SATCOM for Net-Centric Warfare

MilsatMagazine

NOVEMBER 2018

Featuring

- Kratos Defense
- Viasat
- GSR / SES-GS
- Satcom Direct
- Intelsat General
- DARPA
- Paradigm
- Dispatches

PUBLISHING OPERATIONS

Silvano Payne
Publisher + Executive Writer

Hartley G. Lesser
Editorial Director

Pattie Lesser
Executive Editor

Jill Durfee
Sales Director + Associate Editor

Simon Payne
Development Director

Donald McGee
Production Manager

Dan Makinster,
Technical Advisor

Sean Payne
Industry Writer

SENIOR CONTRIBUTORS

Richard Dutchik
Dutchik Communications

Chris Forrester
Broadgate Publications

Karl Fuchs
iDirect Government Services

Dr. Bob Gough
Goonhilly Earth Station

Rebecca M. Cowen-Hirsch
Inmarsat

Giles Peeters
Track24 Defence

Paul Scardino
Globecomm

Koen Willems
Newtec

AUTHORS

Frank Backes

Chris Hudson

Ken Peterman

Ulf Sandberg

Ryan Schradin

FEATURES

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
Satellite Networks

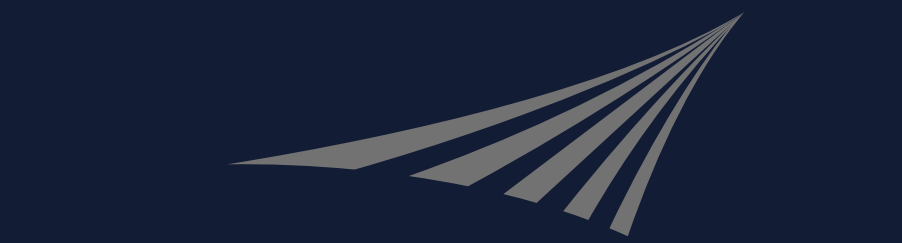
New name, New adventure.

Advantech Satellite Networks, formerly Advantech Wireless Inc., is now

SPACEBRIDGE

We thank all our partners, clients and suppliers for helping us significantly grow our business and we remain committed to the same degree of excellence, spirit of innovation and customer delight. Above all, we commit to reward our customers with unsurpassed technologies and solutions developed by our talented and loyal team that has earned your trust over the past 30 years.

A new journey has begun.



SPACEBRIDGE (Advantech Wireless Inc., doing business as Advantech Satellite Networks)
Tel.: +1.514.420.0045 • Fax: +1.514.420.0073 • spacebridge.com • info@spacebridge.com

DISPATCHES

Comms for first responders

Mobile connectivity is critical for first responders, and addressing this issue is an event dedicated to that issue, Operation Convergent Response (#OCR2018), November 5 - 8, 2018, at the Guardian Centers in Perry, Georgia.

This second annual event is hosted by Verizon and Nokia in collaboration with the Guardian Centers and Aegex Technologies, which attracts those companies that offer solutions for ensuring that satellite communications run smoothly despite the situation.

VT iDirect, Inc. (iDirect) and Kymeta will demonstrate their latest technology that can assist emergency first responders during this event that will bring together dozens of innovative companies to showcase their technologies that can enhance emergency response operations.

Satellite communications is critical in enabling first responders to immediately communicate, coordinate and react to any situation.

Whether in a densely populated urban area with damaged infrastructure, or a remote location where no infrastructure exists, satellite-enabled mobile command vehicles provide a lifeline during emergency response operations by coordinating essential services, helping restore communities and allowing residents to connect with loved ones.

Kymeta KyWay™ Terminal integrates ground breaking mTenna™ flat-panel antenna technology and the industry's leading iDirect X7 modem, to serve a broad range of mobility applications. With the Kymeta™ KyWay™ terminal, first responders can take real-time communications with them to the frontlines.

VT iDirect and Kymeta have teamed up to create a reliable, always-on communications hub for first responders by outfitting an All-Terrain Vehicle (ATV) with a KyWay terminal.

The terminal's flat panel antenna with an integrated iDirect satellite modem is small enough to fit on a variety of emergency vehicles, such as patrol cars, ambulances, fire trucks and SWAT vehicles. This allows first responders to communicate through their existing tools such as radios, smart phones or laptops, providing updated information on the situation they are entering to the command center.

Upon arrival on scene, the mobile communications solution becomes a mobile hotspot, allowing first responders to send crucial data such as readings from radiation sensors or live camera feeds, enabling accurate and detailed emergency response coordination.

Darren Ludington, Regional Vice President of Sales Americas, VT iDirect, said that quick response time makes a difference between life and death in many emergency situations. Their collaboration with Kymeta enables first response teams to be supported by seamless communications and real-time information, helping them to make more informed decisions as they enter disaster situations to save lives.

www.kymetacorp.com

www.idirect.net

AvL TECHNOLOGIES

avltech.com

ENABLING COMMUNICATIONS IN ANY SITUATION

AvL'S FAMILY OF INTEGRATED TERMINALS (FIT)

- Ultra lightweight - meets IATA requirements for carry-on or checked baggage
- One person set-up in less than 10 minutes
- Carbon fiber reflectors - sizes range from 45cm to 1.35M
- All-in-one positioner system & switchable manual or motorized operation
- Quick change tri-band feed and RF kits
- AvL AAQ computer-assisted pointing and acquisition
- Beacon receiver, ODU/modem integration and BUC/LNB integration
- Watch the video at avltech.com/media

DISPATCHES

SWaP for the Rugged ComSys-5301

Elma Electronic Inc. now offers the ComSys-5301, a highly rugged embedded computing system designed for SWaP-constrained, harsh environments.

Based on the industry standard COM Express and mini PCIe form factors, the modular computer is easily configured and upgraded with application-targeted I/O, CPU and storage. Designed using Elma's extensive packaging expertise, the new ComSys-5301 endures tough environmental conditions to provide highly reliable, long-term performance.

With special attention paid to SWaP optimization, the system is lightweight and energy-efficient, while still offering high performance processing.

The integration of advanced computing technology with a rugged, compact design makes the ComSys-5301 perfect for use in ground vehicles, unmanned systems and vehicles, drilling and mining operations, command centers and other mission critical applications.

The fanless ComSys-5301 uses passive conduction cooling and features a fourth Generation Intel Celeron CPU, solid state storage, dual Gigabit Ethernet ports and flexible I/O configurations.

Robust MIL-38999 connectors ensure that the I/O interfaces can withstand severe environmental conditions, such as intense shock, vibration and humidity, typically found in rugged, mobile applications. Approximate weight is just 6 lbs. and the system can be wall or table mounted, per VITA 75.

Product features...

- *Fourth Generation Intel® Celeron® 2.4 GHz Processor with QM87 Chipset*
- *Up to 16 GB Dual Channel DDR3L at 1600 MHz*
- *256 GB solid state storage — inquire about higher capacities*
- *Dual 10/100/1000Mbps GbE Ports*
- *Solid cable-less internal construction*
- *Passive conduction cooled and fanless thermal design*
- *Modular solution using standard Type 6 COMExpress modules*
- *Mighty Mouse I/O connectors for reliable performance in harsh environments*
- *Extended temperature operation*

www.elma.com

DISPATCHES

Hughes brings MILSATCOM to U.S. Coast Guard

Naval Air Systems (NAVAIR) will provide SATCOM systems integration for the U.S. Coast Guard.

A U.S. Coast Guard C-27J surveillance aircraft.

Under the agreement, Hughes, supporting through its partner, ADS, Inc., will integrate communications systems in support of the Coast Guard's Intelligence, Surveillance and Reconnaissance (ISR), humanitarian aid and disaster relief (HADR) missions requiring airborne Communications-on-the-Move (COTM).

Hughes will provide SATCOM integration for the missionized C-27J aircraft which will connect mobile units across a wide geographic area including over the United States, Canada, Mexico, and the Pacific Ocean.

The broad operational regions require proven Beyond-Line-of-Sight (BLoS) system integration expertise to coordinate hardware functions on the C-27J aircraft including antennae, modem, engineering services and technical training.

For this contract, Hughes will deliver cost-effective mobility solutions that will provide multi-mission support including drug interdictions, border control enforcement and search and rescue efforts (SAR) for the agency.

Rick Lober, VP and GM of Defense and Intelligence Systems Division at Hughes said that the company was well-positioned for this requirement to provide comprehensive engineering expertise for integrating a satellite technology and service solution that will enhance the Coast Guard's diverse operational capabilities. The Coast Guard often operates in extremely challenging environments which require robust communications solutions. Hughes values being a trusted partner for their global missions.

www.hughes.com

DISPATCHES

Third milestone completed by Kratos

Kratos Defense & Security Solutions, Inc. (Nasdaq: KTOS) has successfully completed the third phase of a pathfinder study for migrating the Command and Control System – Consolidated (CCS-C) ground system to the Enterprise Ground Services (EGS) architecture — CCS-C currently operates a fleet of over 20 Military Satellite Communications (MILSATCOM) satellites in four different constellations.

In phase 3, Kratos demonstrated the automated deployment of the MILSATCOM EGS (MEGS), using virtualized applications on the Space and Missile Systems Center (SMC)-provided Cooperative Research and Development Agreement (CRADA) Supply Chain Risk Management (SCRM) infrastructure hosted at the Space Management Battle Lab (SMBL).

After successful deployment, the team demonstrated Kratos' web-based user interface and automation capabilities. Traditionally, ground system capabilities take months or even years to deploy and test, however, with automated software deployment and dynamic allocation of resources employed by the Kratos team based on the EGS principles of deploying in a modern IT environment, the demonstration took less than 10 minutes. This dynamic allocation of ground resources demonstrates the portability, resiliency and elasticity of the MEGS.

EGS is a critical technology for the Air Force's Space Enterprise Vision (SEV) focused on a sustainable, resilient space architecture that can respond to emerging threats and protect space-based assets. When implemented, EGS will result in a best of breed, service-based ground architecture for all Air Force spacecraft that will enable Air Force Space Command (AFSPC) to fight and win a war that extends into space. AFSPC is implementing EGS with prototyping activities to mature the concepts, technologies, EGS standards, and transition paths for legacy and future ground systems.

The Kratos study for MILSATCOM is a 27 month effort that consists of four phases and is an essential step in the evolution of CCS-C to exploit the benefits of EGS. Phase 3 concluded on 12 July with a successful demonstration. Phase 4 will be completed in December of 2018.

www.kratoscomms.com

DISPATCHES

Kymeta and Paradigm create a terminal solution

Kymeta and Paradigm have partnered to create an enhanced portable terminal solution for military and emergency responder customers called the MANTA.

The MANTA, which integrates the Kymeta™ **KyWay™** terminal together with Paradigm's **Interface Module** (PIM®) controller, offers increased capabilities to users needing reliable communications on-the-move.

Military and first responder users who need connectivity for remote incident response, in urban environments where existing infrastructure is compromised, or elsewhere in the world where operations demand reliable communications now have a rugged, easily transportable, and mobile connectivity solution.

The MANTA is a one case, all-inclusive solution and needs just one cable (to connect power). The system can operate out of the case or be put onto a vehicle roof in a matter of minutes and eliminates the need for complicated wiring and rack-mounting components.

The MANTA is now shipping with an **iDirect X7** modem and can support modems from various suppliers.

Kymeta **K LO™** network connectivity services can also be bundled with the solution for complete global coverage.

The partnership marks a strong collaboration between two of the most innovative players in the mobile satellite communications market.

The KyWay terminal is an industry-first solution and the world's only commercially-available, flat-panel, electronically-steered satellite terminal.

The PIM® terminal controller has a proven track record from its existing integration into a range of satellite terminals.

Ulf Sandberg, Managing Director, Paradigm, said that with Paradigm PIM-enabling the Kymeta antenna, the company will create superior solutions and the firm is looking forward to working with Kymeta and revolutionizing SATCOM-on-the-Move (SOTM).

David Harrower, SVP of Global Sales, adds that the new KyWay terminal and PIM technology solution is ideally suited to the mobile military, government, and emergency responder sectors — Kymeta is excited about the advances and flexibility that the new MANTA terminal solution will bring to the market.

www.paracomm.co.uk

kymetacorp.com

ADVANTECH
WIRELESS

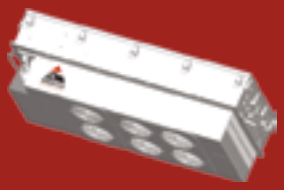
Second Generation GaN based SSPAs/BUCs in C, X, Ku and Ka-Band

250W C-Band
2nd Generation GaN SSPA/BUC

400W C-Band
2nd Generation GaN SSPA/BUC

300W-400W C-Band Rackmount
2nd Generation GaN SSPA/BUC

400W Ku-Band
2nd Generation GaN SSPA/BUC



1,250W Ku-Band
2nd Generation GaN SSPA/BUC

www.advantechwireless.com

DISPATCHES

DISA's industry invitation

The Defense Information Systems Agency's (DISA's) present and future industry partners joined the agency for Forecast to Industry on November 5 at the BWI Airport Marriott Hotel and Conference Center in Linthicum, Maryland.

