SATCOM For Net-Centric Warfare – February 2017

MilsatMagazine

MILSATCOM Concerns Interference

MilsatMagazine

February 2017

PUBLISHING OPERATIONS

Silvano Payne, Publisher + Senior Writer
Hartley G. Lesser, Editorial Director
Pattie Waldt, Executive Editor
Jill Durfee, Sales Director, Associate Editor
Simon Payne, Development Director
Donald McGee, Production Manager
Dan Makinster, Technical Advisor

SENIOR CONTRIBUTORS

Tony Bardo, Hughes
Simon Davies, Spectra
Richard Dutchik, Dutchik Communications
Chris Forrester, Broadgate Publications
Karl Fuchs, iDirect Government Services
Bob Gough, Carrick Communications
Jos Heyman, TIROS Space Information
Ryan Schradin, SES GS
Koen Willems, Newtec

AUTHORS

Martin Coleman
Roger Franklin
Ryan Schradin
Ted Vera

TABLE OF CONTENTS

ADVERTISER INDEX

MilsatMagazine is published 11 times a year by Satnews Publishers, 800 Siesta Way, Sonoma, CA, 95476, USA
Phone: (707) 939-9306, Fax: (707) 939-9235

Advantech Wireless

SMARTER SOLUTIONS, GLOBAL REACH.

Visit us at
Satellite 2017
Booth 1609

GOVERNMENT & MILITARY SOLUTIONS

ENABLING FASTER & MORE SECURE COMMUNICATONS FOR MILITARY & GOVERNMENT LEADERS

- Complete Military SATCOM Solutions
- Advanced GaN for Radar Applications
- Second Generation GaN Troposcatter Amplifiers

At Advantech Wireless, we have over 25 years of experience in helping military special forces and government agencies by delivering cutting-edge innovations in communications that solve mission critical communications challenges.

We understand the challenges that government & military forces face and our technologies bring them the freedom to communicate beyond line of sight quickly, reliably and securely.

WGS CERTIFIED

Multi Services
VSAT Solution

Second Generation
GaN based SSPAs/SSPBs

TROPOSCATTER Modular
Solid State GaN Power Amplifiers

Higher Power and higher Information rates for Mission Critical Operations

sales@advantechwireless.com

www.advantechwireless.com/gov

DISPATCHES

US DoD to Help Ensure Smallsats' Safety

A safe environment is desired by all within which to live their lives and ensure their property is secure… Sky and Space Global has now signed an agreement with the US Department of Defence (DoD) that will help to keep this Perth, Australia, company's smallsats safe in their spatial environs when they are launched the next quarter.

This agreement provides for space situational awareness services as well as real-time info to ensure safe, orbital surroundings for their smallsats.

Such responsibility encompassment includes a variety of safety contingencies that take into account collision avoidance, satellite de-orbiting, satellite re-entry and support for the spacecraft's end of life.

The launch of the Sky and Space Global nanosatellites will be handled by the Indian Space Research Organization (ISRO) and their Polar Satellite Launch Vehicle (PSLV), which just recently shattered the previous world record for the number of satellites carried aloft for launch — the ISRO managed 104 in number, and all but two of these smallsats were for foreign entities.

The build of the firm's smallsat prototype was completed last month and they have been undergoing testing and evaluation by Ayecka Communications, the manufacturer of the satellites.

The overall plan by the firm is have a full constellation of as many as 200 smallsats on orbit by mid-2018.

www.skyandspace.global

Aerojet Rocketdyne's New Vice President of Quality & Mission Assurance

John Schneider has been appointed vice president of Quality & Mission Assurance (Q&MA) at Aerojet Rocketdyne, a subsidiary of Aerojet Rocketdyne Holdings, Inc.

John succeeds Jerry Tarnacki who was recently named senior vice president of the company's Space Business Unit.

Schneider joined Aerojet Rocketdyne in July 1988 and has served in a variety of leadership positions over the last 28 years, most recently as site director for the Los Angeles facility since December 2013.

In his new role as vice president of Q&MA, Schneider will report directly to Chief Operating Officer Mark Tucker and will work closely with Aerojet Rocketdyne's 14 sites and various Space and Defense programs to drive continued implementation of the company's new operating system, build on the company's culture of quality, and improve Q&MA systems and processes across the enterprise.

"*John's exceptional attention to detail and his vast experience in operations and quality leadership make him a natural fit for this new role*," said Tucker. "*John has continuously instilled a 'value added' culture within the organization, resulting in demonstrated success in fulfilling customer expectations and driving performance goals.*"

Schneider holds a Bachelor of Science in Mechanical Engineering from Georgia Institute of Technology, and serves on the board of directors for the Aerojet Rocketdyne Foundation.

Aerojet Rocketdyne is a world-recognized aerospace and defense leader that provides propulsion and energetics to the space, missile defense and strategic systems, tactical systems and armaments areas, in support of domestic and international markets.

AerojetRocketdyne.com

DISPATCHES

Hughes Has BLOS for Choppers

Hughes Network Systems has announced that their Defense and Intelligence Systems Division (DISD) recently demonstrated a 360 degree, Beyond-Line-of-Sight (BLoS) SATCOM capability that transmits HD video through rotating blades on a NorthStar Aviation 407 Multi-Role Attack Helicopter.

This new advancement in SATCOM technology integrates the Hughes HM200 airborne modem and two lightweight antennas mounted on top of the helicopter's weapons platforms via an easy Roll-on/Roll-off installation. As a new lightweight capability—50 percent lighter than previous systems—the antenna can be adapted to any helicopter platform given its low Size, Weight and Power (SWaP) properties, giving pilots more flexibility and uninterrupted transmission of full motion HD video over a full 360-degree range.

The two advanced airborne terminals have very low SWaP constraints, providing a capability that enables NorthStar Aviation to quickly place the antennas at strategic low-risk locations on the helicopter without costly structural changes and re-certification. As result, users have the flexibility to integrate the 360-degree solution on an ever-growing variety of rotary wing platforms for missions that range from ISR gathering, to search and rescue, disaster relief, and other applications requiring live video feeds for situational awareness.

Wayne Marhefka, Senior Director at Hughes DISD, said, *"As a Roll-on/Roll-off system, the two antennas seamlessly hand-off the satellite signal based on aircraft position, with little to no feed interruption. Customers requiring real time SATCOM on helicopters will no longer have to worry about aircraft positioning in order to stream HD video or other data.*

defense.hughes.com/

DISPATCHES

Ready to Defeat the Threat of 'Cyber-Hackers'

Spectra Group (UK) has announced that the company is extending their Cyber Security division in order to give Small and Medium Enterprises (SME) similar options that are available to existing Government, Defence and Public customers in the fight against Cyber Attack.

Spectra has identified cyber services as the 'next huge growth area' and their Spectra Cyber Security Solutions has just debuted.

The Herefordshire-based company can build on their already extensive experience successfully designing, delivering and maintaining networks for military organizations and Government Agencies.

The firm's high grade solutions are designed to integrate seamlessly with business architecture, thereby minimizing downtime. Data is available as and when required and is kept secure and protected from attacks throughout its lifecycle.

Spectra Cyber Security Solutions can provide defense-in-depth, with proactive testing, to identify vulnerabilities in networks and procedures and protect data.

Spectra operates a Security Operations Centre (SOC) which provides 24/7/365 monitoring of networks to immediately identify any breach—or potential breach—as well as providing a UK based help desk. This enables clients to benefit from security monitoring and provides the user with a 24-hour contact, should they have concerns or issues with their network.

Spectra is ISO 27001-accredited which, as an information security management standard, is clear and precise, listing 114 key security controls that should always be at the heart of any organization's approach to security.

The company is also fully compliant with the UK Government-backed Cyber Essentials Scheme. Developed in conjunction with the Information Security Forum (ISF), Cyber Essentials forms a robust and stringent checklist that security companies must meet to be considered eligible to work with highly sensitive information and Government level security contracts.

Spectra is also a Cisco Partner—Cisco Select Certification recognizes and rewards partners that have achieved a Cisco specialization.

Cyber-attack has been identified as one of the four highest priority and most pervasive of risks faced by the UK—with the others being international terrorism, international military crises and major accidents or natural hazards.

In the last year alone, some two-thirds of large businesses in the UK experienced a cyber-attack and, staggeringly, almost a quarter fell victim to breaches at least once a month.

