon System

The Air Force Cyberspace Vulnerability Assessment (CVA) / Hunter weapon system executes vulnerability, compliance, defense, and nontechnical assessments, best-practice reviews, penetration testing, and hunter missions on Air Force and DOD networks and systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. This weapon system can perform defensive sorties worldwide via remote or on-site access.

The CVA/Hunter weapon system is operated by one active duty unit, the 92d Information Operations Squadron, located at Joint Base San Antonio–Lackland, Texas, and one Guard unit, the 262 NWS, located at Joint Base Lewis-McChord, Washington. Additionally, two Guard units are in the process of converting to this mission: The 143d Information Operations Squadron located at Camp Murray, Washington, and the 261 NWS located at Sepulveda Air National Guard Station, California. The crews for this weapon system consist of one cyberspace crew commander, one to four cyberspace operators, and one to four cyberspace analysts. Additional mission personnel support all of the mission crews.

Developed by the former Air Force Information Operations Center, the CVA/Hunter weapon system was fielded to the 688th Information Operations Wing in 2009. Historically, vulnerability assessments proved instrumental to mission assurance during Operations Enduring Freedom and Iraqi Freedom. CVAs continue to provide this vital capability. Additionally, they now serve as the first phase of hunting operations. The hunter mission grew out of the change in defensive cyber strategy from "attempt to defend the whole network" to "mission assurance on the network," offering an enabling capability to implement a robust defense-in-depth strategy. CVA/Hunter weapon system prototypes have participated in real-world operations since November 2010. The weapon system attained initial operational capability in June 2013.

Designed to identify vulnerabilities, the CVA/Hunter gives commanders a comprehensive assessment of the risk of existing vulnerabilities on critical mission networks. It is functionally divided into a mobile platform used by operators to conduct missions either on site or remotely, a deployable sensor platform to gather and analyze data, and a garrison platform that provides needed connectivity for remote operations as well as advanced analysis, testing, training, and archiving capabilities. Specifically, the hunter mission focuses on finding, fixing, tracking, targeting, engaging, and assessing the advanced, persistent threat.

During active engagements, the CVA/Hunter weapon system, in concert with other friendly network defense forces, provides Twenty-Fourth Air Force / Air Forces Cyber and combatant commanders a mobile precision-protection capability to identify, pursue, and mitigate cyberspace threats. It can be armed with a variety of modular capability payloads optimized for specific defensive missions and designed to produce specific effects in cyberspace. Each CVA/Hunter crew can conduct a range of assessments, including vulnerability, compliance, and penetration testing, along with analysis and characterization of data derived from these assessments. The weapon system's payloads consist of commercial-off-the-shelf and government-off-the-shelf hardware and software, including Linux and Windows operating systems loaded with customized vulnerability-assessment tools.

Air Force Intranet Control Weapon System

The Air Force Intranet Control (AFINC) weapon system is the top level boundary and entry point into the Air Force Information Network, controlling the flow of all external and interbase traffic through standard, centrally managed gateways. The AFINC weapon system consists of 16 gateway suites and two integrated management suites. Operated by the 26th Network Operations Squadron (NOS) located at Gunter Annex, Montgomery, Alabama, AFINC has crews consisting of one crew commander, one deputy crew commander, one cyberspace operations crew chief, two operations controllers, two cyberspace operators, and three event controllers, all of them supported by additional mission personnel.

The AFINC weapon system replaces and consolidates regionally managed, disparate AFNets into a centrally managed point of access for traffic through the Air Force Information Network. It delivers network-centric services, enables core services, and offers greater agility to take defensive actions across the network. AFINC integrates network operations and defense via four subdiscipline areas:

1. Defense-in-depth: Delivers an enterprise-wide layered approach by integrating the gateway and boundary devices to provide increased network resiliency and mission assurance.

2. Proactive defense: Conducts continuous monitoring of AFNet traffic for response time, throughput, and performance to ensure timely delivery of critical information.

3. Network standardization: Creates and maintains standards and policies to protect networks, systems, and databases; reduces maintenance complexity, downtime, costs, and training requirements.

4. Situational awareness: delivers network data flow, traffic patterns, utilization rates, and in-depth research of historical traffic for anomaly resolution.