The event provided industry representatives with in-depth information about the agency's upcoming acquisition and procurement plans, and also offered a forum to collaborate with DISA in defense of the nation.

The theme for this year's event, "*Trusted Partnerships*," paralleled DISA Director Navy Vice Admiral *Nancy Norton*'s strategic vision for DISA: To be the trusted provider to connect and protect the warfighter in cyberspace. Norton stressed to industry partners the importance of an integrated relationship during her opening remarks.

"*As the old saying goes, there is strength in numbers*," she said, reflecting on a recent speech by Secretary of Defense Jim Mattis.

She continued, "*When nations pool resources and share responsibility, their burdens become lighter. It also gives the U.S. a better chance to advance its interests and maintain a balance of power that will keep enemies from thinking twice about aggression. The stability that comes from alliances and partnerships can also generate much-needed economic growth*."

Norton then presented a scenario fitting for the event. "*What if we replace 'nations' with 'DISA and industry partners?' Let me read that again: When DISA and industry partners pool resources and share responsibility, their burdens become lighter … and ... the stability that comes from those partnerships can generate much needed economic growth*."

She described DISA's role in defending national interests and acknowledged it takes a team effort to maximize the effect.

"*Our theme, 'Trusted Partnerships,' embodies the way we work closely with industry — to develop solutions for the DOD. Only by working together can we expand our capabilities and support to those protecting our great nation*."

The admiral continued her opening remarks by highlighting how the agency executes the defense secretary's lines of effort.

She talked about how the agency is increasing lethality for the warfighter, strengthening partnerships, and reforming the department.

"*As a combat support agency for the department, DISA is uniquely positioned to take on major tasks and initiatives to connect and protect the warfighter in cyberspace*," she said. "*Be our partner … we can achieve great things together*."

Norton highlighted a handful of initiatives the agency is working on, and her remarks were followed by detailed briefings from subject matter experts later in the day.

She closed her remarks to the approximately 2,000 in-person and online attendees by reminding industry partners the agency is open to collaboration, and she welcomed them to the conversation.

"*Creating trusted partnerships supports DISA's vision to be the trusted provider to connect and protect the warfighter in cyberspace," she said. "I want you to share that vision and our values — to ensure success in defense of our nation*.

"*We look forward to hearing from you and gaining a better understanding of how you can support us with our future requirements. Thank you again for being here today and continuing to partner with DISA*."

Department of Defense Chief Information Officer (CIO) *Dana Deasy* followed Norton's opening remarks, and also emphasized the importance of DoD's synchronized partnership with industry.

"*The annual Forecast to Industry event is incredibly important for the Defense Department*," Deasy said. "*Ongoing dialogue with our industry partners is needed in order for us to continue to maintain superiority*."

Deasy explained how DISA's portfolio is expanding to meet 21st Century challenges, highlighting two mobile apps used in support of Hurricane Florence emergency management and recovery efforts.

At the Army's request, DISA expedited security review and release of the "Ready North Carolina" app within the DoD Mobility Unclassified Capability (DMUC) app store.

DISA and the South Carolina National Guard also worked together to create an app used by guardsmen to determine if their homes were in an evacuation zone.

The app provided ease of mind to the emergency workers because they knew their families could access updated information and were able to find a safe place for evacuation, Deasy explained.

"*Both of these apps allowed aid workers to focus on supporting community rescue efforts. I think it goes without saying that DISA brings a wealth of capabilities in times of national crisis*."

Deasy continued his remarks to industry by reiterating the defense secretary's three lines of effort and said every mission in DISA's portfolio ties back to those objectives.

He also said the agency is inherently tied to industry in this undertaking.

"*The challenges we face at DoD will continue to evolve, but when I look across the room today, I know the department does not face these challenges alone*," Deasy said.

"*As I have said before today, our industry partners are key to the long-term success at DOD. In order to compete, deter, and win, we need your help," he said. "What I like to tell industry is to bring us solutions in the lens of our priorities. How will your solution benefit the greater National Defense Strategy? That is what we are all working toward together*."

DISA's Executive Deputy Director *Tony Montemarano* then gave attendees a DISA overview presentation.

"*DISA supports an ecosystem from Kabul to Seoul, South Korea*," he said. "*We provide enterprise services, unified capabilities, and mobility options to support DOD operations anywhere, anytime*."

He presented DISA's leadership hierarchy, and talked about how the agency provides niche services that support combatant commands and the warfighter, including joint interoperability testing, electromagnetic spectrum management, communications support for the White House and national leadership, desktop support at the Pentagon, and contracting.

Montemarano, who is also DISA's senior procurement executive, stressed the agency is vigilant when it comes to Other Transaction Authorities and contracting.

He asked industry partners not to be discouraged or frustrated by the time it takes to execute a contract, and explained the time invested is beneficial to all involved.

He said not only are procurements double-checked, they're triple-checked.

"*Our focus is on fairness when it comes to contracts," Montemarano said. "If you're going to go after a contract, go after it aggressively. We are working hard to be fair and working hard to be open and transparent*."

DISA Operations Center Director *David Bennett* took to the podium to discuss his center's needs, stressing industry partners must understand his mission and work within that scope when proposing a solution for DISA and the DOD.

"*Many times what works in industry doesn't apply in this space," he said. "I will listen to your pitch and see how it applies within our space. I ask that when you prepare your presentations, you ask yourselves the same question*."

Presentations continued throughout the afternoon. Presenters discussed the procurement and acquisition plans related to business innovation, cyber, mobility, networking, the Joint Service Provider, and small business programs. The event concluded with a "meet the seniors" panel.

disa.mil/

DISPATCHES

Dynetics smallsats to U.S. Army

Dynetics has been selected to develop small satellites for the U.S. Army Space and Missile Defense Command/Army Forces Strategic Command (USASMDC/ ARSTRAT) Technical Center program named Gunsmoke-L.

Through the Design, Development, Demonstration and Integration (D3I), Domain 1 task order, the Gunsmoke-L contract is for two years, plus one option year valued at $8.3 million, to develop, test, integrate and demonstrate two tactical space support vehicles (TSSVs) which will be used to enhance all phases of joint force operations.

The smallsat-based platforms will host the next generation of tactical space support payloads designed to operate in LEO for a minimum of two years. Dynetics will conduct hardware-in-the-loop testing and simulation in conjunction with the command's Payload Development Laboratory (PDL) facility at Redstone Arsenal in Huntsville, Alabama, to optimize TSSV performance and reliability. The TSSV will be developed and integrated at Dynetics' facilities in Huntsville, which include payload development labs, clean rooms and environmental test capabilities. At completion of the two-year base period, the two TSSVs will be qualified and ready for launch.

During the 12 month option period, Dynetics will support on orbit demonstrations using the Technical Center's smallsat ground control system located at Redstone Arsenal to provide command, control, and communication with the TSSV.

Dynetics will work with the Technical Center's Space and Strategic Systems Directorate, which serves as the developmental spearhead for the command's advanced Army space support efforts, which include research, development and demonstration of the next generation of tactical space support payloads.

www.dynetics.com

DISPATCHES

Comms and Intelligence on display

Rohde & Schwarz presented their portfolio of integrated communications and radio reconnaissance solutions at INDO DEFENCE in Jakarta.

Turnkey COMINT/C-ESM systems from Rohde & Schwarz.

Rohde & Schwarz presented themselves as a single-source supplier of integrated solutions for secure communications and radio intelligence. Interoperable, powerful communications systems for deployment on land, in the air and at sea are the cornerstones of the comprehensive communications architecture developed by the independent company.

The **R&S NAVICS** integrated naval communications system delivers mission-ready internal and external voice and data communications for all classes of ships.

The broad communications portfolio from Rohde & Schwarz is built around advanced software defined radios (SDR) based on software communications architecture (SCA). The latest generation of SDR/SCA technology is already fielded with the R&S SDTR for vehicle-based tactical communications and the R&S SDHR for highly mobile applications.

Rohde & Schwarz presented their latest addition to its communications portfolio: the **R&S SDAR** next generation airborne radio. It combines the advantages of a networked radio with the excellent performance of the successful R&S M3AR family of airborne radios. Almost 8,000 software defined airborne radios from Rohde & Schwarz are integrated on more than 70 different airborne platforms.

Another highlight on display was the **R&S ELINT** solution. Created with a focus on user-friendliness and comprehensive functionality, the system is optimized for detecting, monitoring and analyzing advanced radar signals. It was designed to handle challenging signal scenarios and has already proven itself in operation, especially in acquiring weak and LPI signals in dense signal environments and analyzing state-of-the-art, multi-functional radars with complex signal structures.

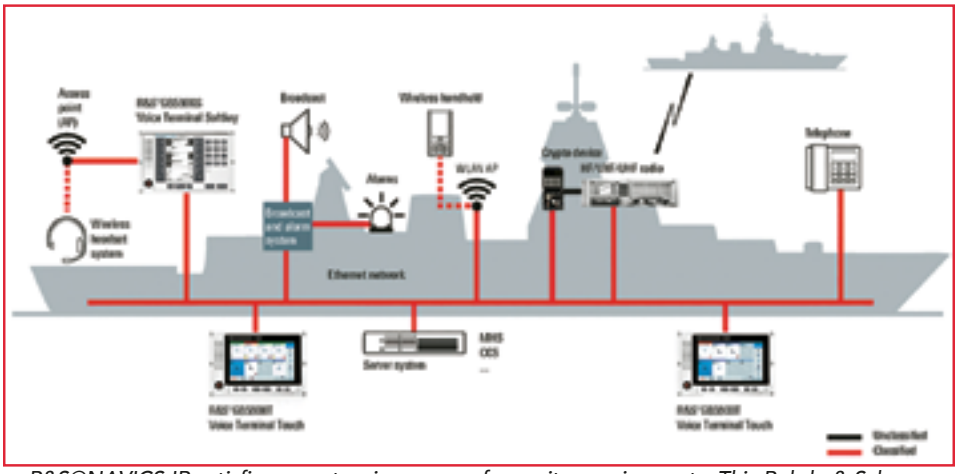
Rohde & Schwarz will also showcase its **COMINT/C-ESM** solutions, which can be fully customized to meet the requirements of the most diverse intelligence missions. These radio monitoring systems from Rohde & Schwarz are deployed worldwide in land-based mobile and stationary applications and on naval and airborne platforms.

The Rohde & Schwarz monitoring and direction finding systems are ideal for stationary, mobile and portable deployment. The R&S DDF1555 is the heart of a full-featured man-portable reconnaissance system for outdoor applications. It combines accurate direction finding with wideband monitoring capabilities. The direction finder is an ideal solution for applications that require portable and mobile direction finders for use in outdoor environments.

The Rohde & Schwarz portfolio also offered a number of solutions for protecting cyberspace. The security of data and communications is the prerequisite for the success of digital transformation, which affects almost all facets of the economy and society.

The explosive growth of networked products makes it easier to launch a digital attack on companies, authorities and critical infrastructures. For their protection, Rohde & Schwarz Cybersecurity, using the security-by-design approach, develops and produces a wide range of leading high-tech hardware and software products that repel attacks proactively instead of reactively.

www.rohde-schwarz.com/



R&S®NAVICS IP satisfies an extensive range of security requirements. This Rohde & Schwarz solution provides red/black separation in single security networks supported by high-quality encryption devices.

Image is courtesy of Rohde-Schwarz.

DISPATCHES

Sixth GPS payload delivered

Harris Corporation (NYSE:HRS) has now provided Lockheed Martin (NYSE:LMT) with the sixth of 10 advanced navigation payloads contracted for the U.S. Air Force's GPS III satellite program.

The advanced MDU on navigation payloads delivered for the GPS III satellites. Photo is courtesy of the manufacturer, Harris Corporation.

The GPS III navigation payload features a Mission Data Unit (MDU) with a unique 70-percent digital design that links atomic clocks, radiation-hardened processors and powerful transmitters — enabling signals three times more accurate than those on current GPS satellites. The payload also boosts signal power, which increases jamming resistance by eight times and helps extend the satellite's lifespan. Harris is committed to delivering a seventh navigation payload by the end of 2018. This latest payload delivery is the third payload Lockheed Martin has received in the last 12 months.

Harris navigation payloads are already integrated on five GPS III satellites. In August, the first GPS III space vehicle (GPS III SV01) shipped to Florida for an expected December launch. Also, in August, the Air Force declared GPS III SV02 Available for Launch, or "AFL," for an expected 2019 launch. GPS III SV03 and SV04 are fully assembled and in environmental testing. GPS III SV05 was integrated with its payload this fall and will begin system testing later this year.