Simon Davies, CEO of Spectra Group (UK) Ltd, said, "*Without doubt, Spectra views cyber security services as the next growth area. We have already been delivering cyber services through our existing networks business so the launch of Spectra Cyber Security Solutions is a natural progression for the company.*

"*Among our talented employees are experts who possess all the knowhow and experience to deliver highly bespoke security solutions to protect against cyber-attacks. As data now plays an increasingly important part in everyday life, ensuring its confidentiality must be of paramount importance to any organisation.*

"*We recognize that not every company can afford to have a large, highly trained, IT department, and some need a straightforward pricing system to plan their business operations. Spectra Cyber Security Solutions aims to make keeping companies safe from cyber-attack as simple and cost-effective a process as possible.*"

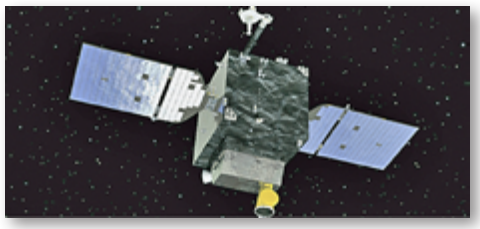
spectra-group.co.uk

Spectra's Slingshot, SlingShot is a unique system that converts UHF and VHF radio to satellite frequencies, enabling users to maintain real-time, tactical, Beyond Line of Sight (BLOS), communications in all situations and locations.

DISPATCHES

USAF's STPSat-6 Now Has Orbital ATK Involvement

Orbital ATK has been awarded a contract by the US Air Force Space and Missiles Systems Center to provide payload integration and support services for Space Test Program Satellite 6 (STPSat-6).



The multipurpose satellite will operationally demonstrate advanced communication capabilities, collect space weather data and support nuclear detonation detection in the Earth's atmosphere or in near space. STPSat-6 is the primary payload on the STP-3 mission which is set to launch no earlier than June 2019.

STPSat-6 will be built on an Orbital ATK satellite bus that will be modified to fit mission requirements. Under the contract, Orbital ATK will integrate and test the spacecraft, deliver operations procedures, and support launch and on-orbit check-out. The satellite will carry nine payloads from the Department of Defense, National Nuclear Security Administration and NASA.

The multiple payloads on board STPSat-6 include the Space and Atmospheric Burst Reporting System (SABRS-3), NASA's Laser Communication Relay Demonstration (LCRD), and seven experiments from the DOD Space Experiments Review Board. Orbital ATK's heritage bus and avionics product line is designed to support multiple payloads and can be adapted to support the customer's desired mission life.

The STP-3 mission is sponsored and managed by the Space Test Program (STP), which is the primary provider of spaceflight for the United States Department of Defense (DOD) space science and technology community. STP is managed by the Advanced Systems and Development Directorate of the Space and Missile Center.

Chris Long, the Vice President of National Space Systems at Orbital ATK, noted that this flexible and modular satellite bus platform provides an especially unique opportunity to host multiple instruments from three departments of government on one spacecraft, achieving customer goals at an affordable price.

DISPATCHES

Airbus Defence and Space Delivers MILSATCOM Support to Africa

Airbus Defence and Space is delivering satellite communications systems for EU military training missions in Somalia (EUTM Somalia) as well as for the EUCAP (European Union capacity-building mission) Sahel Niger and EUCAP Sahel Mali civilian missions.

Initiated on behalf of the European Union, these missions aim to support the efforts of the respective governments to strengthen their stability and to respond to the security issues faced by their populations.

Airbus Defence and Space teams have deployed C-band SATCOM systems between Europe and Somalia, Niger and Mali, as well as satellite-based mobile phone terminals to enable communications in Malian and Nigerien territories. Airbus Defence and Space supplies the ground equipment, communications services and airtime.

Airbus Defence and Space has been providing SATCOM services for the European Defence Agency (EDA) since 2012. Recently, the organization renewed its framework contract for the provision of SATCOM for another four years in order to meet the military and civilian requirements of the European missions.

This new EU SatCom Market contract now encompasses X-band and UHF-band military SATCOM services, in addition to commercial C-, Ku-, Ka- and L-band SATCOM services.

The EU SatCom Market agreement allows EU member states to consolidate their requirements and purchase satellite communication capabilities in a coordinated manner, thus ensuring more economical and reliable access to SATCOM services.

Approximately 20 ministries of defence in Europe and EU organizations are taking part in this project, which allows them to equip themselves with SATCOM solutions and services across the globe.

Satellite communications are a mission-critical instrument for connecting command and control centers, as well as intelligence, surveillance and reconnaissance (ISR) tools.

In light of the increasingly common use of high-throughput applications, like RPAS on battlefields, a great amount of SATCOM is needed to enable the control and transmission of data acquired by sensors.

In addition to covering the complete range of frequency bands (L-, C-, Ku-, Ka-, X- and UHF), the company provides military satellite communications to some of the most high-tech armed forces in the world, including those of the UK, France, Germany, Canada, the US and NATO.

Roland Van Reybroeck, Director Cooperation Planning and Support at European Defence Agency, related that the EU SatCom Market project has successfully developed since 2009 as a solution for interested Members States and EU entities to access better quality satellite communications services, under better economic conditions, with less burden.

This is a perfect example of how EDA can combine its industry knowledge, technical expertise and experience in procurement to support EU operations/missions and Member States in their procurement procedures and save scarce resources at no additional cost.

airbusdefenceandspace.com

eda.europa.eu/

DISPATCHES

Boeing is In Good with USAF

A five year agreement has been signed between Boeing and the US Air Force for Global Positioning Systems (GPS).

Artistic rendition of a GPS BLock IIF satellite. Image is courtesy of Boeing.

The company and the military organization signed a GPS sustainment agreement that will ensure the navigation capabilities relied upon by millions of military and commercial users remain robust for years to come.

Under the agreement, Boeing will support GPS IIA and IIF satellites for the US Air Force that are currently on orbit for the next five years.

Boeing, which has been the prime GPS contractor for more than 40 years, is now part of the Air Force effort that may lead to the next generation of GPS satellites. The Block IIA satellites are not currently in service, but some are retained as back-ups just in case there is an issue with more updated additions to the constellation.

Block IIF is the newest component of the constellation, with the last satellite launched in 2016. It currently transmits the bulk of GPS signals used by the military and civilians across the globe.

Collectively, Boeing GPS satellites have accrued more than 550 years of on orbit operation. In March 2016, the company delivered its 50th GPS satellite on orbit to the Air Force and has built more than two-thirds of the GPS satellites that have entered service since 1978.

"*This agreement continues Boeing's strong legacy of GPS innovation and mission support,*" said Dan Hart, vice president, Government Satellite Systems. "*We are focused on delivering reliable, affordable and resilient GPS capability now and for generations to come.*"

boeing.com/

DISPATCHES

GaN Gains for Advantech Wireless

Advantech Wireless has received a multi-million dollar contract from a NATO member country to provide their ruggedized military grade SATCOM terminals, including the new advanced line of GaN (Gallium Nitride) based Solid State Power Amplifiers.

The Advantech Wireless solution is designed for the most stringent environmental military standards and offers state-of-the-art performance with minimal size weight and power (SWaP).

Advantech Wireless is providing complete terminals for the tactical environment based on its proprietary antenna control systems and fully integrated design.

The Second Generation GaN based SSPAs/BUCs from Advantech Wireless feature exceptional linearity and operating efficiency.

These advanced systems are the smallest fully integrated units on the market today. With built-in design features they are perfectly suited for harsh environments, Satcom-On-The-Move (SOTM) and man-pack terminal deployments.

advantechwireless.com/

Japan's SDF Obtains X-Band Defense Satellite

The Japan Aerospace Exploration Agency (JAXA) and Mitsubishi Heavy Industries, Ltd., have launched an X-band defense communications satellite aboard a H-2A Launch Vehicle No. 32 from JAXA's Tanegashima Space Center in Japan's southwestern Kagoshima prefecture.

The Kirameki-2 satellite is the first communication satellite for the Japanese Ministry of Defense, which shoulders the mission to upgrade the Self-Defense Forces' (SDF) communications network. The Kirameki-2 satellite, operating with X-band technology, is one of three defense communications satellites which will replace three civilian satellites that are presently used by the Self-Defense Forces.

The new satellites will facilitate direct communication among units of the Ground, Maritime and Air Self-Defense Forces through a high-speed and high-capacity network and serve as a communication infrastructure, local media quoted Defense Ministry officials as saying on Tuesday.