Air Force Cyber Security and Control System Weapon System

The Air Force Cyber Security and Control System (CSCS) weapon system provides network operations and management functions around the clock, enabling key enterprise services within the Air Force's unclassified and classified networks. It also supports defensive operations within those AFNets. CSCS is operated by two active duty NOSs, one Air National Guard Network Operations Security Squadron, and two Air Force Reserve Command Associate NOSs aligned with the active duty squadrons. The 83 NOS and 860 NOS are located at Langley AFB, Virginia; the 561 NOS and 960 NOS at Peterson AFB, Colorado; and the 299th Network Operations Security Squadron at McConnell AFB, Kansas. Crews for this weapon system consist of one cyberspace crew commander, one cyberspace operations controller, an operations flight crew (conducting boundary, infrastructure, network defense, network focal point, and vulnerability-management functions), and an Enterprise Service Unit (supplying messaging and collaboration, directory and authentication services, storage and virtualization management, and monitoring management). Additional mission personnel support all of the mission crews.

The CSCS resulted from an operational initiative to consolidate numerous major command–specific networks into a centrally managed and controlled network under three integrated network operations and security centers. In 2007 the Air Force established two active duty NOSs to provide these functions. The Air National Guard Network Operations Security Squadron does the same for the Guard's bases and units. The CSCS weapon system performs network operations and faultresolution activities designed to maintain operational networks. Its

crews monitor, assess, and respond to real-time network events; identify and characterize anomalous activity; and take appropriate responses when directed by higher headquarters. The system supports real-time filtering of network traffic into and out of Air Force baselevel enclaves and blocks suspicious software. CSCS crews continuously coordinate with base-level network control centers and communications focal points to resolve network issues. Additional key capabilities include vulnerability identification and remediation as well as control and security of network traffic entering and exiting Air Force base-level network enclaves. CSCS also offers Air Force enterprise services, including messaging and collaboration, storage, and September–October 2013 Air & Space Power Journal | 40 Space Focus Senior Leader Perspective controlled environments for hosting network-based systems that support the service's missions.

Cyber Command and Control Mission System Weapon System

The Cyber Command and Control Mission System (C3MS) weapon system enables the Air Force mission by synchronizing the service's other cyber weapon systems to produce operational-level effects in support of combatant commanders worldwide. It provides operationallevel C2 and situational awareness of Air Force cyber forces, networks, and mission systems, enabling the Twenty-Fourth Air Force commander to develop and disseminate cyber strategies and plans; the commander can then execute and assess these plans in support of Air Force and joint war fighters.

Operated by the 624th Operations Center at Joint Base San Antonio–Lackland, Texas, the C3MS weapon system has crews consisting of a senior duty officer, a deputy senior duty officer, a defensive cyberspace watch officer, an offensive cyberspace watch officer, a DOD information network watch officer, three defensive cyber operations controllers, three offensive cyber operations controllers, three DOD information network operations controllers, a cyberspace effects planner, a cyberspace operations strategist, a cyberspace intelligence analyst, a cyberspace operations assessment analyst, and a cyberspace operations reporting cell analyst. All mission crews are supported by additional mission personnel.

The C3MS weapon system evolved from the legacy AFNet operations security center's concept, personnel, and equipment. With the activation of US Cyber Command and Twenty-Fourth Air Force, senior leaders recognized the need for an operational-level cyber C2 capability.

The C3MS is the single Air Force weapon system offering perpetual, overarching awareness, management, and control of the service's portion of the cyberspace domain. It ensures unfettered access, mission assurance, and joint war fighters' use of networks and information processing systems to conduct worldwide operations. The weapon system has five major subcomponents:

1. Situational awareness: Produces a common operational picture by fusing data from various sensors, databases, weapon systems, and other sources to gain and maintain awareness of friendly, neutral, and threat activities that affect joint forces and the Air Force.

2. Intelligence, surveillance, and reconnaissance (ISR) products: Enable the integration of cyberspace indications and warning, analysis, and other actionable intelligence products into overall situational awareness, planning, and execution.

3. Planning: Leverages situational awareness to develop long- and short-term plans, tailored strategy, courses of action; shapes execution of offensive cyberspace operations, defensive cyberspace operations, and DOD information network operations.

4. Execution: Leverages plans to generate and track various cyberspace tasking orders to employ assigned and attached forces in support of offensive cyberspace operations, defensive cyberspace operations, and DOD information network operations.

5. Integration with other C2 nodes: Integrates Air Force–generated cyber effects with air and space operations centers (AOC), US Cyber Command, and other C2 nodes.

Why Cyber Weapon Systems?