In 2017, Harris announced that it completed development of an even more-powerful, fully digital MDU for the Air Force's GPS III Follow On (GPS IIIF) program. The new GPS IIIF payload design will further enhance the satellite's capabilities and performance. In September, after a full and open competition, the Air Force awarded Lockheed Martin a contract for up to 22 additional GPS IIIF satellites.

Harris' expertise in creating and sending GPS signals extends back to the mid-1970s – providing navigation technology for every U.S. GPS satellite ever launched. While the Air Force originally developed GPS for warfighters, millions of people around the world and billions of dollars of commerce now depend on the accurate, reliable signal created and sent by Harris navigation technology.

www.harris.com
www.lockheedmartin.com

DISPATCHES

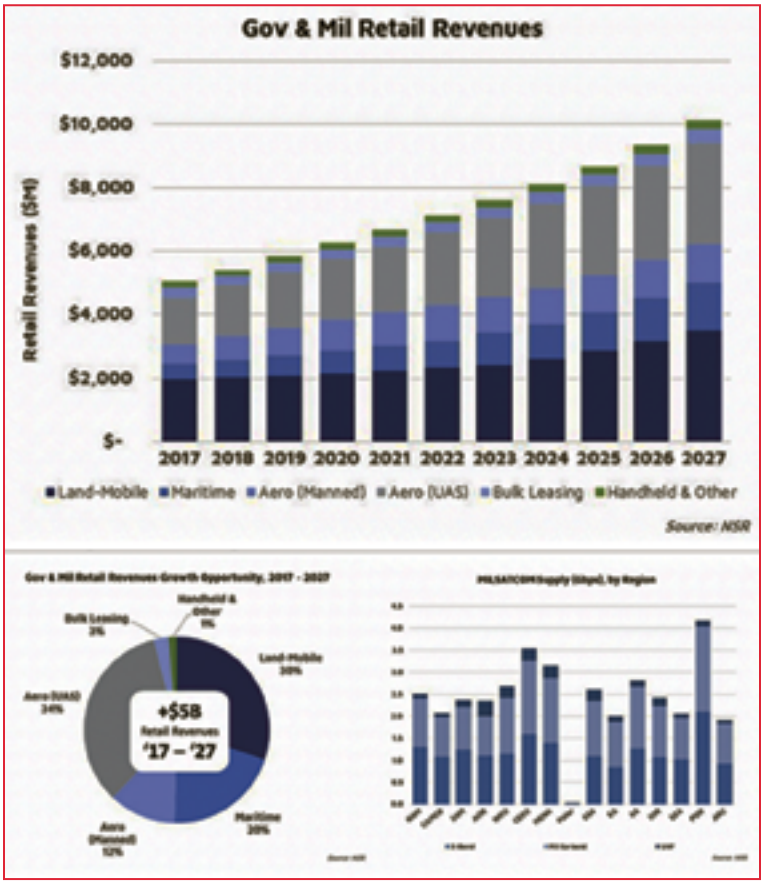
NSR's MILSATCOM analysis and report

NSR's newly released Government and Military Satellite Communications, 15th Edition report finds a rebounding market entering a growth phase after several years of stagnation.

Geopolitics, acquisition reform, and expanded low-cost offerings from the commercial market, all point to expanded opportunities across all regions and applications.

With more than $71 billion in cumulative revenue expected by 2027, commercial suppliers to the MILSATCOM market stand to see sizable gains.

At slightly over $5 billion in revenues in 2017, up nearly $500 million from 2016, annual global MILSATCOM revenue will double over the next decade. Land-Mobile and UAS applications are the leading markets for Government and Military users, as they will generate over 64 percent of revenue.



Renewed interest in bulk leasing, and ongoing integration of commercial managed services into end-user networks, however, is being offset by challenges in terminal acquisition and expanding MILSATCOM capacity.

"Government and Military customers need more connectivity than ever before — from all orbits, and frequencies — and from both commercial and proprietary networks," said report author and Senior Analyst, *Brad Grady*.

Brady note, "*The debate today isn't entirely MILSATCOM vs. COMSATCOM, it's about acquiring new, flexible terminals, and having a holistic view of the entire communications infrastructure.*

"This year, the focus has turned to the 'how' — how to implement acquisition reform, how to design robust and resilient communications infrastructure, and how to integrate commercial technologies within and alongside MILSATCOM networks."

As commercial markets continue to accelerate their uptake of broadband satellite connectivity, these end-users are feeling the pressures of being left behind.

Combined with falling capacity prices, Government and Military markets are taking full advantage of accelerating their adoption of commercial satellite connectivity.

At over 21 Gbps of capacity demand across both FSS and HTS in 2017, increasing to more than 250 Gbps of satellite capacity by 2027, generating $10 billion in retail revenues for the satellite sector, the market is on a growth-trajectory.

Despite several years of turbulence, there is a strong outlook for mil/gov satcom growth on the horizon.

NSR's Government and Military Satellite Communications, 15th Edition, explores the market opportunities available to the satellite industry.

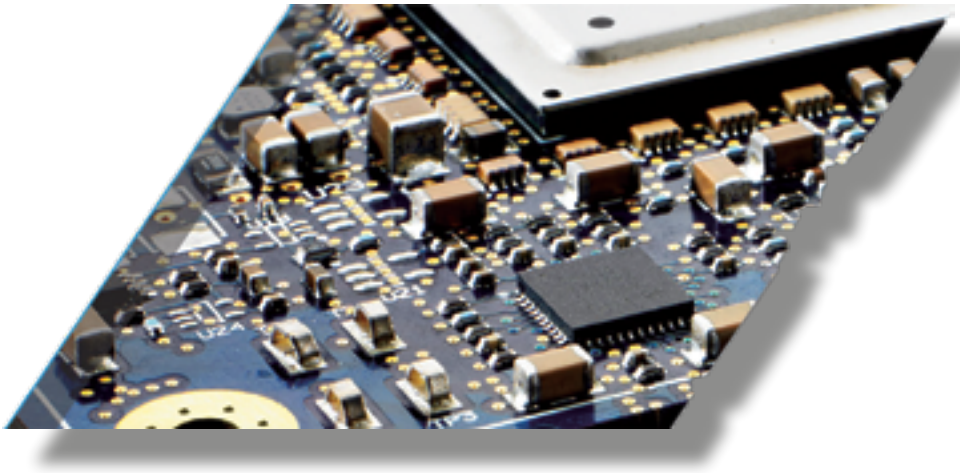
With more than 15 years of insights and analysis, NSR's longest-running report on the government and military satellite communications market provides an in-depth view of the drivers, regional trends, and capacity demand through 2027.

www.nsr.com

DISPATCHES

Viasat's Mini Crypto to U.S.A.F.

Viasat Inc. (NASDAQ: VSAT) has received a Low Rate Initial Production (LRIP) order of 1,000 National Security Agency (NSA)-certified Mini Crypto devices from the U.S. Air Force (USAF).



In today's battlespace environment, technological breakthroughs have enabled smaller sensors and smaller platforms of every kind, but until now, the available high-assurance cryptographic technology did not meet the needs for these devices at the tactical edge.

Viasat's Mini Crypto devices are designed for easy embedment on U.S. Department of Defense (DoD) small form factor systems, allowing them to transmit SECRET and Below data securely across the battlespace.

Systems include unmanned systems, emerging robotics applications, communications devices, and existing and emerging sensors.

According to the USAF, the Mini Crypto device will enable forward-deployed warfighters to secure these small, tactical edge systems in extremely hostile environments.

The Mini Crypto device will ensure tactical communications and data exchanges, no matter where they take place, stay safe and secure. Due to its small size and embedded operational use case, the Mini Crypto device provides high levels of security with minimal additional weight and power.

In addition, because they are embedded and have a self-contained encryption engine capable of generating their own keys, they are not required to undergo the same special handling as other security devices, thereby expanding their operational use case and reducing operational costs.

The initial LRIP order of Viasat's Mini Crypto devices demonstrates a critical transition point for this embeddable security technology, and is a key step towards securing a Full-Rate Production order from the USAF.

First deliveries of Viasat's Mini Crypto devices are expected during the third quarter of Viasat's fiscal year.

Viasat's Mini Crypto device is based on the Company's industry-leading programmable and embeddable PSIAM™ cryptographic technology, which provides accredited cryptography for a wide range of applications including unmanned systems, handheld communications, weaponized platforms and high-speed cloud computing.

Ken Peterman, President, Government Systems, Viasat, said that cyber threats have created a new operational environment and have increased risk across the multi-domain battlespace. Viasat's Mini Crypto will provide substantial operational cost savings to customers through certificate-based Tactical Key Management and non-Controlled Cryptographic Item handling.

He added that the Mini Crypto also brings exceptional ease-of-use to the warfighter with innovations in low Size Weight and Power, enabling longer operational periods and smaller payloads. The company's patented software is upgradable even after deployment, enabling ongoing improvements without removing the system from the field.

www.viasat.com/products/embeddable-security-system

SPACE: THE NEXT CYBER BATTLEGROUND?

By Frank Backes, Senior Vice President, Kratos RT Logic

Cyber-attacks, focused primarily on identity and financial theft in the commercial world, are becoming a critical issue in space.

Cyber-attacks on satellites can include jamming, denial of service (DoS), hacking attacks on communication networks and piracy. Piracy, or unauthorized access, occurs when carriers (with content) are transmitted toward a satellite without any prior contract with the satellite operator.

Intentional jamming can be the result of one party's objection to the content (political, cultural, social, etc.) of the targeted carrier, extenuating circumstances (political situation, social unrest, etc.) and in the worst case, intent to disable a satellite to gain a military or economic advantage.

Roots of Vulnerability

Unlike optical fiber or copper cables, satellites send their radio frequency (RF) signals through air and space, creating the opportunity for anyone with the appropriate knowledge, means and motivation to interfere with the RF signal.

Such interference can be accomplished by jamming, variations of which include blocking undesirable radio and television broadcasts from being transmitted into a country and blocking satellite navigation signals. Increasingly, with the use of Commercial-Off-The-Shelf (COTS) products such as open-source software, vulnerabilities are multiplied. It is one thing to protect proprietary products from latent malware being inserted during development, but the risk is compounded when acquiring the products from a long supply chain.

Another challenge is the speed with which technology advances, coupled with the fact that it can take two to three years to build and launch a satellite designed for a 10 to 15 year lifespan. In these cases, one not only has to embed cybersecurity defenses in the satellite during the design stage but must also be prepared to retro-fit on-orbit satellites with newer cyber defenses during the satellite's life span.

Of all the vulnerabilities those with the most potential for severe disruption are satellite-based navigational systems… ***Galileo*** in Europe, ***BeiDou*** in China, ***GLONASS*** in Russia, the Indian Regional Navigation Satellite System (***IRNSS***), and the U.S. global positioning system (***GPS***), which is the most pervasive and supports much of the world's civil infrastructure.

New Department of Defense Cybersecurity Strategy

The Department of Defense (DoD) recently issued their first cybersecurity strategy since 2015.

On the heels of that announcement, *Patrick Shanahan*, Department of Defense Deputy Secretary, made it known to the defense industrial base that he expects the products and services DoD buys to come secure, just as the department also expects them to be of the best quality.

The new cybersecurity strategy focuses on how the department will implement the priorities of its National Defense Strategy in cyberspace, particularly in defending against Russian and Chinese "*persistent, aggressive cyberspace campaigns that pose strategic, long-term risks to the Nation, our allies, and partners.*"

The strategy sets five objectives DoD will strive to achieve indefinitely into the future:

- *Ensuring the Joint Force can achieve its missions in a contested cyberspace domain.*
- *Enhancing Joint Force military advantages through the integration of cyber capabilities into planning and operations.*
- *Deterring, preempting, or defeating malicious cyber activity targeting U.S. critical infrastructure that is likely to cause a significant cyber incident.*
- *Securing DoD information and systems, including on non-DoD-owned networks, against cyber espionage and malicious cyber activity.*
- *Expanding DoD cyber cooperation with allies, partners, and private sector entities.*

Artistic rendition of the U.S. Global Positioning Satellites on orbit around Earth.

Resilience, Agility and Speed

These vulnerabilities are driving change in military space, as well as in the commercial world and countering them requires more resilience, agility, and speed in order to predict, pre-empt, and prevent the growing range of threats.

Aside from disruption of civil infrastructure, cyber-attacks on satellites could weaken responses to military threats, by compromising satellite command and control (C2), operational monitoring and payload performance.

As such, the DoD plans to spend $2 billion over the next five years on a new constellation of Global Positioning System satellites that will be hardened to withstand electronic interference from hostile nations, satellite ground systems need to be protected, as well.

In making the announcement U.S. Air Force Secretary **Heather Wilson** said the U.S. Air Force is motivated to move ahead with this new constellation amid increasing concerns that a growing number of nations are developing electronic weapons to jam or interfere with GPS signals.

