SATCOM for Net-Centric Warfare

MilsatMagazine

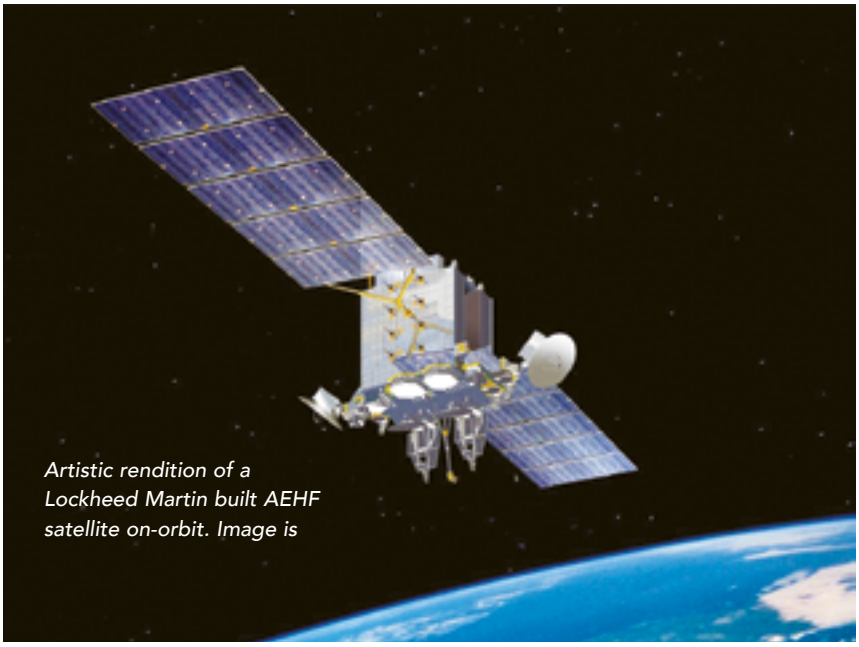
May 2019

TRANSEC
Space Symposium
Saving Lives
Droning On
The Cloud
Briefing
Cybersecurity
Dispatches

A United Launch Alliance (ULA) Delta IV rocket on the launch pad prior to lifting the WGS-10 satellite to orbit. Image is courtesy of United Launch Alliance.

DISPATCHES

Lockheed Martin's AEHF-4 on-orbit test a success



Artistic rendition of a Lockheed Martin built AEHF satellite on-orbit. Image is

Lockheed Martin (NYSE: LMT) has successfully completed their AEHF-4 spacecraft on-orbit test (A4 OOT) that demonstrated the craft has met all requirements.

A4 OOT was the first test to have all six AEHF operational terminals communicating over XDR.

The terminal types include AEHF SMART-T, FAB-T, MMPU, NMT, Global ASNT and ACF-IC2.

The addition of AEHF-4 to the constellation provides a new capability of global extended data rate (XDR) communications. XDR communications provides data rates to its users five times higher than medium data rate (MDR) and 350 times higher than low data rate (LDR) communications.

Milstar, the predecessor to AEHF, uses both LDR and MDR communication modes to directly support the warfighter.

This was the last step before control authority of the satellite is handed over to the U.S. Air Force SMC where it will join the combined AEHF-Milstar constellation.

The AEHF constellation provides global, survivable, highly secure and protected communications for strategic command and tactical warfighters operating on ground, sea and air platforms.

The jam-resistant system also serves international partners including Canada, the Netherlands and the United Kingdom.

Mike Cacheiro, VP of Protected Communications for Military Space, said this is a major milestone to celebrate with the customers at Space and Missiles Systems Center (SMC), the U.S. Air Force and teammates Northrop Grumman, L3 Communications and Aerojet.

As the company turns the focus on launching AEHF-5 in June, one month early, congratulations to everyone involved in completing this one of a kind, high-performance network in space.

This is a tremendous accomplishment for the AEHF program.

www.lockheedmartin.com/en-us/products/aehf.html

SPACEBRIDGE

BRINGING SATCOM TO THE CLOUD

ZERO OVERHEAD, FULLY MANAGED CLOUD-BASED SATCOM SERVICE

SpaceBridge delivers high quality dynamic SCPC BoD (Bandwidth on Demand) satellite connectivity as a fully managed cloud-based service – no hub or even teleport required!

Simply partner up with **SpaceBridge**, sign up for the period of time and amount of bandwidth desired, and you're all set. We'll provision your very own slice of our satellite infrastructure - equipment and optional bandwidth - CAPEX-free, with 24/7 management and technical support, maintenance; full visibility and control included.

Best of all, **SpaceBridge**'s pay-as-you-grow scalability will allow you to cost-effectively expand your satellite communication assets as you go.

Sign up today, and enjoy SpaceBridge's cost-effective, efficient and scalable satellite connectivity-as-a service!

- **High quality dynamic SCPC BoD satellite connectivity**
- **A fully managed, 24/7 cloud-based service**
- **OPEX only subscription engagement basis**
- **Optional teleport services**

SPACEBRIDGE
ALL THINGS CONNECTED

www.spacebridge.com

Table of Contents

Advertiser Index

DISPATCHES

United Launch Alliance Delta IV takes the USAF WGS-10 satellite to orbit

A United Launch Alliance (ULA) Delta IV rocket carrying the tenth Wideband Global SATCOM (WGS) satellite for the U.S. Air Force lifted off from Space Launch Complex-37 on March 15 at 8:26 p.m. EDT. ULA has been the exclusive launch provider for all ten WGS satellites.

"*We are very proud to deliver this critical asset to orbit in support of the U.S. and Allied warfighters deployed around the world defending our national security*," said ***Gary Wentz***, ULA vice president of Government and Commercial Programs. "*Thank you to the entire ULA team and mission partners for their outstanding teamwork and dedication to mission success.*"

The WGS-10 satellite, built by the Boeing Company, is an important element of the new high-capacity satellite communications system. Each WGS satellite provides more wideband communications capacity than the entire Defense Satellite Communications System.