The Kirameki-2 is designed to operate over the Indian Ocean and to serve the SDF personnel taking part in U.N. peacekeeping operations in South Sudan and the anti-piracy mission in waters off Somalia, said the officials. In 2008, Japan's Diet approved a law on general principles for the use of space, allowing non-aggressive defense use of space and overturning a decades-old policy of limiting space development to peaceful uses.

Under the law, the use and exploitation of space should be conducted to serve the security of Japan, relaxing the principle of nonmilitary use based on a parliamentary resolution in 1969 under the war-renouncing Constitution.

The new law changes Japan's policy of space use to "non-aggression" from "non-military" and would allow Japan's defense ministry to launch its own satellites, including surveillance satellites and an early-warning satellite.

global.jaxa.jp

h2a.mhi.co.jp/en/

33RD SPACE SYMPOSIUM

SPACE FOUNDATION

The Broadmoor Hotel, Colorado Springs, Colorado USA

April 3 - 6, 2017

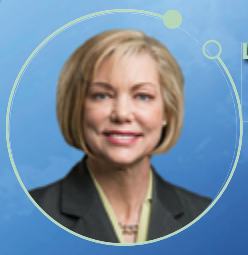
Join Us for 2017's Top Global Space Conference!

Where the World Convenes to Discuss and Shape the Future of Space

Featuring...

Elżbieta Bieńkowska
Commissioner
European Commission

Lt. Gen. David J. Buck, USAF
Commander, 14th Air Force, Air Force Space Command
Commander, Joint Functional Component Command for Space
U.S. Strategic Command



Lynn Dugle
Chief Executive Officer
Engility

Gen. David L. Goldfein, USAF
Chief of Staff
U.S. Air Force

Alan Stern, Ph.D.
Principal Investigator
New Horizons Mission
CEO
Uwingu

We Deliver!

- Targeted Tracks and Plentiful Networking Events
- The Newest in Global Space Technology
- Industry Leaders and Decision Makers

Featured Panel

NASA Center Directors in a Time of Transition

Moderator: David Livingston, DBA, Founder and Host of "The Space Show"

Panelists:

- **Robert D. Cabana,** Director, NASA John F. Kennedy Space Center
- **Janet Kavandi, Ph.D.,** Director, NASA John H. Glenn Research Center
- **Todd May,** Director, NASA Marshall Space Flight Center
- **Ellen Ochoa, Ph.D.,** Director, NASA Johnson Space Center
- **Christopher J. Scolese,** Director, NASA Goddard Space Flight Center
- **Michael Watkins, Ph.D.,** Director, NASA Jet Propulsion Lab

Still Time to Save!
On Standard Industry Registration
Discount ends soon!

Reduced Pricing!
Active Duty Military and Government

Official Media Partner

satnews
Satellite News - SatMagazine - MilsatMagazine

www.SpaceSymposium.net

+1.800.691.4000

AUTOMATING FOR AN INTERFERENCE-FREE SPACE ENVIRONMENT

By Roger Franklin, Chief Executive Officer, Crystal

If you are a regular reader of *MilsatMagazine*, you may have already "seen" me banging the drum for why the military should be using Carrier ID to enable quick and easy resolution of satellite interference.

I still believe that it would make a massive difference, both for those specific users and for the space environment as a whole. However, I also think that better automation throughout the process will be a game changer and it is something the entire industry should be aiming towards.

MILITARY INTERFERENCE

Naturally, as one of the biggest users of satellite technology, the military sees (and contributes) their fair share of interference. In some cases, this interference can be inconvenient, perhaps causing the user to switch satellites or to suffer a degraded service. In other cases, the effect is much more significant, with vital communications potentially lost altogether. When we consider the nature of military operations, that can, quite literally, be a lost lifeline.

Generally, when interference occurs, military users will either increase the output to mask the problem or point to a different satellite. Both of these solutions could potentially cause interference to other users, so of course, these moves are not ideal.

This is however, a natural response, given that in many circumstances, restoring communication can be extremely time-sensitive—this means the military user will be seeking the most immediate, on-the-spot resolution of the interference.

In some cases, the satellite operator will be contacted to resolve the interference, especially long-term cases. The operators are developing tools to enable this, with ways to identify interfering VSAT terminals without the need for CID. This would allow the terminal operator to be informed and the interference halted.

Of course, for the military user, unsure of being identified through CID, that is a daunting prospect. However, these tools are only used by the satellite operator and, as with CID, data would not be visible to, or shared with, any other party. As I've said before, not being identifiable makes you instantly recognizable as a military user.

The other area that makes the military a particularly tricky area for satellite communications is the fact that military personnel change frequently. A new rotation could see someone who has never handled satellite equipment before, in charge of all satellite transmissions. A certain amount of training would naturally be given, but a lot of the expertise needed for satellite equipment comes from years of experience in the field.

Of course the other challenge is that most military personnel won't solely be in charge of the satellite communications, especially when in active duty, with a whole host of roles and responsibilities.

THE ROLE OF AUTOMATION

With so many other areas to concentrate on, and very little margin for error, what the military satellite users really need is a way in which everything can be done, checked, and tested automatically, without any need for intervention by the personnel.

I have often talked about automation being a significant tool in reducing interference. This is important, as most interference is caused by human error so naturally the more we automate, the more we can reduce that chance of error and the amount of interference will be instantly reduced. It is also important for reducing other types of error, not just interference, making processes much more efficient, as well as requiring much less manpower to operate.

With a growing number of hybrid networks, with multiple distribution paths, automation is increasingly important to optimize the delivery of content or communications over the best path in any given situation or at any given time.

An intelligent system can analyze a number of different parameters to determine which path that should be. For those users with CID, automating also ensures that the CID information is always included in your transmissions and displayed correctly.

As well as automating systems, we should be continually monitoring them—24 hours a day, 7 days a week, and 365 days a year. It is especially critical in a military environment that every piece of equipment is monitored, wherever it is in the world, and that errors are flagged up before they become a problem with significant consequences.

Constant monitoring will identify when a piece of equipment is having a temporary glitch or if a terminal is out of alignment. The goal is that issues are responded to and resolved before the effects are felt. If a monitoring solution is used with a recording feature, then problems can later be reviewed for training purposes, helping to ensure the issue is not repeated.

"AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE"

I think most satellite users would agree with Ben Franklin on this sentiment, particularly as it pertains to interference. Although tools to rectify some unexpected interference will remain important, it is much better to prevent it from the onset, when able.

Automation and continual monitoring can drastically reduce errors occurring in the first place and make transmissions much more efficient, ultimately saving time and money, keeping users connected—no matter where in this increasingly dangerous environment they may be operating.

crystalcc.com

Roger Franklin is the President + Chief Executive Officer of Crystal Solutions. He began working for Crystal Solutions at 15 years of age. By age 17 he had exhausted the mathematics offerings of high school and, before completing his senior year, enrolled at Oglethorpe University. Transferring to the Georgia Institute of Technology, he graduated in only three years. Roger has remained with Crystal Solutions and holds a number of positions with increasing responsibilities. He gained experience in all facets of the business, with particular emphasis on product development. Roger acquired the business in 2007.

CYBERSECURITY BEST PRACTICES FOR... SMALLSAT GROUND NETWORKS

By Ted Vera, Business Area Manager, Cybersecurity Lead, RT Logic, a Kratos Company

With numerous examples in the news, there shoud be no surprise that cybersecurity attacks are on the rise.

Verizon's *2016 Data Breach Investigations Report* summarizes 64,199 cybersecurity incidents including 2,260 breaches with confirmed data loss that occurred during 2015 alone[1].

Intel Security / McAfee's conservative estimate of the annual cost to the global economy from cybercrime is more than $375 billion in losses[2]. These attacks targeted all types of public and private organizations and industries, highlighting the fact that there are no network connected systems that are immune from online threats.

Smallsat ground networks are no exception—they, too, are exposed to an increasing number of targeted cyberthreats, including those attempting to exploit vulnerabilities not found in most traditional Information Technology (IT) network environments.

This article is intended to be a security primer for smallsat ground network operators, military or commercial, and discusses security best practices, such as Information Assurance (IA) hardening and continuous monitoring; leveraging frameworks such as Defense Information Systems Agency (DISA) Security Technical Information Guides (STIGs); and tools such as Security Information and Event Managers (SIEMs) and Security Content Automation Protocol (SCAP) compliant applications.