If we truly wish to treat cyberspace as an operational domain no different from air, land, sea, or space, then our thinking must evolve from communications as a supporting function to cyber as an operational war-fighting domain. To fly and fight effectively and to win in cyberspace, the Air Force must properly organize, train, and equip its cyber professionals. For many years, AFNet infrastructure and systems grew as a result of multiple communities adding components to suit their individual needs, often with end-of-year funds. Similarly, the components that now make up these six systems had no lead major command to articulate operational requirements and ensure standardized training as well as the effective management and resourcing of equipment life cycles.

Such an inconsistent approach made mission assurance and the defense of critical Air Force and joint missions in cyberspace nearly impossible. Migration to the AFNet has allowed the service to take great strides towards realizing the vision from nearly two decades ago of operationalizing and professionalizing the network. AFSPC championed the effort to identify these six systems' weapon systems and facilitate this move to a more disciplined approach. Formally designating these systems helps ensure proper management and sustainment of equipment life cycles. It also expedites the evolution of Air Force cyber professionals from a communications or information technology mind-set to an operational one replete with missionqualification training, crew force-management standards, and standardization and evaluation programs (where appropriate) to normalize cyber operations, as is the case with space and missile operations. Furthermore, formally designated weapon systems should help cyber receive the proper manning and programmatic funding necessary to ensure that the Air Force can fly, fight, and win in cyberspace.

The DOD construct for the management and resourcing of air, space, land, and sea superiority occurs via weapon systems. The best way to create and control effects in the cyber domain involves using the same weapon system construct to manage and resource cyber capabilities. Cyber weapon systems offer a path for the Air Force to operationalize, normalize, and ultimately standardize cyber, just as we have with the other war-fighting domains. The Air Force has been charged with securing, operating, and defending its portion of the DOD information networks and with defending Air Force and joint missions in the cyberspace domain. These cyber weapon systems give the Air Force a path to follow in normalizing operations to realize this goal.

The designation of cyber weapon systems created a separate cybersustainment funding line in the overall process of sustaining weapon systems. By normalizing the funding process, the service has instituted proper long-term planning and programming of sustainment funding, thus enabling more effective and efficient use of these limited resources, as compared to uncoordinated execution of unreliable end-of-year funds—key tenets to guaranteeing standardized configuration management and servicewide (and, where applicable, joint) interoperability. We are already realizing these benefits through the deployment of AFNet, whereby the Air Force enterprise has become easier to defend and the user experience continues to improve through ongoing standardization.

The benefits of designating cyberspace weapon systems are similar to those gained by weapon systems in other domains—it is the standard Air Force mechanism for organizing, training, equipping, and presenting mission capabilities. The weapon system construct allows the service to manage operational capabilities in a formalized approach and assure their standardization, sustainment, and availability to combatant commanders. When AFSPC personnel compared the air and space domains' normalization processes, they found that only the weapon system designation delivered the desired end state. Such systems may not always be ideally resourced, but they certainly receive better support than they would without designations.

Furthermore, designating cyberspace weapon systems directly supports AFSPC's role as cyber core function lead integrator, enabling the command to meet responsibilities listed in Air Force Policy Directive 10-9 and facilitating standardization across cyberspace platforms.[4] Designating these weapon systems is also critical to providing tactical units with the resources and training they need to operate in a normalized capacity. The core of cross-domain integration lies in the ability to leverage capabilities from different domains to create unique and decisive effects—if adequately resourced. Such designations will support proper evolution of the cyberspace domain and its relationship with the other operational domains—a critically important point because in modern warfare, cyberspace interconnects all domains. All of these

efforts to normalize and operationalize cyberspace operations and missions drive the Air Force towards the joint information environment (JIE) construct, standards, and processes. As the DOD, US Cyber Command, and services implement the JIE, they are also standing up cyber mission teams to support national, combatant command, and service specific cyber requirements. Designating these capabilities as weapon systems allows these teams to better support national and joint missions in, through, and from cyberspace.

Unique Challenges of the Cyber Domain

The air, land, sea, and space domains are natural areas—we didn't have to build them, as we did the tools to leverage those domains. Although none of the natural domains demands any maintenance, cyberspace predominantly exists within the equipment and devices designed, built, and configured by humans, requiring constant maintenance as equipment becomes outdated or worn out. Additionally, the way we construct cyberspace has a direct effect on our ability to operate and defend the domain. This aspect makes cyberspace unique in that its operation is just as important as its defense. We must constantly feed and care for the domain as well as innovate to stay ahead of or, preferably, drive the technology curve.