This mission launched aboard a Delta IV Medium+ (5,4) configuration vehicle, built in Decatur, Alabama, including a 5-meter Payload Fairing and standing at 218 feet. The common booster core for Delta IV was powered by the RS-68A engine, and the Delta Cryogenic Second Stage was powered by the RL10B-2 engine, both supplied by Aerojet Rocketdyne. Northrop Grumman provided the four solid rocket motors. At liftoff, the main engine and four solid rocket motors combined to produce approximately 1.7 million pounds of thrust.

To date, ULA has a track record of 100 percent mission success with 133 successful launches.

With more than a century of combined heritage, ULA is the world's most experienced and reliable launch service provider. ULA has successfully delivered more than 130 satellites to orbit that provide Earth observation capabilities, enable global communications, unlock the mysteries of our solar system, and support life-saving technology.

www.unitedlaunchalliance.com

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

DISPATCHES

DISA awards Iridium with EMSS ground site contract

Iridium Communications Inc. (NASDAQ: IRDM) has been awarded a new contract by the Defense Information Systems Agency (DISA) to continue supporting the U.S. Department of Defense (DoD) Enhanced Mobile Satellite Service (EMSS) gateway.

The contract, valued at $54 million over 4.5 years, for Gateway Maintenance and Support Service (GMSS), will ensure that this dedicated ground site continues to operate at peak efficiency and in optimal condition for critical U.S. DoD missions.

Dedicated for use by the U.S. DoD, their Iridium gateway serves as the uplink and downlink point for the DoD's EMSS communications capabilities through the Iridium® network.

This includes the enhanced capabilities made possible by Iridium's upgraded satellite constellation, which was formally completed and declared fully operational in February of this year.

The previous iteration of the GMSS contract was awarded in October of 2013 for a five-year term with a six-month extension option.

The subscribers operating under the Iridium EMSS program run by DISA have more than doubled over the five-year period between 2013 and 2018 to 113,000, reflecting a 17.25 percent compounded annual growth rate.

This surge in growth has occurred under the current flat-rate contract program that provides unlimited voice and data services to the U.S. warfighter and other government participants.

Scott Scheimreif, EVP of government programs, Iridium, said this new contract provides the mechanism for Iridium to help ensure the DoD gateway is able to fully support the new capabilities and services needed to meet the emerging requirements of the warfighter. Scott added that this is another example of the strategic, long-term relationship between Iridium and the U.S. Department of Defense. The company remains committed to the U.S. DoD and the warfighter as new ways for addressing critical requirements leveraging Iridium's unique satellite network are explored.

www.iridium.com

DISPATCHES

GetSAT's MilliSAT terminals receive an Inmarsat blessing

GetSAT has reported that Inmarsat has type approved the company's MilliSAT-H-GX and MilliSAT-W-GX for use on its Global Xpress service.

These new terminals, according to the company, are the lightest and most compact all in one on-the-move solutions serving the Global Xpress high-throughput, global network.

Leveraging GetSAT's highly efficient, patented InterFLAT miniaturized flat panel antenna technologies, these MilliSAT-H-GX and MilliSAT-W-GX are the first Communications-On-The-Move (COTM) terminals for ground vehicles using the worldwide Global Xpress network.

These ruggedized terminals have been proven to operate in some of the toughest environmental conditions. Their combination of size, weight, and fast-tracking technology allows for operation on land-mobile and maritime platforms with aggressive vehicle dynamics.

Size and weight limitations have traditionally been a challenging requirement for land-mobile SATCOM applications. The size and weight of the MilliSAT-H-GX and MilliSAT-W-GX make these terminals well suited for widespread adoption in the land mobile market.

The MilliSAT-H-GX's 25x27 cm. flat panel antenna fits inside a 40 cm. radome allowing easy installation. Additionally, the terminals' low power consumption allows for battery operation, adding greatly to their flexibility. With industry leading SWaP (Size, Weight and Power), the units set a new standard for small, Inmarsat type-approved for SATCOM terminals used with Global Xpress.

GetSAT CEO, *Kfir Benjamin*, said the company is pushing the innovation envelope in creating — and constantly delivering — the industry's most miniaturized terminals for airborne, ground and maritime on-the-move applications. The firm's mission to craft micronized technologies to support a small flat panel enables the company's team to consistently find new ways to successfully reduce terminal size while maintaining strength and power. Their MilliSAT-H-GX and MilliSAT-W-GX terminals were developed to meet Inmarsat's exacting standards and provide users with ease of use.

Steve Gizinski, Chief Technology Officer, Inmarsat Government, added that Global Xpress has drawn a significant number of commercial and government customers due to its unique reliability, ease of use and seamless interoperability with military satellite resources. With the Inmarsat type approval of GetSAT's terminals, ground and maritime on the move users have access to a very compact terminal to support their critical connectivity requirements.

www.getsat.com/products/millsat-w-lm/

www.inmarsat.com/service/global-xpress/

First production representative of Northrop Grumman's EOC is delivered to the U.S. Army

Northrop Grumman Corporation (NYSE: NOC) has delivered to the U.S. Army the first production-representative engagement operations center (EOC) for the Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS).

The delivered IBCS EOC has completed all functional configuration audits for major configuration items and system verification review, and is representative of the production configuration for hardware and software that will undergo qualification testing before IOT&E.

Northrop Grumman is on pace to deliver 11 EOCs and 18 IFCN relays for the IBCS program by the end of the year.

IBCS is a paradigm shift for IAMD by replacing legacy stove-piped systems with a next-generation, net-centric approach to better address an evolving array of threats. The system integrates disparate radars and weapons to construct a far more effective IAMD enterprise. IBCS delivers a single integrated air picture with unprecedented accuracy as well as broader surveillance and protection areas. With its truly open systems architecture, IBCS allows incorporation of current and future sensors and effectors and enables interoperability with joint C2 and the ballistic missile defense system.

IBCS is managed by the U.S. Army Program Executive Office for Missiles and Space, Redstone Arsenal, Alabama.

Dan Verwiel, VP and GM, missile defense and protective systems, Northrop Grumman, said this milestone is testament of the significant progress toward operational capability that will make pivotal differences to warfighters, commanders and acquisition officials.