MISSION-UNIQUE ATTACK SURFACE

Ground networks have unique cybersecurity challenges such as: mission-unique equipment and applications, specialized protocols; high regression test costs and tight budgetary constraints. Mission-unique equipment found in satellite ground networks primarily consists of radio frequency (RF) signal processing gear and test equipment such as oscilloscopes, spectrum analyzers and channel simulators.

Specialized protocols and applications include Software Defined Radio (SDR) and Command and Control (C2) suites among others. These niche devices, applications and protocols present unique attack surfaces for potential exploitation. As end-to-end IP architectures become mainstream in smallsat ground networks, additional security challenges are introduced.

Unlike traditional network environments, which are primarily concerned with IP based attacks, satellite ground networks also need to consider RF based threats. For example, in addition to Internet based scans, amateur satellite enthusiasts are on the constant lookout for new satellite feeds detectable using low-cost commodity RF hardware and open-source software.

> **Smallsat Tip**: Attacks like this demonstrate that, when possible, it is important to encrypt not only command and control links, but also telemetry / downlink channels. Even simplex telemetry containing unencrypted metadata can lead to potential exploits.

One such exploit is described in a report by Kaspersky Labs which claims that a Russian-speaking spy gang known as Turla uses hijacked satellite IP addresses of legitimate users, sent as unencrypted metadata, to steal data from

other infected machines in a way that hides their malware command and control server[3].

RESOURCES AND BEST PRACTICES

Recognizing that smallsat ground network operators may lack the resources and budgets of traditional satellite operators, it is beneficial to leverage lessons learned, along with frameworks, and tools from Government and Industry to help better defend their networks.

The NIST Special Publications (SP) library provides a wealth of information and resources that can be leveraged by smallsat ground network operators who are just getting started developing a security program. The SP800 series consists of Computer Security related guidelines, recommendations and reference materials. The new SP1800 series Cybersecurity Practice Guides provide practical user-friendly guidance to help public and private sector users adopt a standards-based cybersecurity approach.

SECURITY PROCESS

Before diving into the technical controls that are often the initial thought for network engineers, a solid security program must include policies and procedures to help manage the security needs of the organization. NIST SP guides and frameworks can be used to help establish and drive policy. Tools, such as the Risk Management Framework and Contingency Planning Guide, can help an organization get a strong starting point for security and IT infrastructure beyond purely hardware related controls.

An overview of the Risk Management Process is contained in ***NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems***. The Risk Management Framework is an iterative process consisting of the following six steps: Categorize, Select, Implement, Assess, Authorize, and Monitor, as illustrated in ***Figure 1*** on the following page.

Figure 1: Risk Management process step.

Step 1: Categorize the information systems and the information they process, store and transmit, based on a risk/impact analysis.

Step 2: Select the baseline security controls and tailor as needed to meet the organization's risk assessment.

Step 3: Implement the selected security controls and document how they are employed within the information system and its operational environment. DISA STIGs and SCAP tools can be used to help automate and document portions of this step.

Step 4: Assess the security controls to ensure they are implemented correctly. Assessment can be accomplished using automated vulnerability scanners (*i.e.*, Nessus) or through manual inspection and validation. DISA STIGs and SCAP tools can be used to help automate and document portions of this step.

Step 5: Authorize operation of the information system based on determinationthat residual risk is acceptable to the organization.

Step 6: Monitor information system security controls on an ongoing basis Practice good configuration management to document changes to the system and operational environment. SIEM and SCAP tools can help automate and document portions of this step.

Smallsat Tip: Each step in the process can be tailored to meet the specific needs of the organization.

SYSTEM HARDENING

NIST 800-53 provides general guidance for security controls; however controls do not always translate easily into actionable items that can be implemented on a system.

DISA Security Requirements Guides (SRGs) are a compilation of Control Correlation Identifiers (CCIs) which break down NIST SP 800-53 controls into actionable items, grouped into specific technology areas such as operating systems, applications, networking devices, and policy.

DISA STIGs are validated hardening guides, updated quarterly for major operating systems, applications and network hardware. Configuring systems in accordance with applicable STIGs can help to remove or mitigate configuration vulnerabilities present in satellite ground network devices.

The DISA STIG Viewer is a freely available tool that can be used to complete and document STIG checklists while implementing system security controls. Download it at:

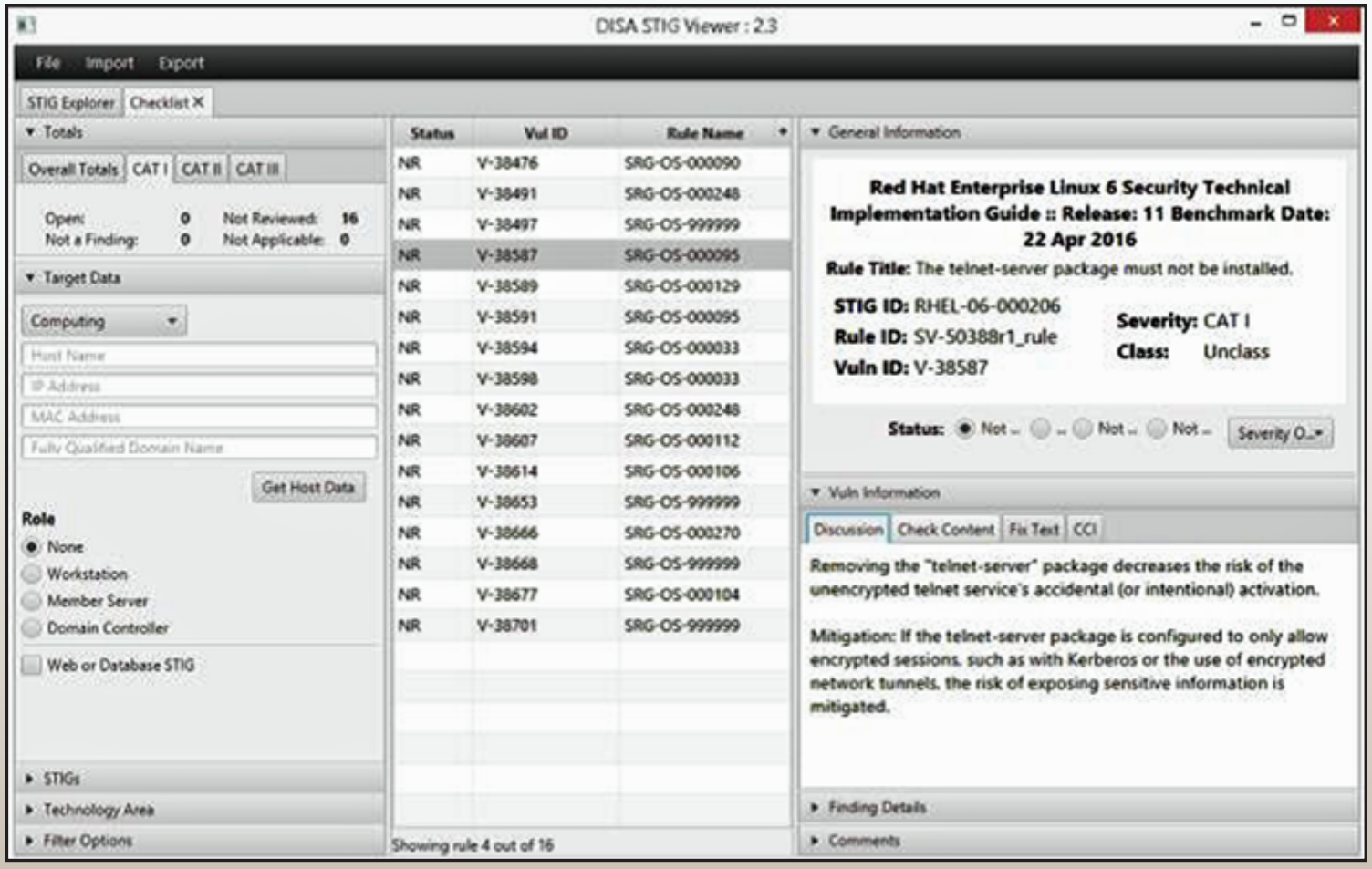
iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

CONTINUOUS MONITORING

SIEMS are a product class that can help organizations meet their continuous monitoring requirements through real-time event processing, alerting and reporting. Included in this category are CyberC4:Alert and CyberC4:Guard from RT Logic, a Kratos Subsidiary.