Defending cyber also presents its own challenges since an adversary can launch a cyber attack virtually without warning from any location on the globe. In the case of intercontinental ballistic missiles, we at least have sensors that detect the launch; thus, depending on the location of the launch, our forces have some modicum of warning and can respond. In cyberspace, attacks can occur without warning or time to craft and execute responses. The Air Force must develop capabilities to detect such attacks, prevent them if possible, and respond accordingly if required, just as it does in all other war-fighting domains. We must also develop the tools to leverage cyberspace for our own benefit. In reality, we may never be able to defend our networks completely—to do so would likely require so much security that we lose the force multiplying benefits that cyberspace offers to all of our missions. If we keep all adversaries out, most likely we will keep ourselves locked in. The key lies in finding a balance so that we effectively defend our networks and the missions that rely on them from attack yet leverage cyberspace for the benefit it offers those same missions.

Moreover, cyberspace is critical to Air Force and joint operations in the other war-fighting domains. Practically everything we do in warfare these days relies on cyberspace, be it providing telemetry to satellites and missiles or controlling our military forces in Afghanistan—we depend upon the cyber domain to execute operations in all of the other domains.

Designating cyberspace weapon systems calls for a tremendous resource commitment to meet the standards of air and space weapon systems. Operating to this higher benchmark requires corresponding funding and manpower greater than the cyberspace domain received as a simple communications or information technology support function. However, failure to make these commitments could prove devastating to future operations throughout every other domain. The operationalization of cyberspace is more than just a way for AFSPC to properly organize, train, and equip cyberspace forces—it is the logical evolution of cyberspace to a true war-fighting domain and a critical enabler of all other war-fighting operations.

Air and Space Operating Center Example

In the late 1990s, the Air Force designated the Falconer AOC a weapon system with little or no formal acquisition, sustainment, or requirements rigor to back it up. Basically, the chief of staff just made it a "go do." The operations community found itself backing into the requirements in much the same way we do today with our cyberspace systems. By declaring the AOC a weapon system, the Air Force sought to normalize what was basically a homegrown "county option" collection of equipment and personnel that varied from one numbered air force to another. This thinking held that a designated weapon system would result in better training for AOC crews, better defense of the program in the program objective memorandum process, and some protection of the numbered air force's staff manpower from poaching to fill AOC billets.

In reality, the AOC funding line has suffered numerous cuts, the equipment baseline has always been problematic in terms of sustainment and modernization, and AOC manpower has remained subject to several efficiency drills, ultimately shrinking the footprint. It stands to reason that many members of the operations community would argue that classification as a weapon system has not necessarily helped the AOC.

In Air Combat Command's opinion, though, in spite of the serious challenges faced during the transition, the AOC is better off today than it was 15 years ago, especially in terms of training its crews. A dedicated formal training unit at Hurlburt Field, Florida, established a program of record, provided a rigorous configuration and change management process, and ultimately resulted in recognition by the operations community that the AOC is the crown jewel in the joint force air component commander's tactical air control system C2 concept. Additionally, assignment to an AOC tour is no longer considered a career-ending event for rated officers—quite a change from the perception in the 1990s when an assignment to a numbered air force staff or an AOC was widely seen as the kiss of death for promotion in the rated career fields.

AFSPC would not let the initial pains of the AOC experience deter us from pushing the cyberspace weapon system concept forward. Every program (fighters, bombers, and ISR) confronted its fair share of challenges, but without a program—something with a name attached to it—cyberspace systems would always fight for scraps in money and manpower. As we integrate these cyberspace weapon systems into the Air Force construct, perhaps we can learn from the challenges of establishing the AOC weapon system and avoid the same pitfalls and mistakes.

Final Thoughts

Through the cyberspace domain, the United States exploits other war-fighting domains. Practically all warfare these days relies on cyberspace— everything from communications, precision navigation and timing, attack warning, ISR, and C2. Designating cyberspace weapon systems will help the Air Force guarantee persistent cyberspace access and mission assurance for other critical weapon systems and domains that rely on cyberspace. By doing so, the service has made a commitment that cyberspace will receive the programmatic and budgetary attention necessary to sustain cyberspace operations, support the cyber mission teams, and drive towards the JIE. Furthermore, cyberspace operations supported by core weapon systems offer increased security, performance, flexibility, and overall capability unmatched in a less normalized environment. The operationalization of cyberspace is more than just a way for AFSPC to properly organize, train, and equip the cyberspace domain—it is the logical evolution of cyberspace to a true warfighting domain and a critical enabler of all other such domains.