The company will be delivering more EOCs as well as IBCS integrated fire control network (IFCN) relays in the near future. These articles will be used for initial operational test and evaluation (IOT&E), which informs future production decisions.

www.northropgrumman.com

25 YEARS
AvL TECHNOLOGIES
1994-2019

CONNECTING THE WORLD FOR 25 YEARS

NEW 2.2M ULTRALIGHT ANTENNA

- The most compact 2m class antenna on the market
- Comparable performance to competing 2.4m antennas with small pack-up
- High-stiffness ultra-lightweight carbon fiber reflector and positioner base
- Quad-band: Ku, Ka, X and C
- Intuitive coarse/fine Az/El positioning
- Simple feed polarization positioning
- Can be assembled and on-network in less than 25 minutes
- Packs into two checkable transit cases with each weighing less than 100 lbs.

AvL TECHNOLOGIES

avltech.com

Visit AvL at CommunicAsia Booth #1N1-01

DISPATCHES

Harris receives contract to strengthen GPS IIIF satellites' signals

Harris Corporation (NYSE: HRS) has received a $243 million contract from Lockheed Martin (NYSE:LMT) to provide fully digital navigation signals for the first two GPS III Follow-On (GPS IIIF) satellites to deliver stronger signals, with greater operational flexibility.

Harris' GPS IIIF fully-digital Mission Data Unit (MDU), the heart of the satellite's navigation payload which generates the GPS signals, will provide more powerful signals, assure flawless clock operations for GPS users, and add flexibility to adapt to advances in GPS technology, as well as future changes in mission needs.

It will provide improved capabilities over Harris' 70 percent digital MDU used for GPS III Space Vehicles 01-10 (GPS III SV01-10). The new MDU also offers the U.S. Air Force a smooth transition to its GPS OCX ground control segment. Harris will seamlessly port its digital signal design, minimizing both integration risks and associated costs.

In September of 2018, the U.S. Air Force (USAF) selected Lockheed Martin, with Harris as its navigation signal partner, to build up to 22 GPS IIIF satellites, with a total estimated contract value up to $7.2 billion. The USAF expects the first GPS IIIF satellite, SV11, to be available for launch in 2026.

Launched aboard GPS III SV01 in December 2018, Harris' first GPS III navigation payload began broadcasting navigation signals on January 8. While testing of the first-of-its-kind satellite continues, the payload has performed beyond expectations. Harris has provided navigation technology for every U.S. GPS satellite ever launched, enabling the reliable GPS signal that millions of people, including U.S. soldiers, and billions of dollars in commerce depend on every day.

www.harris.com

SecureSync from Orolia is approved by DISA

Orolia's SecureSync time and synchronization servers have been selected to support en route radar systems across the U.S.

The only Time and Synchronization Device approved by the Defense Information Systems Agency (DISA) for use in U.S. Government networks, SecureSync provides unparalleled reliability, security and flexibility to synchronize critical aviation operations.

The FAA employs a variety of radar types for short-, medium- and long-range air traffic control requirements.

These diverse radars require different types of timing signals and outputs to suit their operations. Orolia's SecureSync provides the necessary timing outputs and signals required for these radars.

The time server's outstanding ability to provide resilient, accurate and reliable timestamps for the data that it receives from radars is used to quickly organize the data for the aircraft control user interface.

Orolia was selected by the FAA for this competitive program based on its proven timing and synchronization technology, and its ability to offer multiple output options as COTS products that do not require additional research and development time or investment.

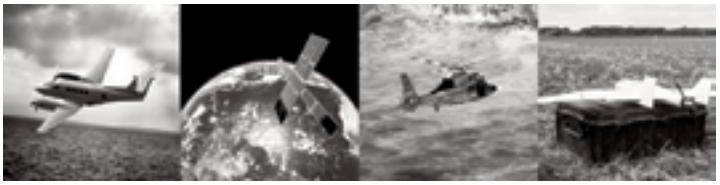
Only SecureSync combines multi-GPS/GNSS signal synchronization, options for alternative signals and BroadShield GPS anti-jamming/ spoofing protection for transportation systems.

Jean-Yves Courtois, CEO of Orolia, stated that consistently accurate timestamps and the synchronization of thousands of real-time flight data points are essential for safe and efficient en route air traffic operations. The company is proud to support the FAA's radar data and aircraft control user interface requirements to improve air travel services nationwide.

www.satnews.com/solutions/ aerospace/aviation-programs

DISPATCHES

From NATO to Horizon... two major orders for FlyingFish™



Horizon Technologies has announced two major NATO end user orders for the company's FlyingFish™ airborne SIGINT system totaling more than 14 million euros over the next few years.

John Beckner, CEO, Horizon Technologies, stated, that these orders are significant because they include new fixed and rotary wing platforms as well as new government end users.

He noted that the units were ordered for immediate delivery and will be used as part of NATO and FRONTEX missions.

The firm's FlyingFish product line continues to be improved and now monitors three satellite networks. Horizon Technologies offers exportable DO-160G airborne-qualified SatPhone SIGINT systems for a wide variety of fixed and rotary-wing aircraft.

In addition, the company's new remote control software allows for seamless integration into airborne tactical management systems as well as enhanced debrief and exploitation capabilities.

Beckner continued that Horizon Technologies is especially grateful for the strong support provided by the UK Government and in particular the Department of International Trade.

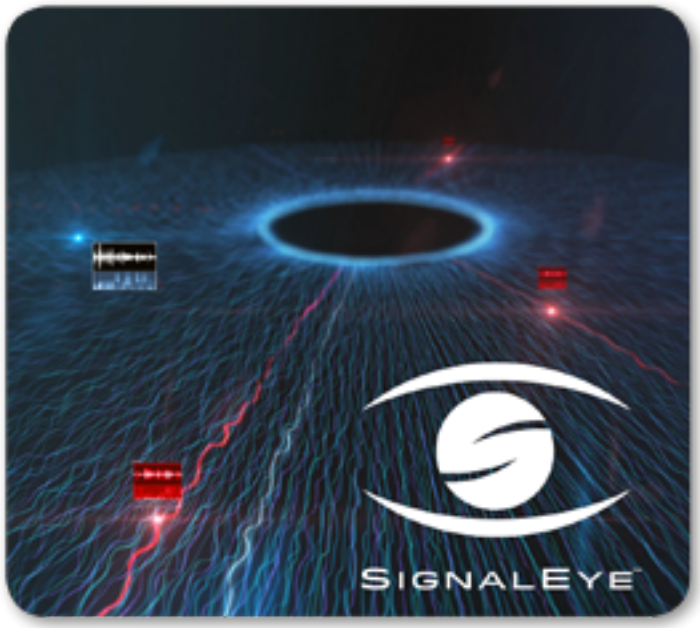
He added that the firm's business is growing faster than ever and is expanding into new areas, such as space with the firm's Amber SIGINT smallsat constellation bringing FlyingFish capabilities to customers as a data service starting in 2020.