CyberC4:Alert, the first SIEM designed for satellite networks and operations, provides real-time cyber situational awareness for satellite ground networks; and CyberC4:Guard to protect satellite control-related communications across unclassified and classified domains within secure networks.

The use of SIEMs in the commercial sector has become an industry-accepted best practice for monitoring security risks. Real-time alerting helps mitigate the risks associated with vulnerable mission-unique equipment, specialized protocols, untimely patching, and deprecated protocols. Furthermore, scripted active response capabilities allow an organization to fight through a contested network environment.



Smallsat Tip: Challenges associated with implementing a SIEM for a smallsat ground network include: developing custom plug-ins for mission-unique equipment; monitoring specialized protocols, and writing rules and scripts for active responses to detected threats.

Smallsat systems are vulnerable to cyber threats and care should be taken as ground networks are designed. The guidelines and tools presented in this article can help secure smallsat ground networks from potential hackers and cyber threats.

Ground operators can benefit from the resources and tools that are broadly in use among Government organizations. NIST Special Publications provide a solid framework for establishing a comprehensive security program.

DISA STIGs and tools can be used to perform and document information assurance hardening of smallsat ground network devices and applications.

Security Information and Event Managers and SCAP compliant tools help the organization to continuously monitor security controls on an ongoing basis.

Ted Vera is a Business Area Manager and Cybersecurity Lead at RT Logic, a Kratos company.

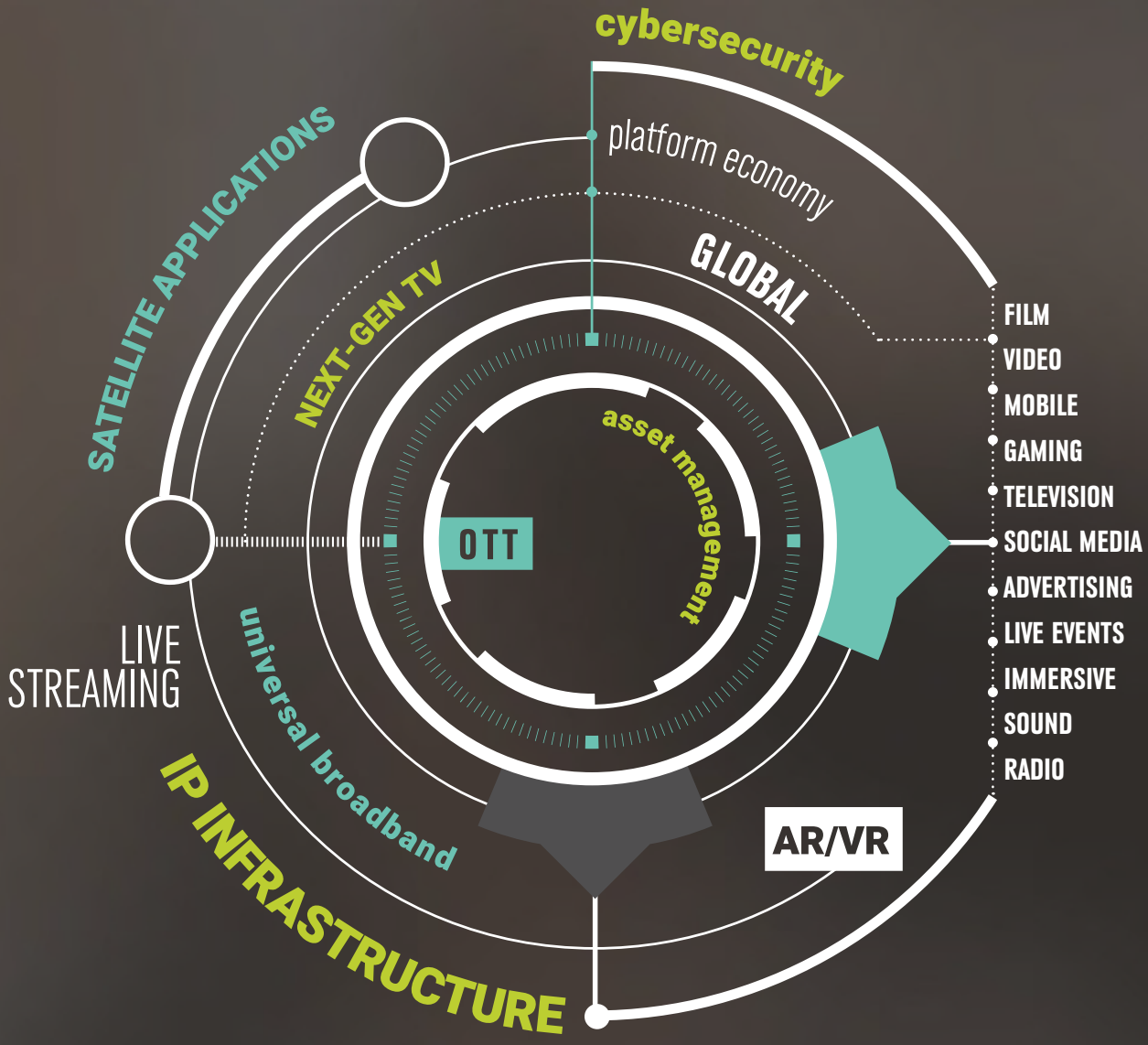
REFERENCES

[1]*Verizon, "Verizon 2016 Data Breach Investigations Report," Basking Ridge, New Jersey, April 2016*

[2]*Intel Security / McAfee, "Net losses: Estimating the Global Clost of Cybercrime," Santa Clara, California, June, 2014*

[3]*Tanase, S., "Satellite Turla: APT Command and Control in the Sky," September, 2015*

Editor's note: *This article originally appeared in the February issue of SatMagazine. Due to the content's relevance to the military/agency/government MILSATCOM segments, the feature has been repurposed for this issue of MilsatMagazine.*



THE M.E.T. EFFECT℠

MEDIA. ENTERTAINMENT. TECHNOLOGY.

NABSHOW®

Where Content Comes to Life

APRIL 22–27, 2017

LAS VEGAS, NV USA • NABShow.com

REGISTER TODAY: FREE EXHIBITS PASS

Use Code: PA164

ENTER THE NEW DIGITAL ECOSYSTEM

Technology is evolving faster than humankind itself. And we're living in a world of our own invention. Behavior and business have merged to redefine content, workflows and revenue streams. It's The M.E.T. Effect℠, a cultural phenomenon fueled by hybrid solutions and boundless connectivity that's changing the very nature of how we live, work and play. **At the center of it all is NAB Show®.**

LET'S THRIVE.

THE GOVERNMENT SATELLITE REPORT INSIGHTS

A NEW APPROACH TO MILSATCOM

Presented by Ryan Schradin, Executive Editor, The Government Satellite Report, and MilsatMagazine Senior Contributor

The United States Air Force is currently conducting a series of programs called the Commercial Satellite Communication (COMSATCOM) Pathfinders.