"*All those things are an obvious awareness of American dominance in space. I cannot think of a military mission that doesn't depend on space. Our potential adversaries know it, and we need to protect those vital assets*," she said.

Also, in a move to enable Air Force Space Command to focus entirely on space superiority, the responsibility of fighting hackers in cyberspace has been transferred to Air Combat Command. According to Wilson, the transition will "*drive faster decisions as we fight by realigning the cyber operations and intelligence, surveillance and reconnaissance missions under the same command.*"

LEO/MEO Constellations… Pawns in Space?

Contending with the reality of future attacks, the strategy of investing in more agile, resilient satellite capabilities is being bolstered by new space.

Newly planned LEO and MEO constellations (by **OneWeb**, **SpaceX**, **O3B/SES** and others) are radically changing the economics, lowering the cost of satellites an order of magnitude that makes the concept of resilience through numbers and basic protection capabilities viable. As space becomes an ever more contested environment, small satellites can act as pawns on a chessboard… protecting large military and commercial satellites… the Kings, Queens, and Bishops of space.

Protecting a few critical and expensive satellites, which are obvious targets, with larger numbers of less expensive, yet agile satellites–pawns, if you will, creates a more defensible space. Or, as *Joshua Hartman*, Managing Partner at **Renaissance Strategic Partners** at a CyberSat conference in Washington DC, said, "*…if I disaggregate a mission around a multi-satellite architecture … I make it harder for my adversary to take away my capability, whether it's a kinetic or non-kinetic threat. If I have 200 satellites and they manage to take out two satellites, I still have 198 satellites available — and so the impact is minimized on a per satellite basis, which correlates to overall mission capability.*"

…And on the Ground

Cyber-attacks against vulnerable ground systems could result in the ability to access and potentially compromise sensitive satellite data and/or payloads.

A report from the **Secure World Foundation** identifies three primary access points for targeting a satellite: the supply chain, the land-based infrastructure that interacts with the satellite and the actual satellite while on orbit. Of the three access points, the supply chain and land-based infrastructure are ideal targets of opportunity for attackers because they are the most accessible.

Figure 2. Withour proper cyber security measures, ground stations are suceptible to cyber attacks.

In a recently published interview, KPN Chief Information Security Officer (CISO) *Jaya Baloo* said that, with respect to cyber vulnerability, she would focus on the ground station to determine how one could spoof or clone the communications over a poorly authenticated or an un-authenticated channel. The hacker would assume that on the un-authenticated channel, there would be one or two bands you could communicate with from your ground station to the satellite. If it was un-authenticated, the hacker could then pirate your signal communications to that satellite, she explained.

Approaches to Cyber Security

For terrestrial and space environments Kratos offers a range of cybersecurity testing, monitoring and hardening solutions to reduce vulnerability and minimize risk:

Interference Cancellation

Deliberate jamming, or RFI, is one of the more prevalent attacks. Traditional approaches to resolving interference require identifying the source and when possible working with the interfering party to mitigate the effects.

Monics SigX® is a proactive signal cancellation solution from Kratos that offers an alternate approach to resolving interference without relying on cooperation from the interfering party.

SigX directly mitigates RF interference (RFI) as shown in ***Figure*** 3 below by simultaneously canceling up to four continuous wave (CW) or sweeping CW signals in real-time to protect valuable bandwidth and help assure application and/or mission effectiveness.

RF monitoring data has long been used to manage signal interference issues; however, RF monitoring can advance Space Situational Awareness (SSA) with its ability to identify the behavior and performance of the satellites themselves. By leveraging RF data — the information about satellite signals— SSA can better detect, characterize, and attribute threatening space activities.

With space evolving to a warfighting realm, RF data can effectively fill the gaps in traditional SSA sensors to provide more timely, thorough, and predictive awareness.

With the correct RF analytics, machine learning, and AI tools, personnel can characterize the attributes of satellites, predict the maneuvers or actions they may undertake, and discern intentions. For example, the automated classification of bandwidth use, transmission type, and timing can help identify satellite modems, payload activities, and attribute behavior.

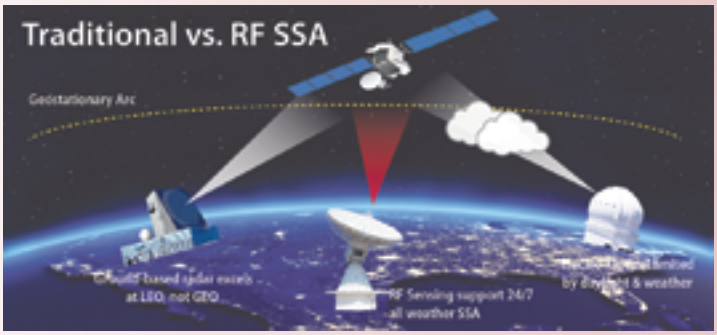


Figure 4. Traditional versus RF Space Situational Awareness (SSA).

Coupled with its global sensor network, consisting of 21 worldwide RF monitoring sites, hosting more than 80 fixed and steerable sensors and antennas in C-, Ku-, X-, Ka-, L- and S-bands, Kratos' advanced analytics and AI tools process RF data for real-time SSA awareness, predictive insights, historical trending, and patterns of life. Fused and correlated with data from optical, radar, terrestrial and space-based sensors, this provides more timely, accurate, and complete SSA.

Information Assurance

Information Assurance (IA) hardening is another approach to protecting operating systems to ensure system software, firmware and applications are updated to stay ahead of exploits that attack flaws in the underlying code.

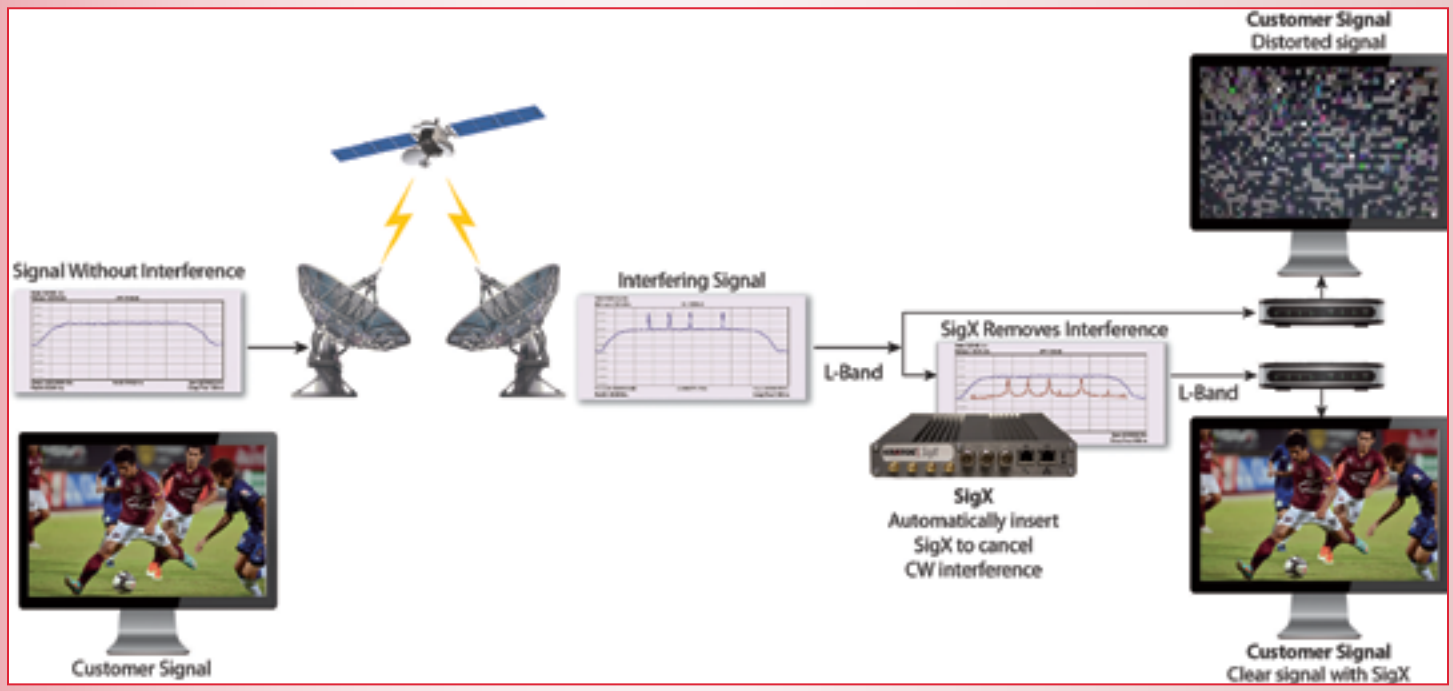


Figure 3. SigX cancels Continuous Waveform interference signals in real-time to protect valuable bandwidth.

Kratos has a proven history of executing IA hardening for commercial and government organizations. The company now offers IA hardening as a service that provides consistent IA hardened operating system (OS) updates on a quarterly basis and is fully compliant with the U.S. Defense Information Systems Agency (**DISA**) *Security Technical Implementation Guide* (**STIG**) hardening requirements.

Security Assessments

Satellite operators use traditional security monitoring tools as well as those uniquely designed for satellites.

Kratos offers a **SATCOM Cybersecurity Assessment** service that addresses the increasing threats and unique requirements of the satellite industry. Cybersecurity Assessments assist satellite organizations in the identification and prioritization of threats and their mitigation.

The result is a detailed view of satellite network preparedness in addition to recommended steps required to mitigate risks and ensure compliance with applicable regulations, standards and guidelines.

CyberC4 is an integrated family of products designed for the unique cyber defense needs of satellite ground network environments including situational awareness, and active defense for total protection from cyber-attacks.

Kratos protected communications products and services continuously monitor SATCOM networks for cyber threats, harden SATCOM equipment against exploits and defend against insider threats.

The Market

The global military cyber security market is expected to have been nearly $10 billion in 2017 and is expected to increase to almost $14 billion by 2027 — that represents a CAGR of approximately 3.5 percent during the forecast period.

According to the "*Global Military Cyber Security Market 2017-2027*" report, the global market for military cyber security is expected to be valued at more than $130 billion during the forecast period and is expected to be dominated by North America, followed by Asia-Pacific and the European markets.

Conclusion

The cyber threat to satellites is not a U.S., European or Asian threat… these attacks are of global concern.

While anti-cyber technologies and strategies that can anticipate threats as well as react to them will be key to neutralizing cyber-attacks, they will be far more effective if nations work together, share information, develop industry-led standards for knowledge exchange, risk assessment and management, and share technology advances in a timely manner.

Just as industrial stove-piped structures can cripple innovation, so, to, can a stove-piped national approach to cyber security defeat these insidious threats.

www.kratoscomms.com

SATNEWS PUBLISHERS

DIGITAL EDITIONS

SatMagazine • MilsatMagazine • SatNews.com

» *Free subscription and access*

Timely news and editorial «

» *Complete archives*

Join at: *satnews.com/reg*

LEVERAGING THE POWER OF COMMERCIAL INNOVATION

Developing improved battlefield communications

By Ken Peterman, President, Government Systems, Viasat

Across today's evolving battlespace, our forces need to stand at the ready — prepared to deploy anywhere in the world at a moment's notice.

When a military crisis unfolds, the nation's warfighters must be equipped with the latest advancements in technology to ensure they maintain and secure the tactical edge against hostile actors.

Historically, the U.S. Department of Defense (DoD) has been the driver of technological innovation. Starting with the space race that propelled Americans to the moon in the late 1960s, to the creation of the World Wide Web, the DoD pushed the boundaries of what the world thought was possible to implement.

Yet, over the past 25 years, a shift has occurred in many areas — technology leadership is no longer being driven by the military, but rather by the private sector.

Driven by exponential market pressures, today's commercial industry clearly leads development in mobile networking and satellite communications; this is technology that is now essential for nearly every warfighter mission set.

As threats from worldwide terrorist organizations and near-peer adversaries continue to grow, warfighters must be provided with the most advanced technology and communications solutions available.

While a number of military leaders are keenly aware and supportive of the need to leverage the power and speed of commercial innovation, such views are still not widely accepted. In fact, the U.S. Government must be transformed about the way in which agencies and organizations think about, acquire and deploy new technologies.

At Viasat, a new approach is being taken to government procurement. Viasat is able to identify and apply the technologies so desperately needed to rapidly solve actual battlespace challenges.

Through an agile development process and flexible business model, Viasat continually develops new capabilities to meet warfighter requirements as a non-developmental item (NDI). This unique approach allows the company to deliver game changing products and services in a matter of months, compared to what often takes nearly 10 years through standard government procurement practices.

An example is a commercial model-at-work — the development of Viasat's **AN/PRC-161 Handheld Link 16** (***HHL16***) radio (***see image to right, center***).

In June of 2014, there was an air strike that marked one of the most tragic "friendly fire" incidents in more than a decade of U.S. military operations in Afghanistan. When Viasat learned of this calamity, the company's team immediately acted — a better way had to be developed to assist in preventing similar friendly fire incidents in the future.