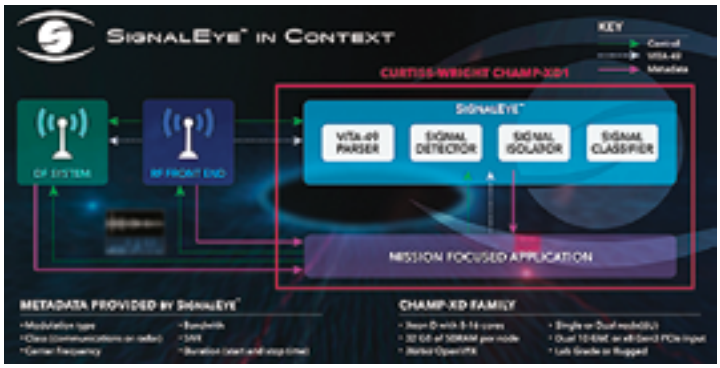
The Horizon Technologies quality management system has been certified by the British Standards Institution (BSI) to EN 9100:2018.

www.horizontechnologies.eu

DISPATCHES

Collaboration between Curtiss-Wright and General Dynamics for EW situational awareness applications





Curtiss-Wright's Defense Solutions division is collaborating with General Dynamics Mission Systems to deliver open architecture artificial intelligence (AI) based Commercial-Off-The-Shelf (COTS) solutions for Signal Intelligence (SIGINT) and electronic warfare (EW) situational awareness applications.

The combination of **General Dynamics Mission Systems**' ***SignalEye*** threat detection software and **Curtiss-Wright**'s Intel® Xeon® D processor-based CHAMP-XD1 module (*image below)* provides system designers with a deployable COTS solution for RF spectrum situational awareness that automatically classifies signals through the use of machine learning.

The 3U OpenVPX™ CHAMP-XD1 is a rugged digital signal processor (DSP) engine module designed for use in computer-intensive defense, aerospace and applications.

The technology enables developers of High Performance Embedded Computing (*HPEC*) systems to take full advantage of the unmatched performance of today's leading-edge Xeon D processor architecture.

The 3U VPX processor card is available in a range of ruggedized configurations to deliver optimal performance in the harshest deployed environments, including air-cooled and conduction cooled variants.

General Dynamics SignalEye™ solution provides spectrum situational awareness by automating the classification of signals through the use of machine learning.

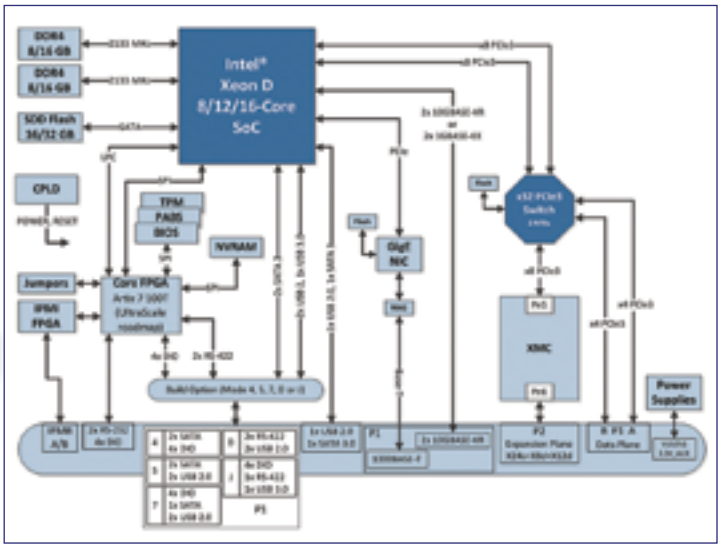
This electronic warfare software provides tactical warfighters and security personnel with a timely, accurate view of the threat in the RF spectrum.

SignalEye is always on — learning and alerting you to the signals that threaten missions. With SignalEye, the user will know what is normal and what is a threat at the speed a mission requires.

"*We are excited to collaborate with General Dynamics Mission Systems to bring the cutting-edge advantages of machine learning to deployed EW situational awareness applications*," said ***Lynn Bamford***, Senior Vice President and General Manager, Defense Solutions division. "*Our supercomputing class CHAMP-XD1 module is an ideal processor for SignalEye software, easing and accelerating the delivery of RF threat detection to our warfighters.*"

"*The evolving EW and SIGINT threat confronting warfighters today requires an integrated solution*," said ***Bill Ross***, Vice President, RF and Broadband Products at General Dynamics Mission Systems. "*By combining our SignalEye machine learning software with Curtiss-Wright's CHAMP-XD1 processor, we can provide warfighters with a greater understanding of the RF threats on the battlefield.*"

www.curtisswrightds.com



DISPATCHES

Northrop Grumman completes rapid smallsat development demo in record time for DARPA

Northrop Grumman Corporation (NYSE: NOC) successfully demonstrated rapid spacecraft development for the Defense Advanced Research Project Agency (DARPA), with the Radio Frequency Risk Reduction Deployment Demonstration (R3D2), which launched on March 28, 2019.

Northrop Grumman led a unique team of commercial suppliers to deliver a 150 kg. smallsat from concept to orbit in 20 months. Traditional satellites of comparable complexity typically take many years to get to this stage.

The significantly accelerated timeline of R3D2 was enabled by DARPA's approach of reducing requirements, reviews, and deliverables, while accepting greater levels of risk than is typical for an operational system.

Northrop Grumman used innovative rapid-development processes and commercial suppliers to keep schedule and risk balanced.