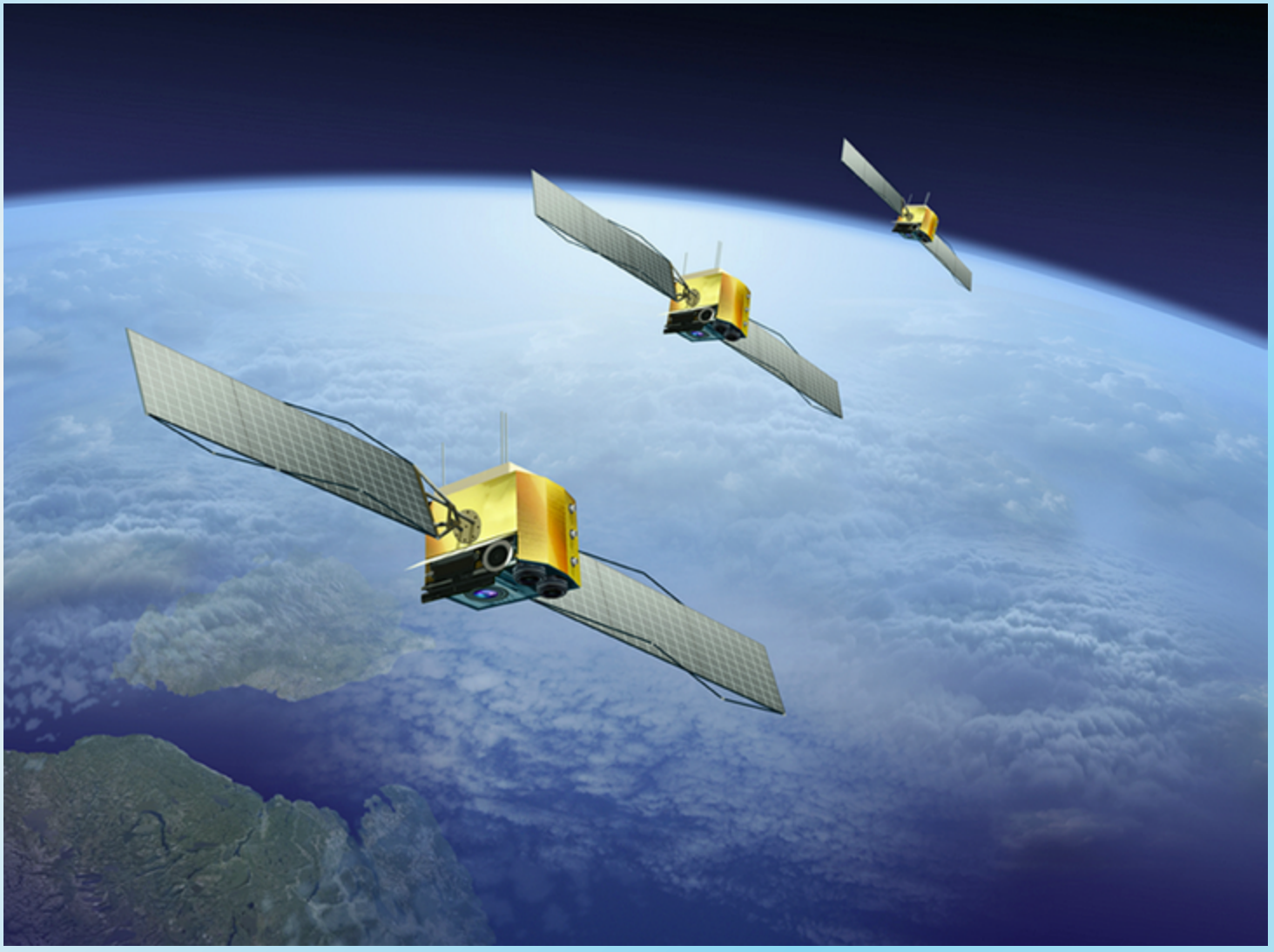
The COMSATCOM Pathfinders are a five-phase project to enable DoD to acquire COMSATCOM using innovative, longer-term approaches that should yield increased efficiency and effectiveness.

The COMSATCOM Pathfinder Initiative explores multiple facets of flexible, long-term investment-based acquisition models for access to commercial SATCOM capabilities and infrastructure from a diverse supplier base, including identifying any legal, policy, regulatory, management, cultural, or other barriers to government adoption of such business models at scale.

Each Pathfinder is an independent program and builds off previous efforts. Ultimately, the COMSATCOM Pathfinders will be referenced as the DoD completes its Wideband Communication Systems Analysis of Alternatives (AoA).

The first Pathfinder Program, coined Pathfinder One, involved the purchase of transponders and capacity aboard a SES GS-owned satellite. This marked a departure in how the military paid for and acquired COMSATCOM services. It also involved the use of traditionally cheaper satellite alternatives – inclined satellites.

"*Pathfinder One changed the way the DoD purchased COMSATCOM capabilities by procuring transponders on a commercial satellite versus the traditional model of leasing bandwidth on the spot market,*" said Pete Hoene, the CEO of SES GS. "*This solution included the utilization of inclined*



satellite capacity which allowed the government to pay significantly less than traditional station-kept bandwidth."

Inclined satellite capacity is often cheaper than geostationary (GEO) satellite capacity because of the nuances required to take advantage of it.

Inclined satellites are effectively older GEO satellites that are in the later stages of their operational lives. To maximize their remaining fuel, operators reduce station-keeping adjustments and extend the life by allowing the spacecraft to drift in the north/south direction. The square box that GEO satellites usually sit in becomes a rectangle and the satellite drifts in an elongated figure eight pattern within that box.

This north/south movement around the Equator is what makes inclined satellite capacity unique. The movement of these satellites requires a tracking antenna that can follow them as they move in their rectangular box. As you might imagine, there are many satellite use cases that call for tracking antennas, such as USAF planes.

According to Mr. Hoene, "*As remotely piloted aircraft (RPAs) have antennas capable of tracking inclined satellites, AFRICOM can use Pathfinder One capacity to support MQ-1 (Predator), MQ-9 (Reaper), and RQ-4 (Global Hawk) operations. In fact, United States Africa Command (AFRICOM) approved the use of inclined capacity on these platforms and is currently using the available Pathfinder One bandwidth to command and control their critical RQ-4 Global Hawk Intelligence, Surveillance, and Reconnaissance missions…*"

Pathfinder One was a success for the Air Force, and it's clear that the military took notice of the program's accomplishments. However, the military may not have been the only organization to observe the lessons learned from Pathfinder One. Private industry recognized the innovative use of inclined orbit bandwidth as well.

Just a few weeks ago, an article was published that disclosed that Global Eagle Entertainment, one of the world's leaders in in-flight entertainment, "*…had purchased all the capacity on an undisclosed satellite to support aeronautical customers, in particular Southwest Airlines, the company's largest customer.*"

Artistic rendition of the SES AMC-3 satellite.

That satellite was revealed to be SES satellite AMC-3, which carries 24 Ku-band transponders and launched in September 1997 on an Atlas 2A rocket."

SES will operate the satellite and provide support for Global Eagle.

What does that have to do with Pathfinder One? Well, it's pretty much the same situation. Global Eagle Entertainment is effectively purchasing the capacity onboard an inclined satellite.

Also, much like Pathfinder One, the satellite in question will be used for a purpose that is a perfect fit for inclined capacity—in-flight entertainment (IFE) onboard airplanes already fitted with tracking antennas.

The Global Eagle announcement illustrates the benefits that inclined satellites could have for both private enterprise and the federal government.

This could become a best practice to use this less-expensive capacity in any implementation or use case where tracking antennas are already being utilized.

Whether it's on Navy ships, RPAs or airplanes, inclined bandwidth could be an economical, effective way to deliver connectivity and communications on the move.

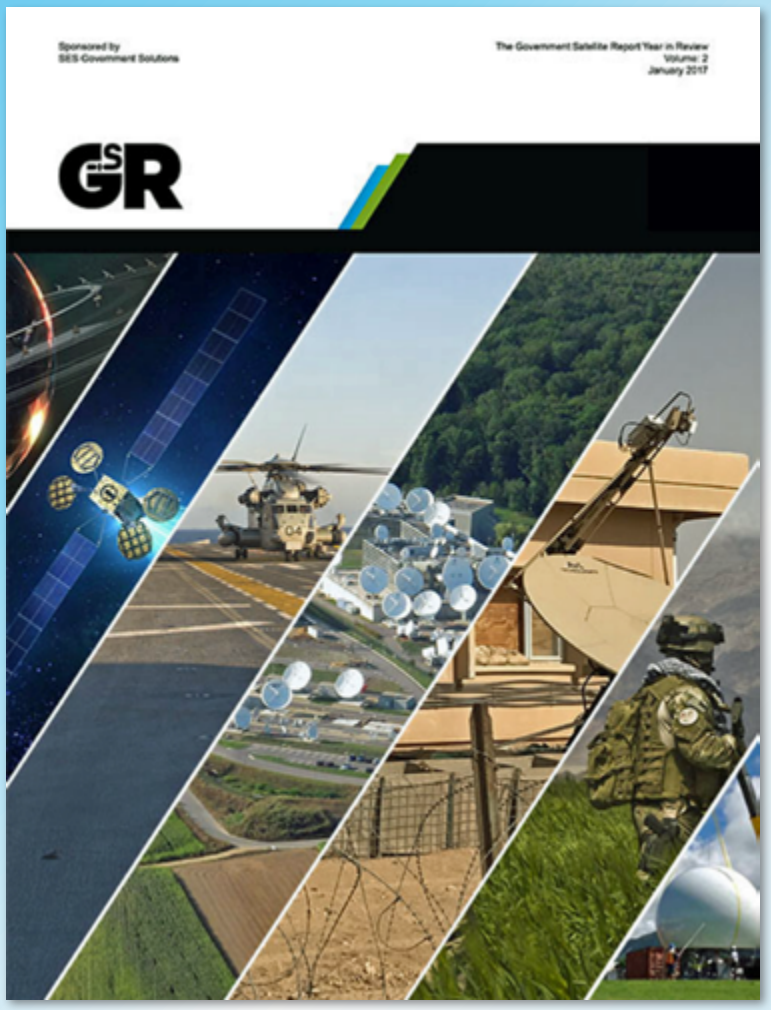
There's a two-part podcast series on the Pathfinder Programs that can be accessed at
ses-gs.com/govsat/tag/pathfinder-podcast/

SES GS President Pete Hoene wrote that ***The Government Satellite Report*** launched just two years ago, in 2015. The timing of this new, government satellite publication could not have been better.