Viasat met with active and former military personnel and learned that targeting coordination, which includes the positions of friendly fire and ground forces, was conducted almost entirely by voice communications between the **Close Air Support** (***CAS***) pilot and warfighters on the ground. Due to a multitude of factors, including intermittent and unreliable communications, Viasat learned this was an imprecise process that had to be changed.

In just 17 short months, Viasat took the concept of a HHL16 radio that was sketched on the back of a napkin to delivering a number of units to **Special Forces Joint Terminal Attack Controllers** (***JTACs***) to undergo operational assessment. Shortly thereafter, the HHL16 successfully completed operational assessment and the radio immediately entered production earning the official nomenclature "**AN/PRC-161**."

Today, Viasat's AN/PRC-161 HHL16 radio provides precise targeting coordination through what is now called **Digitally Aided Close Air Support** (***DACAS***). Pilots and JTAC's are now equipped with a tool that provides precise position and location accuracy and reliable communications, so that deadly mistakes are less likely to happen.

Viasat's development of the AN/PRC-161 is but one example of successful communications provisioning; by leveraging the power of technology leadership and the agility of commercial innovation, the DoD can now ensure they are delivering lifesaving technology to warfighters when most needed — on the battlefield.

At Viasat, the steps the DoD is taking to provide military forces with commercial technologies is most heartening; however, more needs to be done to ensure cultural inertia does not bog down development and that an overly complex acquisition processes becomes just a reminder of past challenges.

Leveraging commercial innovation is a largely untapped opportunity for military and government leaders to revamp their acquisition models for the 21st century — leaders must accelerate the deployment of new warfighter capabilities to shorten missions and save lives.

www.viasat.com/industries-applications/defense

Ken Peterman serves as Viasat's President of Government Systems, a market leader in tactical networking and Link-16 datalinks; information assurance and cybersecurity; assured, high capacity satellite communications; and air/ground situational awareness. Under Ken's leadership, Viasat is leveraging shifts in technology paradigms to bring game-changing operational capabilities to the warfighter faster than ever before to dramatically enhance mission efficacy and improve safety for warfighters both in the U.S. and among international coalition forces.

THE GOVERNMENT SATELLITE REPORT

U.S. Army demands consumer-like access to SATCOM

By Ryan Schradin, Executive Editor, GSR, and MilsatMagazine Sr. Contributor

A satellite-focused breakfast and panel discussion was held at this year's recent Association of the United States Army (AUSA) Annual Exposition and Convention.

This panel included a number of senior decision makers from the Army and United States Department of Defense (DoD), as well as senior thought leaders from private industry, who came together to talk about the Army's satellite requirements. What many of the panelists at this breakfast were asking was, "*why can't acquiring satellites be as fast and easy as buying a cell phone*?"

The answer may not be as cut and dry as some would think. Military decision makers are increasingly relying on data-centric operations and capabilities that require high bandwidth connections in theater.

The Army is demanding ISR comprised of high definition, real time video instead of static, low quality images. They want geospatial intelligence available to soldiers to ensure they have knowledge of the terrain around them and the movements of alliance forces.

Satellite connectivity is necessary for filling these connectivity and bandwidth requirements abroad. In places where terrestrial networks have never been built, or can't be trusted, satellite can deliver bandwidth for mission-critical capabilities.

This is especially the case in places like the AFRICOM Area of Responsibility (AOR), where, as Brigadier General ***Christopher Eubank***, the Commandant of the **U.S. Army Signal School**, claimed, "*We relied heavily on SATCOM in the AFRICOM AOR. That is a place in the world where they skipped generations of IT. They went from copper to 4G LTE. There is not a lot of CAT5 and CAT6 cable in that country.*"

The U.S. Army remains one of the largest consumers of satellite services for a very good reason — they're extremely large and really spread out geographically. To get IT capabilities to the warfighter at the tip of the spear – sometimes in the world's most isolated and remote locations — satellite is essential.

With satellite playing such a vital role in a modern military, why is it so hard for the Army to get the bandwidth they need at a faster rate?

What are the Warfighter Concerns?

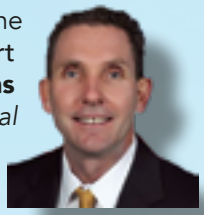
If something was essential for your survival and wellbeing, you'd want it close by or relatively easy to find.

People that need to take medicine to survive don't usually let their prescriptions run out. Why is satellite connectivity so difficult for the Army to access? Especially with the military owning and operating their own satellite constellation — the **Wideband Global Satellite** (***WGS***) system?

Part of the challenge rests with WGS itself. There are simply too many stakeholders and internal customers within the military for the bandwidth that's available via WGS.

If military satellite communications (MILSATCOM) isn't going to be available to U.S. Army users, then commercial satellite communications (COMSATCOM) needs to be there to fill those holes. Unfortunately, getting COMSATCOM services has never been fast or easy for the branches of the military.

A panel of military and industry satellite experts discussed the need for faster access to higher bandwidth satellite services.



According to ***Mike Nichols***, the Chief of the Commercial SATCOM Technical Support Branch at the **Defense Information Systems Agency** (DISA), "*This is a very transactional business... each requirement that comes in is an individual acquisition. Generally, we have plus or minus 100 contracts…for SATCOM services. Each one of these is an individual acquisition, and acquisitions can take some time... If I hear one thing from my customers, it's that the acquisition takes too long.*"

The reason for the delay comes down to how satellite service procurement is conducted, and those procurements are often conducted just like acquisitions for everything else — from rations to tanks.

As Mr. Nichols explained, historically, COMSATCOM services have been acquired in singular transactions to fill individual needs on the spot market. This is effectively the most expensive way to purchase satellite bandwidth.

It also puts military users in a situation where they're purchasing whatever satellite bandwidth is left available, as most of the capacity has already been sold to commercial customers.

Artistic rendition of the Wideband Global Satellite (WGS) system.

As the CEO of **SES Government Solutions**, ***Pete Hoene***, explained, "*Only 10-20 percent of revenue for COMSATCOM owner/operators comes from the U.S. government. The majority is from commercial customers that strike long term contracts and business relationships with owner/operators to ensure they get exactly what they need at an affordable price. This is very different from the U.S. Government buying* capacity on the spot market using LPTA contracts that sub optimize on performance, cause a race to the bottom on pricing, and provide little incentive for industry to invest in capabilities the U.S. Government needs."

However, there has been some positive movement away from purchasing, LPTA ("lowest price, technically acceptable") satellite connectivity on the spot market. One of these positive steps was the recent blanket purchase agreement (BPA) that the Department of Defense (DoD) awarded to SES for their O3b MEO satellite services.

This BPA allows military users to purchase SES O3b MEO managed services up to $516.7 million over five-years. By putting the BPA in place, the DoD has been able to drastically cut the amount of time needed to acquire satellite services.

The BPA, and its ability to cut acquisition time, was touted by Mr. Nichols, who said, "*We're initiating a number of Blanket Purchase Agreements. This cuts the acquisition time down to a remarkable level, really, when you think about it…Most BPA task orders can be awarded within 17 business days.*"

However, that could be 17 days too many when mission-critical satellite solutions are needed. When a problem arises, the **Combatant Commands** (COCOMS) face massive pressure to have connectivity available immediately, like it would be in a commercial environment.

Brigadier General ***Christopher Eubank*** did an excellent job of describing this pressure when he said, "*As a COCOM J6 with an AOR of 53 countries – massive continent – your boss walks in and says, 'I have a problem in Country X. I need this. I need it now.' The last thing he wants to hear is that it takes me 17 days to get that bandwidth. Let me explain what he's expecting. He's expecting that [it's similar to when] he walks into Verizon and buys a phone. It's provisioned and he walks out with a service.*"

How can the military create a situation where SATCOM services are always available to the warfighter when and where they're critically needed?

Partnering for a SATCOM Pool

Although the BPA is a step in the right direction, it still takes time between identifying the need for SATCOM solutions and effectively acquiring them through the BPA.

In addition, the bulk of satellite purchases outside of the BPA are still done on the spot market. A system that, according to Mr. Hoene, treats COMSATCOM services as a "*commodity*" and COMSATCOM providers, "*just like any old vendor*," when they should be treated, "l*ike a strategic partner*," and the capacity treated as vital infrastructure (similar to the way the U.S. Government buys fiber).

That's because, by more closely aligning with the satellite industry, the military could find some reasonable alternatives that will make satellite bandwidth more readily accessible at the speed of war.

One concept floated by the panelists involved the creation of a "*bandwidth on demand*" pool of satellite resources that could be tapped into by military organizations when and where they needed them.

In this instance, satellite resources would be acquired in advance. With tight, restricted budgets, it was difficult for military organizations to spend dollars on something that they wouldn't benefit from or use immediately. However, the appetite for that could be changing.

According to Mr. Nichols, "*One of the areas that we are exploring is establishing a core network... As customers have a demand for service, we would already have a core network in place in various bands for various services that would essentially lead to a very rapid ability to acquire that bandwidth because that bandwidth would already be in place.*"

To help make such a system as this possible, industry and the military could work together to shape requirements and identify an acquisition model that would work for both parties.

This sentiment was shared by Mr. Hoene when he said, "*When we talk about bandwidth on demand, we understand that there's an affordability aspect. There has to be a creative and innovative way to make this happen from a contracts perspective...*"

As the discussions at this year's AUSA SATCOM panel illustrated, today's military relies too heavily on IT services and capabilities to not have immediate, on-demand access to the secure satellite communications they need to keep the warfighter connected.

COMSATCOM providers can no longer be, "*just another old vendor.*" They are key strategic partners providing a necessary warfighting tool.

By working together, the military and satellite industry can identify innovative acquisition models and methods to ensure that satellite connectivity is always there when it's needed.

This article first appeared on GovSat. To read additional, informative articles, please visit ***ses-gs.com/govsat/#***

Ryan Schradin is the Executive Editor of GovSat Report. A communications expert and journalist with more than a decade of experience, Ryan has edited and contributed to multiple popular online trade publications focused on the satellite, unified communications and network infrastructure industries. In addition to editing content and establishing editorial direction, Ryan also contributes articles about satellite news and trends, and also conducts both written and podcast interviews for the GovSat Report. Ryan also contributes to the publication's industry event and conference coverage, providing in-depth reporting from leading satellite shows. Ryan is a Senior Contributor for MilsatMagazine.

SATCOM DIRECT CYBERSECURITY GUIDANCE

Protection from take off to touchdown...

These days, the buzz word "*cybersecurity*" is tossed around frequently — but what does this word it really mean?

Cybersecurity is the business and processes of protecting IT systems, networks and computers from the theft of electronic assets, information and data. This is a real concern in a constantly connected and digitally evolving world.

When device mobility is added in, and then topped off with an extremely dynamic, technological landscape, the chances of a malicious attack by an unauthorized party grows exponentially. Data or information can be hijacked and compromised from ransomware, phishing schemes, brute force attacks, denial of service or engineered malware. Even the most vigilant organizations, which understand the gravity of the situation, are still prone to a myriad of attacks.

Return-on-Investment (ROI) for cybersecurity used to be something that was difficult to monetize. Every day cybersecurity is becoming easier to quantify and, some would argue, invaluable for organization and business inclusion.

The damage that a carefully orchestrated attack on an organization can do, financially and in terms of damage to the brand and image, far exceeds the costs necessary to protect the organization, whether a major corporation or a small or medium business.

In fact, a report in 2015 by **Lloyds** estimated that cyber attacks cost worldwide businesses as much as $400 billion a year — a number that includes direct damage to business resources, as well as an enormous amount of funding to correct for post-attack disruption to the normal course of business.

Estimates are that this dollar amount will continue to increase in the future. Cyber strikes incursions that require just a minimal amount of time to infect a target business could take a surprisingly long time to remove from the victim's system, and then sanitize.

Cybersecurity: SD's Protection

Within the constantly connected and digital world, these environments — the home, the office and, yes, the sky — are now rich targets for digital infection.

Connectivity is required for most forms of videoconferencing, emails, messaging, social media and entertainment, to name but a few. Users who are traveling at 500 knots per hour at an elevation of 40,000 feet might believe they are impervious to these attacks. Unfortunately, such is not the case.

Persistent threats do not care how fast or high a target is traveling — system compromise is the goal. Add in that those traveling in the world of organizational and private aviation often have a great deal to lose if they become the focus of a cyber attack, from top secret government documents, military plans, monetary assets, confidential corporate information or Intellectual Property — all can be acquired by those whose aim is to disrupt and destroy data.

An example of successful counter cyber attack security is a recent flight completed by a Fortune 50 client within their corporate jet that was outfitted with SD hardware and software. This configuration, coupled with SD 24/7 threat monitoring, allowed the SD Cybersecurity team to proactively prevent an ongoing threat to a device in use aboard the plane. Flying internationally, the team of executives were all connected via several devices on board the plane.