The Northrop Grumman-led team, included Blue Canyon Technologies, provider of the spacecraft bus, and Trident Systems, who designed and built R3D2's software-defined radio. R3D2 was launched from the Mahia Peninsula in New Zealand by Rocket Lab.

Scott Stapp, VP, resiliency and rapid prototyping, said the company's team's success with the R3D2 program is a strong proof of concept that the rapid development of future space capabilities is possible.

He noted that Northrop Grumman looks forward to continuing to lead the cultural change necessary in the industry, by partnering with the U.S. government, commercial suppliers and startups to deliver prototypes and demonstrations for critical national security missions. Taking thoughtful risks and eliminating bureaucracy allowed us to streamline our processes to achieve rapid timelines.

www.northropgrumman.com

DISPATCHES

Department of Homeland Security awards contract to expand cyber-training platform

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has awarded a total of $5,900,000 to the *Norwich University Applied Research Institutes* (NUARI) to expand the Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE) cyber-training platform.

DECIDE was originally developed in tandem with and transitioned to the financial services sector; this new effort will build similar simulation-based scenarios and exercises specific to the energy sector.

DECIDE allows users to conduct collaborative, realistic, fully immersive, scenario-based exercises where the consequences of each participant's actions feed back into the exercise.

The exercises are designed to help trainees understand the systemic ramifications of their actions and improve communication during potential high-stress threat events.

S&T's cybersecurity mission is to enhance the security and resilience of the nation's critical information infrastructure and the internet by developing and delivering new technologies, tools, and techniques to defend against cyberattacks.

S&T conducts and supports technology transitions and leads and coordinates R&D among the R&D community, which includes DHS customers, government agencies, the private sector and international partners.

"*DHS S&T is committed to investing in the security of our nation's critical infrastructure, and that includes ensuring that organizations are properly trained to recognize and respond to potential cyber threats*," said *William N. Bryan*, Senior Official Performing the Duties of the Under Secretary for Science and Technology.

He added, "*We are excited to soon make this proven platform available to even more of our private sector partners.*"

"*Bringing players together in a safe, immersive environment where they can run through existing response tactics allows them to identify vulnerabilities and develop mitigation strategies prior to a real-life crisis*," said *Greg Wigton*, S&T program manager.

He noted, "*DECIDE offers organizations seeking to bolster their cyber strategies a low-risk, high-value tool, and we look forward to working with NUARI and our energy stakeholders to customize the technology to their unique needs.*"

https://www.dhs.gov/science-and-technology/decide

Orbit Communications has unveiled their new airborne terminal

Orbit Communication Systems Ltd. (TASE: ORBI) has unveiled their new MPT 87 Airborne Terminal.

This advanced, MIL-STD qualified terminal initially features a high gain 87 cm. (34-inch) hybrid, Ku-band antenna, with a Ka-band configuration in development.

The antenna will operate across the full Ku-band and can be easily switched in real-time between different operators and satellites.

The MPT 87 is the latest addition to the innovative MPT terminal family and is planned for initial service operation later this year.

Like all other MPT versions, the MPT 87 will be delivered fully integrated with RF and control electronics, and associated software.

The lightweight, small-footprint terminal couples high performance and reliability.

The MPT modular approach facilitates its adaptation to different aircraft and platforms.

Orbit Communications MPT™ 30-90 Military Airborne Stabilized VSAT Systems.

Brian added that the underlying MPT architecture and engineering has allowed them to again expand and tailor their airborne terminal family in a timely and cost-effective manner.

orbit-cs-usa.com/

UAV image is courtesy of NASA.

This allows the antenna to address new opportunities and help grow emerging aeronautical communications markets.

Ben Weinberger, Orbit's CEO, noted that following the company's recent announcements of new maritime and airborne SATCOM terminals, developed in coordination with two of the largest satellite operators (SES and Inmarsat), this high-speed terminal fulfills key requirements for one of the leading defense segment customers.


The advantages of
Advantech Wireless
Technologies
are clear
Deployments in over 150 countries
New state-of-the-art research and manufacturing facility
Broadest SATCOM RF product portfolio in the industry
Part of the Baylin Technologies Group of Companies
ADVANTECH
Wireless Technologies
Solid State Power Amplifiers
Satellite Frequency Converters
Satellite Antennas
Radar GaN Amplifiers
Terrestrial Microwave Radios
advantechwireless.com

ENHANCING TRANSMISSION SECURITY

Protecting critical communications

by Karl Fuchs, Senior Vice President of Technology, iDirect Government, and Senior Columnist

The need to protect the flow of communications to wherever the military and government agencies may operate is critical. Wherever this may be, threat actors readily stand by to monitor, exploit or intercept communications with malicious intent.

Thankfully, Transmission Security (*TRANSEC*) technology and capabilities are available in the marketplace to mitigate this threat. **iDirect Government**'s (**iDirectGov**'s) ***Evolution*** software is one example with TRANSEC capabilities, and with the release of ***Evolution 4.2***, the company has further enhanced those abilities by extending protection to cover both one-way and two-way networks.

In combatant situations, where even a small "spike" in traffic can be a critical piece of intelligence, the need to mask any communications activity becomes apparent. The National Security Agency (*NSA*) has outlined the following vulnerabilities inherent in an IP-based Time Division Multiple Access (*TDMA*) transmission that must be addressed in order to provide true TRANSEC:

- *Channel Activity — The ability to secure transmission energy to conceal traffic volumes.*
- *Control Channel Information — Disguise traffic volumes to secure traffic source and destination.*
- *Hub and Remote Unit Validation — Ensure remote terminals connected to the network are authorized users.*

TRANSEC requires all network control channels and Management & Control (*M&C*) data to be encrypted, and that any and all traffic engineering information be obfuscated from an adversary. For example, TRANSEC requires a communications channel to appear completely full to an adversary, even if little or no actual data is flowing.

Contrast this with communications security (*COMSEC*). With COMSEC, the actual communication (*e.g.*, voice, video or data stream) is encrypted, but certain header information is sent in the clear. While the encryption is virtually impenetrable, the information in the IP header including the source address, destination address and, most importantly, the type of service (ToS) field are visible to the enemy if they are intercepted. This gives the adversary critical information and the ability to determine how much of the traffic stream is voice, video or data. More significantly, an adversary could easily see when high-priority flash-override traffic has been initiated and from which location.