The past couple of years have been an exciting time for the satellite industry. New technologies, increased demand for satellite-enabled solutions and the introduction of revolutionary, innovative players to the industry has the government watching the skies and looking to our commercial satellite industry for solutions.

There are many reasons for this renewed interest and focus on SATCOM. The desire to quickly have advanced capabilities and services everywhere—including on the move and at the tactical edge—has created a renewed need for resilient satellite services that can deliver incredible bandwidth, with lower latency and extremely high throughputs.

Simultaneously, the adoption of next-generation High Throughput Satellites (HTS) and the emergence, and subsequent expansion, of MEO constellations across the



satellite industry will ensure that our market is prepared and poised to meet the challenges of a more sophisticated and demanding customer.

These same technologies also make COMSATCOM more accessible and cost effective for the government as it looks to satellite to deliver mission-critical communications across the globe.

The advancement and proliferation of space capabilities continued in 2016, as did the sober realization that traditional US government owned and operated systems may be vulnerable to service denial, disruption or degradation. The space environment is certainly not the benign environment it once was. That has caused our government and military leadership to seriously consider integrating additional commercial capabilities.

For example, by systematically leveraging a commercial satellite architecture and utilizing commercially hosted payloads, the US government could leverage an architecture poised to provide capability across the range of operational needs. As an example, 2016 saw the introduction of multiple exciting hosted payload programs across the government —including NASA's GOLD program and the FAA's WAAS program.

Many experts and satellite owner-operators—including SES—are anticipating near-record demand for satellite services across global governments in 2017 and beyond. The US Department of Defense (DoD), seeing the need to evaluate it's future space architecture, launched an innovative Analysis of Alternatives (AoA) to fully examine their options. The commercial satellite industry figures to weigh heavily in that analysis.

Winston Beauchamp, Deputy Undersecretary of the Air Force for Space, relayed the following at a round table discussion at the World Policy Institute last year, "*Today we build a military satellite constellation, and if we run out of capacity we lease more from the commercial world. But that may not be the best solution in the future. Instead we may want a balance of both commercial and military so that we give incentive from industry to build additional mission assurance and resilience measures into their architecture. By inviting our partners to weigh in in the analysis of alternatives, we can vastly improve our mission assurance.*"

The Government Satellite Report remains committed to bringing you the latest satellite news, editorial glimpses into the trends driving commercial satellite adoption, discussions about the latest satellite technologies and insightful interviews with government and satellite industry leaders in 2017. But first, here is a look at some of the articles that our readers found most compelling in 2016. Thank you for being a loyal reader.

Download the *Government Satellite Report*'s ***Year in Review for 2016*** by selecting this URL:
ses-gs.com/govsat/resources/government-satellite-report-year-review/

ses-gs.com/govsat/

These articles are republished, courtesy of The Government Satellite Report (GSR) and Executive Editor ***Ryan Schradin****. He is a communications expert and journalist with more than a decade of experience and has edited and contributed to multiple, popular, online trade publications that are focused on government technology, satellite, unified communications and network infrastructure. His work includes editing and writing for the GovSat Report, The Modern Network, Public Sector View, and Cloud Sprawl.*

His work for the Government Satellite Report includes editing content, establishing editorial direction, contributing articles about satellite news and trends, and conducting written and podcast interviews. Ryan also contributes to the publication's industry events and conference coverage, providing in-depth reporting from leading satellite shows.

The Government Satellite Report is sponsored by...
SES Government Solutions

REGISTER BY 31ST JANUARY FOR A £200 DISCOUNT • REGISTER BY 28TH FEBRUARY FOR A £100 DISCOUNT

SMi
LINKING BUSINESS *with* INFORMATION

SMi Group Proudly Presents its 12th Annual Conference on...

Military Space Situational Awareness

26th - 27th APRIL 2017

Overcoming Key Situational Awareness Challenges in an Increasingly Contested, Congested and Competitive Space

Copthorne Tara Hotel London Kensington, United Kingdom

CHAIRMAN:

Allen Antrobus, Space Security Delivery Manager, **UK Space Agency**

EXPERT SPEAKERS:

Colonel Scott Trinrud, Chief, Space Policy Division, **US Strategic Command**

Colonel Jeff Dooling, Director Space Requirements, Director-General Space, **Canadian Forces**

Colonel Franck Schrottenloher, Commander, Environmental Control Office, **French Joint Space Command**

Colonel Rafal Borek, Chief of Section, Defence Projects Department, **Polish Space Agency**

Wing Commander Rayna Owens, AS Strat 4, **UK MoD**

Charlotte Wiin Havsteen, Branch Chief, Defence Centre for Operational Oceanography, **Danish Defence Acquisition and Logistics Organization**

Lieutenant Colonel Jaime Sanchez Mayorga, Head of Space Programs Unit, **Spanish MoD**

Major Bernie Buijs, Lead RNLAF Space Office, C4ISR/Space, **Royal Netherlands Air Force**

Nicolas Bobrinsky, Head of the SSA Programme, **European Space Agency**

Simon Machin, Met Office Space Weather Operations Centre (MOSWOC) - Defence Space weather Lead, **Met Office**

Dr Francis Chun, Head of the Center for Space Situational Awareness Research, **United States Air Force Academy**

Dr Clezio Marcos De Nardin, Head of the Embrace Space Weather Program, **Brazilian Space Agency**

Johan Kohler, Head of Solar System Science, **Swedish National Space Board**

Professor Thomas Schildknecht, Astronimical Institute, **University of Bern**

Dr Alex Ellerey, Professor, **Carleton University**

Dr Stephen Hobbs, Director, Cranfield Space Research Centre, **Cranfield University**

EVENT HIGHLIGHTS:

1. **Hear from new countries** seeking to develop their space programmes such as Poland, Denmark, the Netherlands and many more
2. **Learn from leading nations** such as USA, UK, France, and Canada on how they continue to enhance space security through Space Domain Awareness technologies
3. **Discuss key topics** that affect space situational awareness; from space-borne sensors to effective information management systems
4. **Gain a unique insight** into the challenges faced beyond the atmosphere and how defence forces and industry are striving to overcome them

www.military-space.com/MAsatnews

Register online or fax your registration to +44 (0) 870 9090 712 or call +44 (0) 870 9090 711

SPECIAL RATES AVAILABLE FOR MILITARY AND GOVERNMENT REPRESENTATIVES

CPD CERTIFIED The CPD Certification Service

@SMiGroupDefence
#milspace2017

A CASE OF MILITARY INTERFERENCE

By Martin Coleman, Executive Director, the Satellite Interference Reduction Group (IRG)

Maintaining assured and reliable satellite communications links across both commercial and military sectors is critical—technology plays a big part in that endeavour.

In my role at the Satellite Interference Reduction Group (IRG), the pain of satellite interference of course takes center stage and our job is supporting the industry to develop new technology, processes, and initiatives to combat it. The technology that has come out of that work in recent years, from both from our members and others, is already a game-changer and we now have the potential to make a huge impact in reducing satellite interference. However, most of that technology does far more than that, delivering a much more reliable, efficient and cost-effective service for users and satellite operators alike.