The SD Incident Response team discovered a situation where one user was connecting to a host website with an unencrypted login, where the user's credentials were being relayed in plain text. This presented a concern, for the user was being

Screenshot of Satcom Direct Threat Monitoring solution.

exposed to significant risk in having their login credentials and personal, identifiable information potentially stolen.

The SD cybersecurity technology immediately blocked the connection and at no time was the legitimacy of the network in jeopardy. The SD team followed up quickly with the CIO and team at the client location to explain the situation and details in depth.

Satcom Direct takes cybersecurity seriously. The SD Threat Monitoring subscription provides real-time data monitoring, safeguarding valuable information. The SD Direct team also provides security discovery and on-site risk assessments to protect an organization, aircraft and hangar.

www.satcomdirect.com/cybersecurity/

Satcom Direct (SD) and its companies provide global connectivity solutions for business and general aviation, military, government, and head of state aircraft. The company also provides land mobile services to areas with connectivity limitations. Since 1997, SD has worked to advance the technology of global connectivity, being first to market with many new capabilities in communications technology. SD's industry leading connectivity solutions are complemented by their divisional capabilities including SD Avionics cabin and flight deck systems and SD software solutions. A premier Inmarsat distribution partner (including Jet ConneX), Iridium service partner, and ViaSat Ku preferred reseller, SD is also the exclusive service provider for SmartSky Networks, and the Master Distributor of Intelsat FlexExec.

SD World Headquarters and primary operations center is located in Melbourne, Florida, with additional office locations in the United States, Canada, UK, UAE, Switzerland, Hong Kong, Australia, Russia, Brazil, and South Africa.

SATCOM FRONTIER

PERSPECTIVE

KU-BAND VERSUS KA-BAND… SEPARATING FACTS FROM FICTION

By Chris Hudson, Senior Technical Advisor, Intelsat General

The launch of next-generation, high-throughput satellite (HTS) constellations by multiple commercial operators has ushered in a new age of performance in satellite communications and has also reinvigorated an enduring debate within the industry regarding which frequency is superior: Ku-band vs. Ka-band.

With that debate has come many mis-characterizations and obfuscations regarding the power, resiliency and availability that Ku-band, including Intelsat's global HTS, brings to bear for the company's government customers — I aim to separate fact from fiction.

At Intelsat General, we've written on this topic before and recent claims have led me to return to the issue. In particular, I read with interest some of the statements made in a blog post published by an Inmarsat executive earlier this year.

In the piece, the author states that "*Ka-band terminals can switch seamlessly between MILSATCOM and COMSATCOM always-on systems, permitting users to make the best choice for their mission.*"

This was surprising, as there is no publicly advertised terminal that can 'switch seamlessly' between military and commercial Ka-band systems. I know of no terminals approved for use on commercial Ka-band systems, such as Inmarsat Global Xpress (GX) or ViaSat Exede, that are also approved to operate on the U.S. government's Wideband Global SATCOM (WGS) satellite constellation. Similarly, in the reverse, I know of no WGS-approved terminals that are compatible with, let alone can seamlessly switch to, Inmarsat GX or ViaSat Exede.

A WGS-approved terminal is authorized to operate on Inmarsat's leasable, steerable spot beams. While this provides access to some 500 leasable TPEs (transponder equivalents of 36 MHz each) worldwide, it pales next to Ku-band, which has a global supply of over 7,000 leasable TPEs. Ku-band provides the desired compatibility with an unrivaled depth and breadth of bandwidth options.

There are terminals with swap-out kits for C-, X-, Ku- and military Ka-band. Using a kit, an installer can swap a few terminal parts, even while in the field, and convert a terminal from Ku- to Ka-band operations, but this does not qualify as "seamless switching."

The blog post also claims ubiquitous coverage, "*Another advantage of Ka vs Ku stems from the fact that older Ku-band satellites distribute power throughout the world via large regional beams, resulting in irregular 'hot' and 'cold'*

spots for data transmission. Platforms in a cold spot can experience bandwidth drop by as much as 90 percent. Ka-band high-throughput satellite (HTS) coverage, on the other hand, is created by many smaller 'spot' beams whose hot spots can be 'stitched' together, resulting in highly consistent coverage. This ubiquitous coverage leaves no AISR user 'out in the cold' when the need for high-fidelity intelligence from a remote area is required."

This statement is patently incorrect. First of all, the statement leads with an apples-to-oranges comparison of older Ku-band wide-beam satellites to the newer Ka-band HTS. Ku-band HTS constellations are here now and have been for years. The Intelsat **Epic^{NG} IS-29e** satellite has been in service since early 2016. Ku-band HTS have the same hot spots which can also be stitched together for consistent, efficient, high data rate services.

Putting that comparison aside, the only ubiquitous, fully global, Ka-band system — namely, Inmarsat's Global Service Beams — has a 19 percent hole in each "ubiquitous" coverage area. Per the blog's terminology, each satellite stitches together 89 spot beams to provide ubiquitous coverage. However, per Inmarsat, at any one time, only 72 of those 89 beams can be active. In other words, at any given time, 19 percent of the beams are off, so 19 percent of the coverage area has no meaningful bandwidth available for use.

Another key coverage difference, and advantage, of Ku- over Ka-band HTS is satellite depth and overlap. There are four Inmarsat I-5 GX satellites to cover the entire globe. Two-thirds of all locations see only a single I-5 satellite and are, therefore, only covered by a single Global Service spot beam. There is no overlapping satellite to provide additional and/or backup capacity.

The Intelsat Epic^{NG} constellation has five satellites worldwide that are designed to provide layered coverages in many areas, with a sixth one launching in 4Q18. In addition, these HTS overlays are backed up by Intelsat's global constellation of wide-beam satellites. This depth of coverages provides end users with resiliency and redundancy unavailable in Ka-band. Switching between these Ku-band options is possible because of the open architecture compatibility between Intelsat Epic^{NG}, Intelsat wide-beam and other Ku-band HTS and wide-beam satellites.

This aspect of open architecture is a critical aspect of Intelsat Epic that is completely unaddressed in the Inmarsat blog post. An HTS offering can be either 'open' or 'closed.' Each type has common characteristics in terms of technologies used and services supported. Closed HTS architectures include **ViaSat Exede**, **Inmarsat Global Xpress**, **Hughes Network Systems Jupiter**, and **Eutelsat KA-SAT**. Open HTS architectures include **Intelsat Epic^{NG}**, **Telesat VANTAGE** and **SES Ku HTS**, to name a few.

On a closed-architecture HTS, a customer can use only operator-selected platforms and terminals. In addition, there is no switching between closed systems. An Inmarsat GX Ka-band terminal will not operate on ViaSat's nor Hughes' Ka-band systems. With Intelsat's open-architecture Ku-band HTS, users choose their preferred ground equipment, be that an installed base or a newly selected platform.

The ability to use existing ground equipment in open systems can lead to substantial cost savings, while the ability to select a new platform now, or in the future, protects end users from the trap of proprietary systems where they do not have control. These end user platforms can operate on Intelsat's and easily switch to others open-architecture Ku-band systems.

In addition to requiring proprietary ground equipment, closed HTS systems offer only star topology networks. This means that all remote terminal traffic must route via a limited number of gateways or access stations. That is similar to commercial airline travel, where one must travel through an airline's hub to reach a certain city, even if that is not the shortest or fastest way to the final destination.

Closed architecture HTS do not allow loopback within a single spot beam, nor custom beam-to-beam connections. Both are possible with Intelsat Epic^{NG}. This flexibility enables faster routing and, possibly more importantly, installation of all ground hardware at end user locations, not at third party facilities.

One part of the Inmarsat blog with which I can agree is the call for increased industry and government collaboration in support of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) operations. Toward that end, Intelsat is constantly innovating, improving the technology on each Intelsat Epic^{NG} satellite. For example, the soon to be launched **Horizons 3e** will be the most advanced HTS satellite to enter service.

Horizons 3e is the first satellite to feature an entire Ku-band payload using multi-port amplifiers that optimize power distribution across the satellite's beams. With the multi-port amplifier, if one spot beam is lightly utilized, its allocated power can be distributed to other beams to meet customer throughput demands.

When you distill the facts from the claims and counterclaims, Ku-band SATCOM provides the most compelling HTS value proposition for customers requiring resilient, flexible and secure high-throughput global coverage.

www.intelsatgeneral.com

Chris Hudson is the Senior Technical Advisor of the Engineering and Services Delivery for Intelsat General Corp.

The preceding article is courtesy of Intelsat General's SatCom Frontier infosite, their editorial team and the named author.

DARPA ACTIVELY ADDRESSING AI

Playing a leading role with the "AI Next" campaign

Over the agency's 60 year history, DARPA has played a leading role in the creation and advancement of artificial intelligence (AI) technologies that have produced game-changing capabilities for the Department of Defense (DoD).

Starting in the 1960s, DARPA research shaped the first wave of AI technologies, which focused on handcrafted knowledge, or rule-based systems, capable of narrowly defined tasks. While a critical step forward for the field, these systems were fragile and limited.

Starting in the 1990s, DARPA helped usher in a second wave of AI machine learning technologies that created statistical pattern recognizers from large amounts of data.

The agency's funding of natural language understanding, problem solving, navigation and perception technologies has led to the creation of self-driving cars, personal assistants, and near-natural prosthetics, in addition to a myriad of critical and valuable military and commercial applications.

However, these second wave AI technologies are dependent on large amounts of high quality training data, do not adapt to changing conditions, offer limited performance guarantees, and are unable to provide users with explanations of their results.

To address the limitations of these first and second wave AI technologies, DARPA seeks to explore new theories and applications that could make it possible for machines to adapt to changing situations.

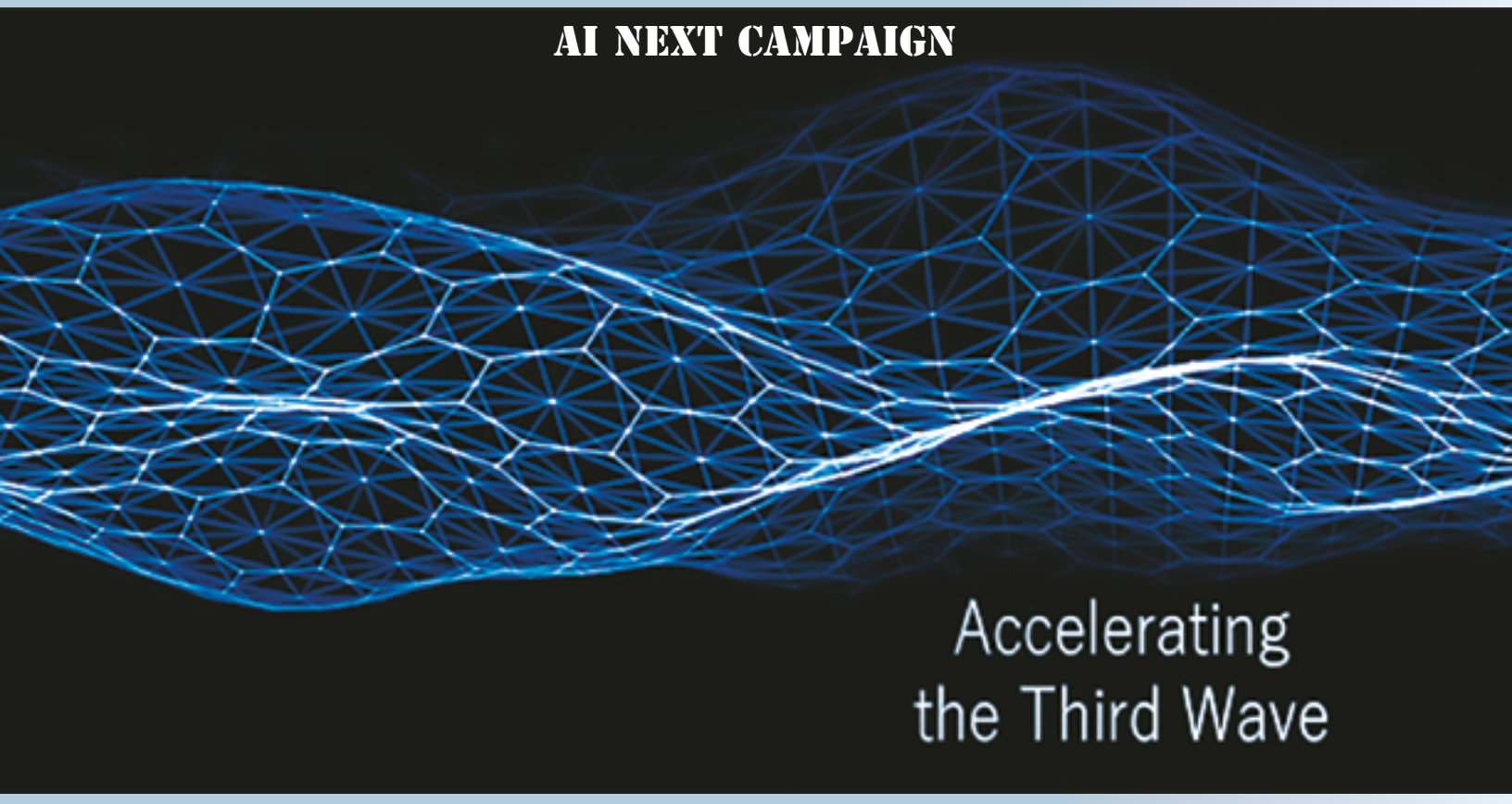
Accelerating the Third Wave

The advance of technology has evolved the roles of humans and machines in conflict from direct confrontations between humans to engagements mediated by machines.