In a traditional *SCPC* (*single channel per carrier*) satellite network topology, achieving TRANSEC compliance is relatively straightforward. For SCPC connections, a bulk encryptor is employed to decipher any data and control information traversing the network. The IP header of the packet would be encrypted by the bulk encryptor before being transmitted to the satellite. In addition, since an SCPC link is static, always on and no control information needs to be exchanged between the SCPC modems, all TRANSEC requirements are met.

In a TDMA network, TRANSEC compliance is more difficult. A TDMA network dynamically allocates bandwidth to remotes; therefore, there must be some type of control information transmitted to each device in the network. This control data containing traffic engineering information, as well as information available from an encrypted IP packet header, can be exploited by an adversary. For example, anomalous traffic volume to a specific remote can indicate new activity in that area while varying ratios of voice-to-data traffic can denote the distribution of intelligence (data) compared to lower priority voice traffic.

While there are several solutions to secure vulnerabilities associated with TDMA very small aperture terminal (VSAT) networks, iDirectGov has found solutions to the following scenarios to be the most successful.

Scenario 1
Masking Channel Activity

The first vulnerability that exists in a TDMA network is the availability of traffic engineering information. In an SCPC network, the link is static with no variation in transmission characteristics based on end user communications. An adversary looking at a satellite transponder with a spectrum analyzer will see a constant RF signal.

Contrast this with a TDMA network. A TDMA in-route carrier energizes and de-energizes as traffic flows and stops. The on-and-off nature of a TDMA in-route is the natural extension of the ability to allocate satellite transponder space to remotes that have transient demands.

Although this characteristic makes TDMA networks much more bandwidth efficient, it allows an adversary to determine peak periods of activity, identify unusual or unexpected activity spikes and identify locations of remotes that have remained quiet for a period and suddenly experience increased traffic volumes. The obvious risk in having this information in the hands of an adversary is the potential to extrapolate timing, location and scale of a strategic activity.

To keep critical information from falling into the enemy's hands, iDirectGov has implemented free slot allocation in its TDMA bandwidth distribution algorithm. This method basically builds a wall of data keeping adversaries from getting critical data regardless of traffic profiles. As the name implies, free slot allocation keeps the in-routes active despite actual traffic flows. It preserves the efficiencies of a TDMA system while obfuscating actual traffic volumes, negating the risk of using transmission activity as an intelligence gathering mechanism.

Scenario 2
Obfuscating Acquisition Activity

The rate at which remotes get into a network can give critical information to an adversary about troop activities. All TDMA networks provide a dedicated channel for remote acquisition activity. If adversaries monitor the activity in this channel, they will be alerted to troop movements by a flurry of acquisition activity.

To counter this problem, iDirectGov goes beyond TRANSEC requirements by addressing the acquisition activity vulnerability. This acquisition algorithm inserts dummy bursts from remotes already in the network and intentionally skips acquisition bursts at times of high activity, ensuring an adversary sees only a random distribution of acquisition activity.

Taking it a step further, the algorithm randomly varies the dummy burst's frequency, timing and power. This randomization makes sure an adversary cannot distinguish between a dummy burst and actual acquisition activity.

Scenario 3
Control Channel Information

A great deal of traffic volume and priority information can be gleaned by examining the in-band or out-of-band control information within an encrypted TDMA network.

As previously discussed, the IP header of a packet contains source, destination and priority information. For a TDMA network to provide the **quality of service** (*QoS*) needed to support real-time traffic, data quantities and prioritization information must be gathered. Because it is specific enough to delineate between general communications such as email and web traffic versus tactical communications, this information could be more useful to an adversary than channel activity data.

The only solution available for this vulnerability is to completely encrypt all Layer 2 information plus any control information disseminated to the remotes. The encryption methodology must be secure enough to thwart an adversary long enough that the data becomes old and unusable.

Once again, iDirectGov has implemented **Federal Information Processing Standard** (*FIPS*) 140-2 certified 256-bit keyed **Advanced Encryption Standard** (*AES*) for all Layer 2 and control information. The encryption of the Layer 2 frames has a side benefit of re-encrypting the data payload. Therefore, the transmitted IP header itself is AES-encrypted. Additionally, the iDirectGov TRANSEC TDMA slot is a fixed size, again to obfuscate any traffic characteristics. This Layer 2 encryption solution solves all existing control channel vulnerabilities.

The iDirectGov Layer 2 encryption method goes a step beyond to feature **over-the-air** (*OTA*) key updates and a unique Layer 2 frame format, including an Initialization Vector that ensures randomization of repetitive data streams. The net result is that adversaries are precluded from detecting any repetitive pattern, which can aid in deciphering encryption algorithms.

Scenario 4
Hub and Remote Authentication

Another vulnerability of a TDMA VSAT system is the concept of hub and remote validation. In traditional SCPC architectures, a link remains active for very long periods of time when it is established. Because these connections are fixed and there is a significant level of coordination between personnel commissioning the SCPC, a high degree of confidence exists that an adversary is not trying to assume the identity of a trusted entity.

In TDMA networks, remotes are routinely coming into and dropping out of the network. This is especially true of networks with mobile or itinerant terminals where terminals are located in moving vehicles, aircraft and maritime vessels.

This type of dynamic environment gives an adversary a greater opportunity to obtain a VSAT remote through licit or illicit channels, spoof the device ID and insert a rogue remote into a secure network. Equally feasible is an adversary acquiring a VSAT hub terminal and coaxing a "blue force" remote into the adversary's network.

To mitigate this risk, iDirectGov has implemented **X.509** digital certificates on TRANSEC remotes. An X.509 certificate uses RSA public key cryptosystem. With this cryptosystem, two related keys are generated: One private key and one public key. Here's how the keys work — anything encrypted with the public key can only be decrypted with the private key, and anything encrypted with the private key can only be decrypted with the public key.