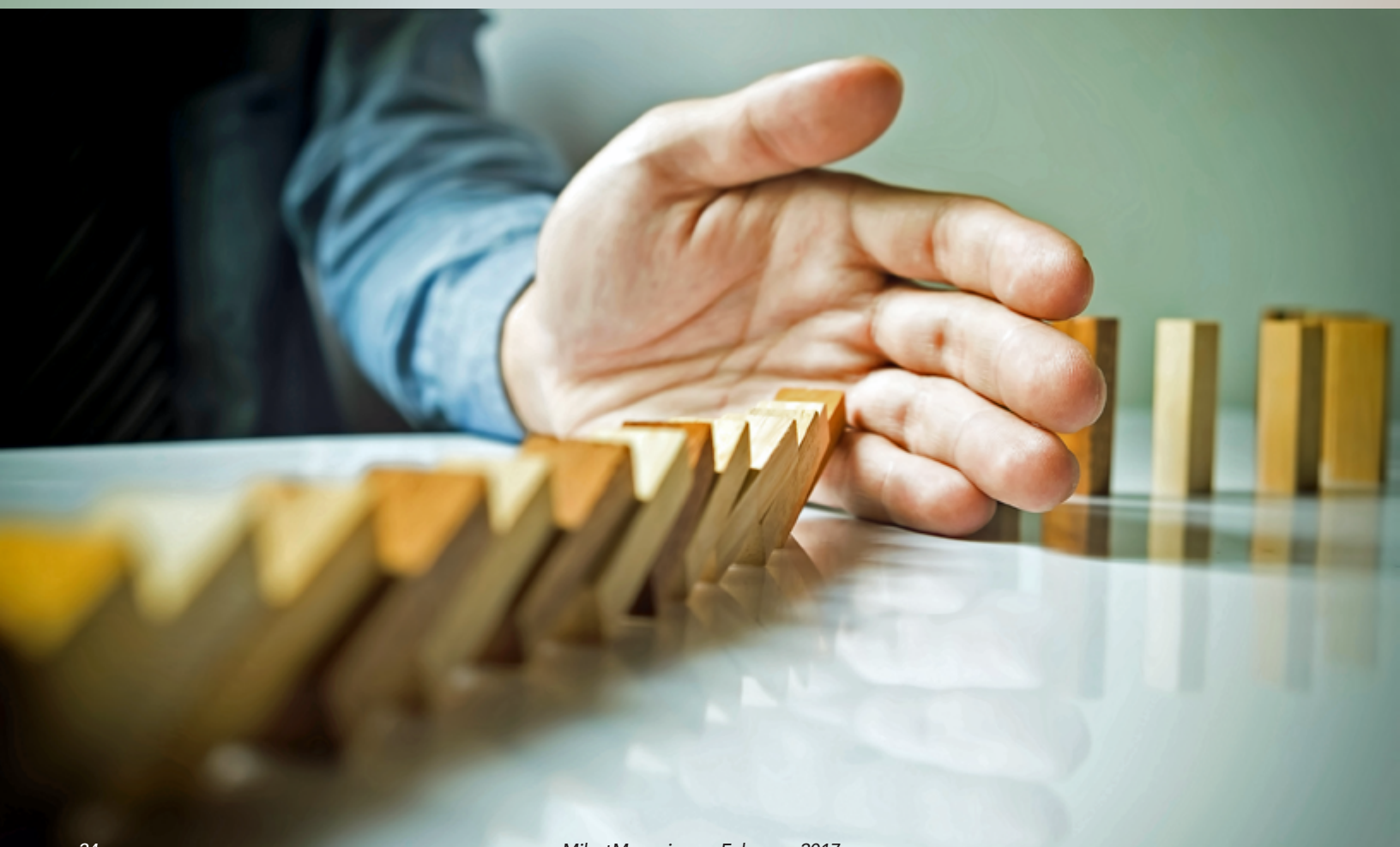
In this article, I will look at some of the technology drivers that will drive us closer to our goal of an interference-free space environment.

TECHNOLOGY

There have been numerous developments relating to new technology, especially for the VSAT market, that include the commercial availability to auto-cancel rogue carriers in most of today's high quality modems and transmission systems as well as the inclusion of software defined products. IRG members are at the forefront of developing and implementing these creative additions to their product portfolios. Taking each in turn…

VSAT: Members have launched truly innovative solutions for this sector, both in terms of resolving interference and preventing it before it occurs. This includes technology from Integrasys making installation of VSAT systems much simpler more accurate and error-free for VSAT installers.

Then there are the developments by such firms as VeriSat (now Kratos) for finding interfering VSAT transmissions in minutes, rather than the normal days, months or even years.



This is of huge benefit for all satellite operators as this mean VSAT interference can be quickly identified and no cost impact on current or future VSAT systems.

Cancellation: Other IRG members, such as Newtec, NovelSat and Kratos, have redefined the rule book on removing or avoiding rogue carriers through cancellation, smart automation and RF over IP techniques. This is available now in many products and is growing, making our future transmissions more robust when interference is present.

Software Definition: With the push for networks to be autonomous, mixing, seamlessly both terrestrial and satellite connections then software definition is becoming the norm within most complex products such as SDWANs. As new networks are built and the complexity required increases we need to ensure that network designs are armed with the latest knowledge and technology available, to be smart enough to deal with the quantity, quality, mix and speed of services that are required, and yet have the ability to mitigate problems automatically.

These solutions and others naturally bring with them other benefits and functionality. As technology is refreshed, these new developments in transmission management will become the norm and interference reduction becomes reality.

In addition, Carrier ID continues to be important when we are not talking VSAT burst mode, TDMA systems. The military is generally concerned by anything that could identify them, but as I've stated previously, only the Mac address will be displayed and it is envisaged that the military will manage their own ID regime with commercial satellite operators feeding unknown interference IDs to military control centres.

We continue to work this initiative in the commercial sector and this is leading to further developments for a simple, cost effective CID module to cater for all installed systems including narrow band data. This development and discussion with military organisations continues. Interestingly, as we move towards full implementation across other sectors, it will be more noticeable if you don't have CID!

BIG DATA

Big data is a hot topic right now and with good reason. By collating vast amounts of data and coupling that with intelligent processing systems, we can achieve a new level of personalisation across nearly every imaginable sector and that has been a massive driver for Big data.

Crucially for IRG, we believe it can help in error resolution through predictive analytics and deep learning algorithms and using cognitive computing techniques to join the dots quickly and automatically. There is value in data and the trick is to the relevant information efficiently.

The more we can analyse quickly and effectively will gain accuracy and used to evolve decision-making and problem solving scenarios for interference mitigation with the overall aim of predicting an error before it happens. By collecting every statistic, every incident, every detail of satellite interference, eventually, as our Data store grows, with smart analysis of that store, "signatures" could be extracted that could lead to possible auto-classification of interference types and better user-friendly tools to progress our mission of mitigating interference.

THE ROLE OF THE MILITARY

As we continue to work for an interference-free satellite environment, the military remains a key user group to enable that, not the least being because it is a major user of satellite communications. For that reason, over the coming months, it will remain an important sector for the IRG to engage with, along with continuing to reach out to commercial users.

Along with other planned IRG events throughout the year I am particularly excited that I will be heavily involved with Defence Satellites in Rome next year. I will be chairing the conference sessions, which will give me a really valuable opportunity to listen to the challenges being experienced by the sector at the moment, not just interference-related.

I see this as key, because although our group is focused on technology to reduce satellite interference, as mentioned above, a lot of that technology also makes satellite networks better and more efficient. Understanding the pain points, whether directly related to interference or not, will help us to work with our members and industry to solve them. In some cases, we may even already know the solution.

As well as chairing the main event, we are working with the organizers to host a workshop the day before, on May 22—this workshop will be solely focused on military interference, the specific challenges and the tools to resolve it.

irg.org/

Martin Coleman is Executive Director of the Satellite Interference Reduction Group (IRG). Martin is responsible for spearheading a number of significant initiatives and is committed to introducing new technology and processes to mitigate all types of satellite interference: VSAT TDMA Systems, BIG Data; a reference guide to Interference; sorting out those Difficult Cases including new standards and processes within the Geolocation industry; assisting the ITU in dealing with Harmful Interference; and implementing Carrier ID (CID). Martin regularly addresses the industry on the subject of satellite interference, at global industry events, on an individual basis, and at IRG-led conferences and webinars.

5th DoD Unmanned Systems Summit

Advancing Unmanned Systems Capabilities in Multi-Domain Environments

DEFENSE STRATEGIES INSTITUTE

ADVANCING THE MISSION - SUPPORTING THE FORCE

March 7-8, 2017

AUSA Conference Center, Alrington VA

FREE For Military & Government

To Register, Download Agenda, & Explore Exhibit Opportunities:

UNMANNEDSYSTEMS.DSIGROUP.ORG