Originally, humans engaged in primitive forms of combat. With the advent of the industrial era, however, humans recognized that machines could greatly enhance their warfighting capabilities. Networks then enabled teleoperation, which eventually proved vulnerable to electronic attack and subject to constraint due to long signal propagation distances and times.

The next stage in warfare will involve more capable autonomous systems, but before we can allow such machines to supplement human warfighters, they must achieve far greater levels of intelligence.

Traditionally, we have designed machines to handle well-defined, high-volume or high-speed tasks, freeing humans to focus on problems of ever-increasing complexity.



In the 1950s and 1960s, early computers were automating tedious or laborious tasks. It was during this era that scientists realized it was possible to simulate human intelligence and the field of artificial intelligence (AI) was born. AI would be the means for enabling computers to solve problems and perform functions that would ordinarily require a human intellect.

Early work in AI emphasized handcrafted knowledge, and computer scientists constructed so-called expert systems that captured the specialized knowledge of experts in rules that the system could then apply to situations of interest. Such "first wave" AI technologies were quite successful — tax preparation software is a good example of an expert system — but the need to handcraft rules is costly and time-consuming and therefore limits the applicability of rules-based AI.

The past few years have seen an explosion of interest in a sub-field of AI dubbed machine learning that applies statistical and probabilistic methods to large data sets to create generalized representations that can be applied to future samples.

Foremost among these approaches are deep learning (artificial) neural networks that can be trained to perform a variety of classification and prediction tasks when adequate historical data is available.

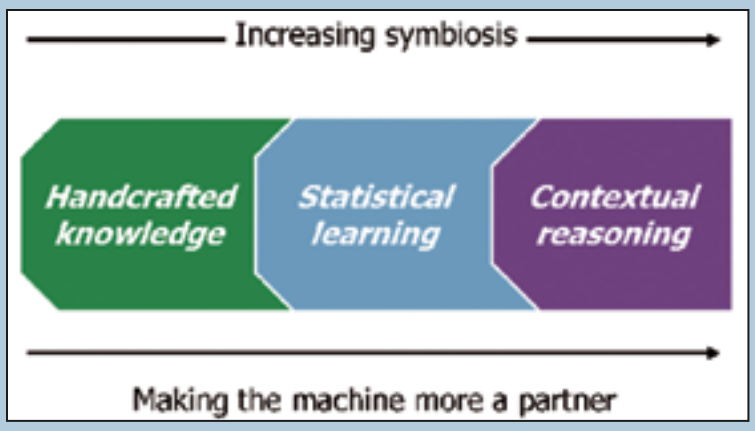
Therein lies the rub, however, as the task of collecting, labelling, and vetting data on which to train such "*second wave*" AI techniques is prohibitively costly and time-consuming.

DARPA envisions a future in which machines are more than just tools that execute human-programmed rules or generalize from human-curated data sets. Rather, the machines DARPA envisions will function more as colleagues than as tools.

Toward this end, DARPA research and development in human-machine symbiosis sets a goal to partner with machines. Enabling computing systems in this manner is of critical importance because sensor, information, and communication systems generate data at rates beyond which humans can assimilate, understand, and act.

Incorporating these technologies in military systems that collaborate with warfighters will facilitate better decisions in complex, time-critical, battlefield environments; enable a shared understanding of massive, incomplete, and contradictory information; and empower unmanned systems to perform critical missions safely and with high degrees of autonomy.

DARPA is focusing its investments on a third wave of AI that brings forth machines that understand and reason in context. The agency sees this next generation of AI as a third wave of technological advance, one of contextual adaptation. To better define a path forward, DARPA is announcing today a multi-year investment of more than $2 billion in new and existing programs called the "***AI Next***" campaign.



DARPA is currently pursuing more than 20 programs that are exploring ways to advance the state-of-the-art in AI, pushing beyond second-wave machine learning techniques towards contextual reasoning capabilities.

In addition, more than 60 active programs are applying AI in some capacity, from agents collaborating to share electromagnetic spectrum bandwidth to detecting and patching cyber vulnerabilities.

Over the next 12 months, DARPA plans to issue multiple Broad Agency Announcements for new programs that advance the state of the art in AI.

Under ***AI Next,*** key areas to be explored may include automating critical DoD business processes, such as security clearance vetting in a week or accrediting software systems in one day for operational deployment; improving the robustness and reliability of AI systems; enhancing the security and resiliency of machine learning and AI technologies; reducing power, data, and performance inefficiencies; and pioneering the next generation of AI algorithms and applications, such as "explainability" and commonsense reasoning.

In addition to new and existing DARPA research, a key component of the campaign will be DARPA's ***Artificial Intelligence Exploration*** (AIE) program that was first revealed in July 2018.

DARPA announced in September of 2018 a multi-year investment of more than $2 billion in new and existing programs for this campaign.

AI Next builds on DARPA's five decades of AI technology creation to define and to shape the future, always with the Department's hardest problems in mind. Accordingly, DARPA will create powerful capabilities for the DoD by attending specifically to the following areas:

New Capabilities

AI technologies are applied routinely to enable DARPA R&D projects, including more than 60 exisiting programs, such as the Electronic Resurgence Initiative, and other programs related to real-time analysis of sophisticated cyber attacks, detection of fraudulent imagery, construction of dynamic kill-chains for all-domain warfare, human language technologies, multi-modality automatic target recognition, biomedical advances, and control of prosthetic limbs.

DARPA will advance AI technologies to enable automation of critical Department business processes. One such process is the lengthy accreditation of software systems prior to operational deployment. Automating this accreditation process with known AI and other technologies now appears possible.

Robust AI

AI technologies have demonstrated great value to missions as diverse as space-based imagery analysis, cyberattack warning, supply chain logistics and analysis of microbiologic systems. At the same time, the failure modes of AI technologies are poorly understood.

DARPA is working to address this shortfall, with focused R&D, both analytic and empirical. DARPA's success is essential for the Department to deploy AI technologies, particularly to the tactical edge, where reliable performance is required.

Adversarial AI

The most powerful AI tool today is machine learning (ML). ML systems can be easily duped by changes to inputs that would never fool a human. The data used to train such systems can be corrupted. And, the software itself is vulnerable to cyber attack. These areas, and more, must be addressed at scale as more AI-enabled systems are operationally deployed.

High Performance AI

Computer performance increases over the last decade have enabled the success of machine learning, in combination with large data sets, and software libraries. More performance at lower electrical power is essential to allow both data center and tactical deployments.

DARPA has demonstrated analog processing of AI algorithms with 1000x speedup and 1000x power efficiency over state-of-the-art digital processors and is researching AI-specific hardware designs. DARPA is also attacking the current inefficiency of machine learning, by researching methods to drastically reduce requirements for labeled training data.

Next Generation AI

The machine learning algorithms that enable face recognition and self-driving vehicles were invented over 20 years ago. DARPA has taken the lead in pioneering research to develop the next generation of AI algorithms, which will transform computers from tools into problem-solving partners.

DARPA research aims to enable AI systems to explain their actions, and to acquire and reason with common sense knowledge. DARPA R&D produced the first AI successes, such as expert systems and search, and more recently has advanced machine learning tools and hardware.

DARPA is now creating the next wave of AI technologies that will enable the United States to maintain its technological edge in this critical area.

In addition to new and existing DARPA research, a key component of the campaign that was previously mentioned will be the agency's Artificial Intelligence Exploration (AIE) program.

AIE constitutes a series of high-risk, high payoff projects where researchers will work to establish the feasibility of new AI concepts within 18 months of award.

Leveraging streamlined contracting procedures and funding mechanisms will enable these efforts to move from proposal to project kick-off within three months of an opportunity announcement.

AIE is an agency-wide program, based on the successful "*Disruptioneering*" fast-tracked solicitation process pioneered by DARPA's Defense Science Office, which supports a variety of technology development concepts.

As with Disruptioneering, AIE will periodically issue special notices, known as "***AIE Opportunities***," tied to topics of interest. The simplified proposal, contracting, and funding process makes it even easier for individuals and organizations to contribute to DARPA's mission.

AIE awards may be worth up to $1 million each, as described in each AIE Opportunity.

Forthcoming AIE Opportunities will be published on the FedBizOpps website (***www.fbo.gov***) (under P**rogram Announcement DARPA-PA-18-02**.

Agency director, Dr. ***Steven Walker*** officially unveiled this large-scale effort during closing remarks at DARPA's **D60 Symposium** that occurred at the **Gaylord Resort and Convention Center** in National Harbor, Maryland.

He said, "*With AI Next, we are making multiple research investments aimed at transforming computers from specialized tools to partners in problem-solving. Today, machines lack contextual reasoning capabilities, and their*

training must cover every eventuality, which is not only costly, but ultimately impossible. We want to explore how machines can acquire human-like communication and reasoning capabilities, with the ability to recognize new situations and environments and adapt to them."

Dr. Walker continued, "*In today's world of fast-paced technological advancement, we must work to expeditiously create and transition projects from idea to practice. Accordingly, AIE constitutes a series of high-risk, high payoff projects where researchers will work to establish the feasibility of new AI concepts within 18 months of award. Leveraging streamlined contracting procedures and funding mechanisms will enable these efforts to move from proposal to project kick-off within three months of an opportunity announcement.*"

For more information about AI Next, please visit:
www.darpa.mil/work-with-us/ai-next-campaign

An informative video that presents DARPA's view on AI is available for veiwing at
www.darpa.mil/about-us/darpa-perspective-on-ai

Major C. David Lewis, USAF Defense Sciences Office (DSO) Program Manager, joined DARPA as a program manager in the Defense Sciences Office (DSO) in January of 2018. Trained as an officer and physicist, Major Lewis is interested in applying the forefront of fundamental physics in unique ways to DoD challenges using the disciplines of quantum mechanics, space and plasmas, and gravitational physics.

He offered information at the DARPA infosite regarding the DARPA Space Environment Exploitation (SEE) program, which seeks to develop new models and sensing modalities to predict and observe the dynamics of the near-Earth space environment.

The SEE program explores how to go beyond magnetohydrodynamic descriptions of the magnetosphere, ionosphere, thermosphere coupled system to include wave/wave, wave/particle, and particle/particle interactions while using the latest advances in high performance computing such as GPUs and TPUs.

Furthermore, SEE is exploring how to unify current space environmental sensing networks to produce a common operating space environment picture and how to develop low cost, non-traditional, exploitive, and expeditionary means to observe near-earth plasma dynamics.

Another big component of SEE is understanding the viability of how AI and Machine Learning can be used to help assimilate environmental data into models and virtually produce synthetic data.

The expected outcomes of SEE will give future commanders and operators the necessary and precise space environment situational awareness to make relevant space operational/tactical decisions and differentiate between human-made and natural dynamic perturbations of the environment.

Posted at the Novawurks infosite is additional information regarding the DARPA SeeMe project, which will provide small squads and individual teams the ability to receive timely imagery of their specific overseas location directly from a small satellite with the press of a button—something that's currently not possible from military or commercial satellites.

NovaWurks seeks to develop a constellation of satlets, at a fraction of the cost of airborne systems, enabling deployed warfighters overseas to hit 'see me' on existing handheld devices to receive a satellite image of their precise location within 90 minutes. The SeeMe constellation may consist of some two-dozen satellites, each lasting 60-90 days in a very low-earth orbit before de-orbiting and completely burning up, leaving no space debris and causing no re-entry hazard.

www.novawurks.com/

Image is courtesy of Novawurks.

SPOTTING AND STOPPING THE SPECTRUM SABOTEURS

A new research project has been launched with the aim of developing a system for detecting threats to the electromagnetic space.