In the iDirectGov system, X.509 certificates can be generated via the network management system (NMS) server. Certificates are placed on all TRANSEC line cards and protocol processors as well as on the remotes. The hub system keeps the public keys of each remote configured to operate on the hub, and the remotes have the public keys of each hub device. During network acquisition, the remote encrypts its X.509 certificate with its private key, and the hub verifies by decrypting the certificate with the remote's public key and vice versa. This process ensures a remote is not only authorized to operate in the network, but that the hub is a trusted entity

Scenario 5 Operational Implementation

Implementing security and ensuring all security policies are followed can be a burden to the soldier in the field. Implementing TRANSEC and performing key management are no exception.

Challenges faced in operating a TRANSEC network include creation, distribution and revocation of X.509 certificates; ACQ and data channel key generation, distribution and management; and zeroizing modems.

A robust TRANSEC network also requires the use of at least two network-wide keys: The ACC key for acquisition, and the DCC key for the data channel. A long-lived, user-generated passphrase is used to protect the keys during initial commissioning. The use of front-panel displays to enter the passphrase and external key fill mechanisms places an undue burden on the warfighter and introduces security vulnerabilities.

iDirectGov has implemented a FIPS-approved software method of key generation and automatic, OTA key distribution protocol. Not only does the software-based key generation and key distribution mechanism make TRANSEC operation simpler and more convenient for the warfighter, it makes the system much more secure by removing a human from key distribution.

Another advantage of automatic key generation and distribution is that it seamlessly enables a global **Communications-On-The-Move** (*COTM*) TRANSEC network. By automatically generating and distributing new acquisition passphrases, a single, dynamic passphrase can be used across global networks.

Enhancing TRANSEC and Security with the 9-Series and DLCs

iDirectGov has expanded its existing FIPS 140-2 certification from Level 2 to Level 3 in its ***9-Series Satellite Routers and Defense Line Cards***, as opposed to FIPS 140-2 Level 2 in its ***8-Series*** products and ***eMxDx*** line cards.

As part of the effort, iDirectGov developed a TRANSEC module designed to meet the stringent FIPS 140-2 Level 3 requirements as defined by the **National Institute of Standards and Technology**. Through hardware and software development, the embedded yet independent TRANSEC module on the 9-Series and DLCs operates through a separate and trusted path from all other interfaces on the product.

The module also features a strong physical security measure for tamper prevention and the capability to zeroize the security keys or **critical security parameters** (*CSPs*) stored on the module itself. If required, the revocation or zeroization of the keys can be accomplished either OTA by the hub operator or locally on the remote by authorized personnel.

One-Way Networks

iDirectGov has further enhanced its TRANSEC capabilities by securing one-way broadcast transmissions. Based on its encapsulation method, **lightweight encapsulation generic stream** (*LEGS*), the iDirectGov platform can provide the same level of security for one-way networks to that of two-way networks as described earlier.

The 900 and 9350, with dual-demodulator support, are capable of dual-domain TRANSEC; the ability to establish two independent chains of trust (sets of X.509s) between two different certificate authorities (CA).

An example use case of this feature would be one demodulator on a two-way TRANSEC network while the second demodulator receives a separate one-way TRANSEC-secured broadcast. **Elliptical Curve Cryptography** (*ECC*) is used for key generation along with X.509 certificates for authentication in each security domain.

www.idirectgov.com/

Karl Fuchs is Senior Vice President of Technology of iDirect Government (iDirectGov). Fuchs joined iDirectGov in 2004 as the director of sales engineering, just as the satellite-based IP communications company was expanding its very small aperture satellite (VSAT) market presence into the federal government and international Internet Protocol (IP) networking world. With more than 20 years of experience in technology and with the federal government, Fuchs leads iDirect Government's team of federal systems engineers and serves as chief architect for new product integration. Active in the satellite industry for more than 15 years, Fuchs has contributed editorial to publications including Federal Computer Week, Institute for Defense and Government Advancement, COTS Journal, Military Information Technology, Via Satellite, MILSATMagazine and Satellite Evolution Global. He is also a senior contributor to MilsatMagazine. Fuchs holds a Bachelor of Science degree in electrical engineering from George Mason University, Fairfax, Virginia, and an MBA from Averett University, Danville, Virginia.

Introducing the

WALTON DE-ICE

Portable Radome

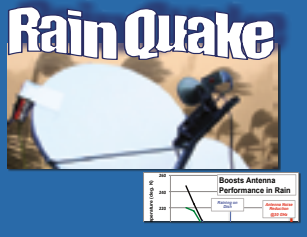
Unleash new SATCOMS capabilities in extreme conditions

NOW AVAILABLE
Call for details!

Whether the mission demands staying on-air in a 85 mile-per-hour (136 kph) wind storm, a sandstorm, a blizzard, hail, or torrential rains – the **Portable Radome** helps make satellite networks more survivable and deployable into extreme or harsh environments. Gain significant cost saving vs. conventional radomes for military or civilian networks.

The industy's most powerful, cost-effective De-Icing. For antennas from 3.7 to 32 meters.

Sheds off snow before ice forms. Huge — up to 100 X — energy savings compared to conventional systems. 0.6 to 6.3 meters.



Minimize Signal Loss due to Rain Fade. Reduce data loss — by 20X or more.

Meet at SOFIC May 20 – 23 Tampa, FL

Call Ray Powers at 1.951.683.0930 or email Ray@de-ice.com

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

WB Walton Enterprises, Inc. P.O. Box 9010 San Bernardino, CA 92427 USA

THE SPACE SYMPOSIUM

Realizing the urgency and prioritization of space programs

By Wendy Lewis, Contributing Editor

With speakers from the highest government offices, including two members of the President's cabinet, the 35th Space Symposium, which took place in Colorado Springs from April 8 through 11, attracted roughly 9,000 people from around the world.

The 60,000 square foot International Center at the **Broadmoor** hotel was filled to capacity with attendees who wanted to hear from luminaries such as Acting Defense Secretary ***Patrick Shanahan***, Secretary of Commerce ***Wilbur Ross***, Secretary of the U.S. Air Force (USAF) ***Heather Wilson***, and NASA Administrator ***Jim Bridenstine***.