Notes

1. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (as amended through 15 June 2013), 303.

2. Joint Publication 3-13, Information Operations, 27 November 2012, II-9.

3. Mandiant, APT1: Exposing One of China's Cyber Espionage Units ([Washington, DC: Mandiant, 2013]), 2, 3, 20, 59.

4. Air Force Policy Directive 10-9, Lead Command Designation and Responsibilities for Weapon Systems, 8 March 2007.

Editor's note

We wish to thank the USAF's Air & Space Power Journal (ASPJ) for permission to republish General Skinner's article from their September–October 2013 issue, Volume 27, No. 5. You can access ASPJ at: ***http://www.airpower.au.af.mil***

BECAUSE VIDEO AND DATA ARE IMPORTANT TO YOUR NEXT MISSION

Media Technologies for Military and Government

Exclusive Training + Tour at NAB Show®

NAB Show presents a free, private event for Federal, State and Local government personnel, including all branches of the military, tasked with acquiring and moving media assets. You'll learn from broadcasting counterparts who are paving the way in this industry's technology.

Join attending colleagues from:

- NASA
- FEMA
- Federal Law Enforcement Training Center
- California State Senate
- Library of Congress
- FDA
- Department of Veterans Affairs
- Fairfax County Government
- Long Beach Fire Department
- FBI
- DoD
- DHS
- City of Greensboro Channel 13
- US House of Representatives
- State of Alaska DHSS
- CDC
- Federal Reserve Board
- Defense Media Activity
- NGIA
- All Military Branches and more

Topics and training include:

- Video and audio technologies
- Video standards
- Creating broadcast quality content
- Hardware and software demos
- Commercial solutions

FREE for all Military and Government Personnel With a Valid Government ID.

The insight you need to accomplish your next mission is here, at NAB Show, the world's largest digital media technologies marketplace.

MARK YOUR CALENDAR: Wednesday, April 9

Includes access to all exhibits and the Technology Luncheon.*

Registration opens early November.

**Luncheon included for the first 50 who register with code MG01*

NAB SHOW®
Where Content Comes to Life

Conferences: April 5–10, 2014 | **Exhibits:** April 7–10
Las Vegas Convention Center, Las Vegas, Nevada USA

www.nabshow.com

Join Us! #nabshow

PHOTO CREDITS: Department of Defense and Dvids Defense & Imagery Distribution System

CABSAT

www.cabsat.com

11 - 13 MARCH 2014

DUBAI WORLD TRADE CENTRE

NEW FEATURES. NEW TRENDS. NEW OPPORTUNITIES.

THE CABSAT CONFERENCE

CABSAT | NABSHOW

Save 25% on delegate registration before 30 Jan.
+971 4 308 64 81 ▮ Jake.Benitz@dwtc.com

CABSAT GLOBAL MEETINGS PROGRAMME

Exclusive, ROI elevating, one-to-one meetings platform for exhibitors and visitors

CONTENT DELIVERY HUB

CONTENT DELIVERY HUB

Lucrative exhibitor zone dedicated to multiscreen streamed and consumed content platforms & solutions

CABSAT CONNECT

Attend the launch of CABAST's new Networking Event Series at the exclusive Jumeirah Beach Hotel in Dubai. Limited spaces available. Register today at www.cabsat.com

VISIT FOR FREE

Register today:
www.cabsat.com/visit

BOOK EXHIBITION SPACE

Confirm now! Limited space
Tel: +971 4 308 6077/6282
Email: cabsat@dwtc.com

EARLY BIRD ALERT!

SAVE 25% on delegate registration before 30 January 2014
Tel: +971 4 308 6481
Email: jake.benitez@dwtc.com

CABSAT | NABSHOW

ACQUISITION & PRODUCTION | PRO / BROADCAST AUDIO | MANAGEMENT SYSTEMS | POST PRODUCTION | CONTENT & COMMUNICATION | DISTRIBUTION & CONTENT DELIVERY PLATFORMS | SATELLITE & COMMUNICATIONS

Organised by: DUBAI WORLD TRADE CENTRE

Proudly an ufi Approved Event

Official Publisher: ITP

Official Travel Partner: ALPHA TOURS

Knowledge Partner

Supported by: ABU, iabm, 6VF, SSPI, WTA, FOBTV

Get Involved
CABSATSHOW
CABSAT2014
CABSAT

Scan the QR code to register now