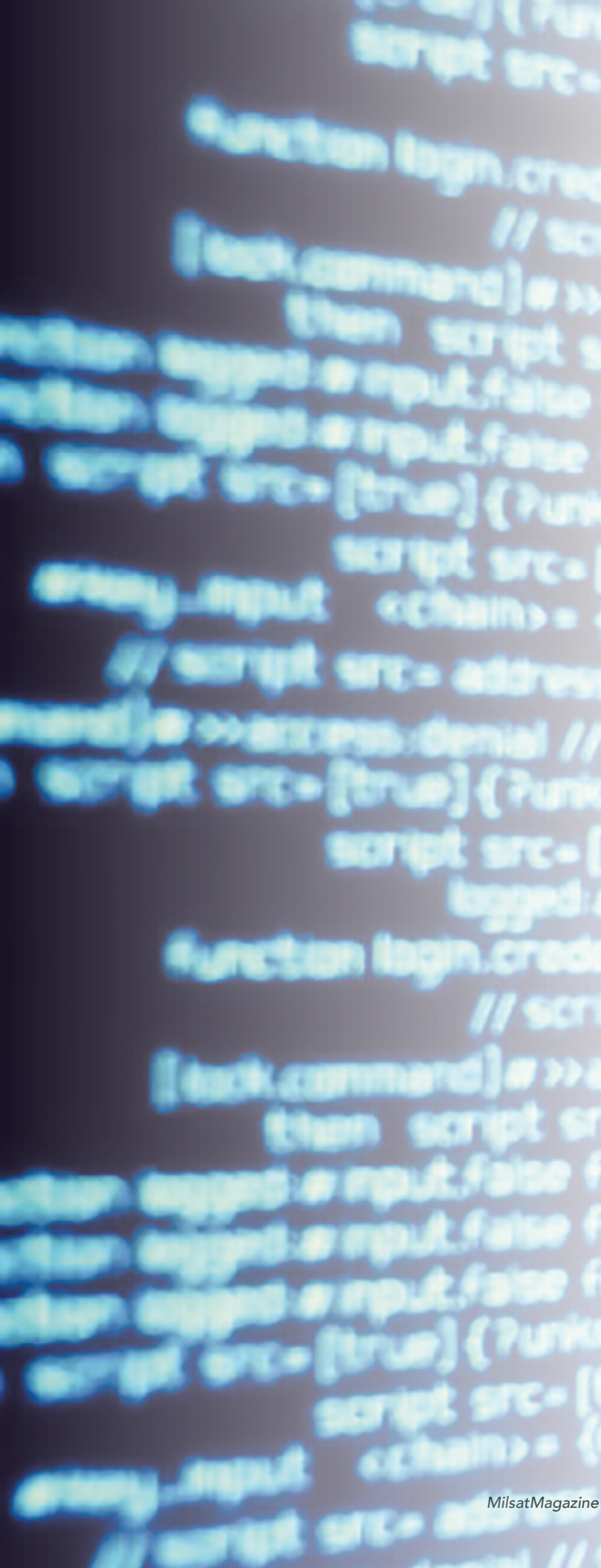
Led by IMDEA Networks Institute (a networking research organization based in Madrid, Spain), the **SOCRATES** project has recently been awarded funding by **NATO's Emerging Security Challenges Division — Science for Peace and Security Program** (SPS).

The two other collaborating partners on the project are the **ElectroSense** non-profit association of Switzerland (a crowd-sourcing initiative that collects and analyzes spectrum data) and **Katholieke Universiteit (KU) Leuven** of Belgium. Their work will be concluded by May of 2021.

In the 21st century, the security of the electromagnetic spectrum has tremendous strategic importance to society. In particular, the wireless infrastructure that carries services such as cellular networks and GPS is especially critical. However, the cost of commodity radio technology prices is now so low that access to it is no longer restricted to governments and network operators. It is now affordable to individuals, giving them the potential to become malicious intruders.

More frequent and more sophisticated threats from such infiltrators could wreak havoc and are among the most serious challenges faced by society. For example, unauthorized transmissions could threaten the operation of networks used by air traffic control systems, police, security and emergency services. The SOCRATES project will deliver a security system to protect the electromagnetic environment and the services and users that depend upon it.

Dr. *Domenico Giustiniano*, Research Associate Professor at IMDEA Networks Institute who is coordinating the project, offered an overview of the project. "*SOCRATES will provide an*



accurate, autonomous, fast and secure system based on a novel and disruptive IoT (Internet of Things) architecture. By detecting and locating unusual RF signal and source activity it will identify intruders in the electromagnetic space, before a threat can become serious, learning about its physical layer features and its geographic location."

Describing his institute's contribution to the project, the researcher continued, "*IMDEA Networks will lead the investigation of the quality of spectrum sensors in a crowdsourced system, challenged by the large amount of data processed by the system, and of the distributed localization of emitters, challenged by the lack of synchronization among the spectrum sensors — two areas in which we build upon our extensive expertise.*"

The SOCRATES solution will need to be suitable for real-world implementations. Giustiniano explains how this will be achieved.

"*We plan to test the SOCRATES system in controlled and realistic conditions, operating in both licensed and unlicensed spectra. Real experiments will showcase the system's ability to detect the waveforms and wireless technologies of adversaries who are misusing wireless resources. We'll also demonstrate how the physical location of an intruder can be swiftly identified. Adopting an agile approach, we'll build, demonstrate and showcase early prototypes throughout the project.*"

By providing the capability to detect, identify and locate potential threats to electromagnetic infrastructure security, SÓCRATES (Large Scale Collaborative Detection and Location of Threats in the Electromagnetic Space, Grant G5461) represents an important step in ensuring society's readiness to respond effectively to them. SOCRATES will shield economic and social structures from those who would harm them.

www.networks.imdea.org

Dr. Domenico Giustiniano is Research Associate Professor (tenured) at IMDEA Networks Institute and leader of the Pervasive Wireless Systems Group. Dr. Giustiniano is leader of the OpenVLC project, an open-source platform for research in visible light communication networks and co-founder of the non-profit Electrosense association, a crowd-sourcing initiative to collect and analyze spectrum data. Before joining IMDEA, he was a Senior Researcher and Lecturer at ETH Zurich. He also worked for a total of four years as Post-Doctoral Researcher in industrial research labs (Disney Research Zurich and Telefonica Research Barcelona).
IMDEA Networks Institute is a research organization on computer and communication networks whose multinational team is engaged in cutting-edge fundamental science and technology. As a growing, English-speaking institute located in Madrid, Spain, IMDEA Networks offers a unique opportunity for pioneering scientists to develop their ideas.

MISSION: BROADBAND IN A BACKPACK

At the top of the world...

By Ulf Sandberg, Managing Director, Paradigm

Paradigm's high-speed SWARM satellite terminal provided invaluable support for the RAF on their Himalayan Venture 18 (HV18) this September.

HV18 was the principal expedition of RAF100 — the celebration of the centenary of the formation of the **Royal Air Force**, the first independent Air Force in the world. The expedition united 75 members of the wider RAF family in a pioneering expedition to the **Rolwaling** and **Khumbu** regions of the **Nepalese Himalayan** range. The event brought together individuals with a variety of outdoor experience, ranging from the absolute novice to the experienced mountaineer. HV18 was the largest single service mountaineering expedition to be undertaken.

The SWARM had already been successfully deployed by the RAF for the RAF100 Flypast over Buckingham Palace, back in July 2018. It provided the Air Command Media team with constant communications in the face of high demand from the public on the terrestrial 4G network. For an expedition such as HV18, the SWARM was a perfect fit.

The HV18 expedition aimed to have a significant media presence throughout the venture, to bring awareness to the centenary and exposure for its many charitable and commercial sponsors. In addition, they were climbing in a remote region known for earthquake risk combined with difficult to predict and extreme weather patterns. Contact with the other teams, with the Kathmandu Embassy and access to weather reports was critical to their success.

The four Trekking Teams would be able to access power and WiFi at various tea-rooms and other locations along the way. However, the Alpine Team were going to be climbing at very high altitude, in a remote corner of the **Rolwaling Himal**, with no access to power or existing communication networks.

Consequently, satellite communication was going to be essential. Previous expeditions had relied on BGAN and satphones. While these provided voice options, they were notoriously slow and unreliable for any sort of data upload/download.

The suitability of the SWARM was down to a combination of key features. The complete system is lightweight and easily carried in a backpack; weight is clearly a major consideration on any expedition where everything has to be carried.

Although lightweight, the SWARM is still extremely rugged and specifically designed to operate in tough and demanding environments.

Deployment is rapid — only around 90 seconds is required, with straightforward assembly of the unit's three modules. High-speed, broadband connectivity can then be achieved in less than four minutes with the easy-to-use PIM® (Paradigm Terminal Interface) terminal controller.

In an emergency, and when there are countless other tasks to perform at a base camp, this level of speed is critical. The pointing process is also intuitive and tool-free, using integrated audio and visual pointing cues on the PIM's keypad, and so keeps training to a minimum.

With **Inmarsat** providing the airtime on their **Global Xpress** Ka-Band network, the SWARM was on the team. Now the media plan and Command & Control for the venture could be planned around it.

"*Having the SWARM meant that for the first time on such an expedition we would have a high-speed, high-data connection wherever we were*," said RAF Squadron Leader ***Gordon Henderson*** of the Alpine Team.

With the knowledge of this capability, the RAF was able to plan for a much bigger media presence with daily updates of hi-res photos and full quality videos. Command & Control between all teams would be possible every day, plus increased access to information on weather and regular contact with the embassy would improve safety and knowledge. A super-reliable, easy-to-use broadband connection would also keep the team's morale high during the weeks away from home, often in very challenging conditions.

Once underway, the SWARM did not disappoint. The Alpine Team used the system every day. SWARM's performance was completely unaffected by the heavy monsoon rains, by snow or by sub-zero temperatures nearing -20 degrees.

Using SWARM was so straightforward that, as the expedition progressed, a spare five minutes here and there was enough time for other team members to be trained up to assemble and point it.

At camp, precious power was conserved by switching off the SWARM once the business of the day had been completed. Once pointed, the PIM's commissioning feature meant that any of the team members could simply power it back up and be automatically back on the network, calling family and friends back home and updating their own social media feeds. Command & Control requirements were more straightforward with all teams being able to maintain regular contact with the expedition leader and embassy staff. The media coverage throughout the expedition was exceptional and maintained high levels of exposure for the expedition's sponsors.

The teams provided daily updates on Facebook, Twitter and Instagram, posting hi-res photos and video. The Alpine team were able to stay in touch with the media updates of the other teams too. When the satphones were unable to connect, the SWARM provided the WiFi necessary for daily WhatsApp calls between teams and back home, to family and friends. As RAF Squadron Leader Gordon Henderson said, "*using the SWARM was like having the equivalent of a home WiFi system while living at 5,200 meters.*"

Paradigm's SWARM makes the team.

The Alpine Team achieved their goal of making the first British ascent of Mt Langdung standing at 6,357 meters and also established a new international route.

Squadron Leader Gordon Henderson added, "*On the day of the summit attempt on Langdung, we were able to get up in the early hours, clear the snow off the SWARM and download a weather report before we set out.*"

With the SWARM already deployed across five continents following a swift adoption by the international military and NGO sectors, Paradigm was confident of the product's success during HV18. However, the teams' first-hand accounts of the unit's ease-of-use and high-throughput in such challenging conditions are clear demonstrations of how this remarkable little terminal can make all the difference to mobile users needing reliable communications in areas where terrestrial options are either unavailable or unreliable.

Ulf Sandberg, the Managing Director of Paradigm, noted that the company is proud of the contribution and the difference that the SWARM made to HV18, adding that no other portable terminal on the market can provide the same performance and reliability in those sorts of conditions.

paracomm.co.uk/

Ulf Sandberg has more than 30 years experience in the global satellite and telecommunications world and has spent the past 20 years at the Managing Director of Paradigm.

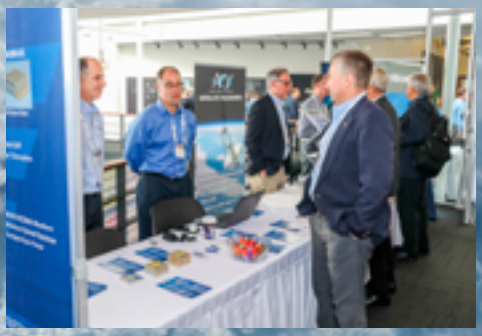
After completing his MSc in Physics at the Royal Institute of Technology in Stockholm, he served in the Swedish Armed Forces. From there, Sandberg joined Notelsat, the operating company for Tele-X, one of the earliest Nordic Communication satellites. From there, he was with the Swedish Attaché for Science and Technology office, based in the USA. Leaving the Government sector, Mr. Sandberg worked for Swedish Telecom International and then Unisource, where he advanced to be Managing Director for the satellite business based in the Netherlands. As well as Versatel in the Netherlands, Mr. Sandberg was also involved in the start-up and creation of a number of companies and ventures in Europe and the USA.

satnews events

Workshops: February 4th
Conference: February 5th-7th

SMALLSAT SYMPOSIUM™

SILICON VALLEY 2019



Register today to unlock the knowledge required to leverage cutting edge SmallSat technology into next-generation solutions.

SMALLSATSHOW.COM