Key themes across the numerous, well-attended conference sessions included:

- *The urgency of prioritizing space and accelerating programs*
- *The importance of international partnerships to achieving goals*
- *The desire for the U.S. government to collaborate with commercial industry*

Acting Defense Secretary Patrick Shanahan was the opening speaker at the four-day event. He was surprisingly outspoken about the current threats facing the nation and said that China and Russia have weaponized space with laser systems to target Low Earth Orbit (*LEO*) spacecraft as well as hypersonic weaponry, which the U.S. is not currently capable of tracking.

Other speakers concurred, saying that slow and meticulous development of space assets has been the status quo for many years; however, with the recognition that space is now a contested environment, the U.S. government must focus on making space a priority.

Shanahan noted that despite its importance, USAF General ***John Hyten***, the Commander of the **U.S. Strategic Command,** cannot keep a constant focus on space issues.

According to the General Hyten and Shanahan, this was acceptable in the days when space was a peaceful domain.

In a private briefing, General Hyten reiterated that space was his third priority, at best. Despite his love of space, he said that nuclear and nuclear command and control demand most of his attention and must come first.

He stated that we need a commander with a focus on space all the time, and he lauded the nomination of General ***Jay Raymond*** to lead the new **Space Force**.

Shanahan said that having a dedicated branch of the military to focus on space will be a significant deterrent to the nation's adversaries. He explained that as a sixth branch of the armed forces, the Space Force would defend the U.S. in space, just as the U.S. Navy is focused on battles at sea, the USAF on aircraft warfare and the Army on ground forces.

He believes that a strong U.S. Space Force will protect the domain and promote the new space economy.

Conference sessions at the International Center were well-attended

General Hyten met with the press to answer questions at the Space Symposium

General Hyten discussed the need to move quickly, as did Heather Wilson in her address. Hyten said that fear of risk has caused the buildup of a big bureaucracy, which was acceptable when space was a benign environment.

To move faster, he suggested that the USAF needs to learn to take on more risk and to delegate down without every decision being reviewed at the highest levels.

He referenced **Apollo 1**, both in a press briefing and later at the Space Symposium's **Corporate Partnership Dinner**, where he was the featured speaker.

He said that after the failure of Apollo 1, there were many in favor of abandoning the Apollo program altogether. However, understanding the risk and moving forward anyway prevailed, in part due to the support of international partners.

The Honorable Heather Wilson, Secretary of the U.S. Air Force.

Heather Wilson drew a standing ovation following her address in the general session.

She said that it is essential to build and deploy faster — under her management, the USAF has stripped away 100 years of bureaucracy from the acquisition process.

She said the USAF is removing the barriers to entry for small and innovative companies and she specifically mentioned companies such as **SEAKR Engineering**, **Millennium Space Systems** and **Blue Canyon**.

She said Millennium is on schedule to deliver a constellation of smallsats in GEO just one year after the contract was awarded.

In response to the attention that smallsats are currently garnering, Wilson quoted ***H. L. Mencken***, saying, "*For every complex problem there is an answer that is clear, simple and wrong.*"

She explained that hundreds of inexpensive satellites will not provide enough options for all of the varying phases of conflict.

"*Different missions will require different solutions. One size does not fit all. Increasing the numbers of satellites helps, but numbers alone are not enough... Space missions that are not well aligned with commercial Low Earth Orbit satellites are better off staying where they are*," she said.

General Hyten also highlighted the need for a mix of different orbits, each with differing benefits. He advocated for a complex architecture that ensures that it is too difficult for adversaries to deny service.

Increased Funding

Nearly all of the key speakers advocated for increased funding for space programs. Wilson said that the USAF budget for unclassified programs is $13.7 billion for 2019.

This is an increase of 17 percent over the 2018 budget, which was greater than the 2017 budget.

In his address, NASA Administrator Bridenstine discussed the acceleration of the mission to return humans to the moon, including the world's first woman to walk on the surface of the moon.

Originally planned for 2028, Vice President ***Mike Pence*** challenged NASA to move the mission up to 2024.

As a result, Bridenstine said that NASA is going back to congress with an increased budget request and his talk included a plea for bi-partisan support to meet the aggressive deadlines.

NASA Administrator Jim Bridenstine discussed the acceleration of the mission to return to the moon.

General ***David L. Goldfein***, Chief of Staff, USAF, brought humor and humanity to his speech, starting with a tribute to Lieutenant Colonel ***Dick Cole***, a World War II airman who flew a heroic mission known at the Doolittle Raid and had just passed away at age 103.

Reinforcing the need to invest in space infrastructure, the USAF Chief of Staff gave a heartfelt testament to the nation's goals.

"We're the best in the world in space, but our adversaries know it. As acting secretary Shanahan properly stated, since desert Storm they've studied our ways, and invested in means to deny us access to space capabilities in crisis or conflict.

"Our job is to never let that happen so we can maintain space as a peaceful domain where common interests can align and flourish."

USAF General David Goldfein was passionate about working together with our allies in space.

He also addressed the importance of how space has become a place for commercial profit and competition, which is energizing industry, and he talked about working together with allies.

Driving home the importance of the work the USAF does in space, he said, "*We have to protect and defend what we have in space because it's going to be there for a while and we all depend on it. We must harden our networks, build resilience in our systems, enhance existing capabilities as we improve information sharing in areas like satellite communications, and missile warning.*"
USAF General David Goldfein was passionate about working together with our allies in space

He was heartfelt in his passion for the responsible, peaceful and open use of space for all and said, "*We do this by creating military capabilities that underwrite deterrents, preventing war from extending to space. Just as we continue our work to do so, in the air, at sea, and in the cyber domains, the global commons. Because historically, those with allies win. And America's greatest strength has always been its ability to attract partners with common interests.*"

Article photos are courtesy of Wendy Lewis.

Wendy Lewis lead external communications for Space Systems Loral for 12+ years and has a deep understanding of how satellites connect, protect and inform the world. She is a contributing editor to Satnews Publishers, MilsatMagazine and SatMagazine and is the principal of Strategic Voice, a company that develops and executes strategic communications programs that drive awareness and engagement in support of business objectives.

The 36th Space Symposium will be in session at the Broadmoor, Colorado Springs, Colorado, and will be held from
March 30 - April 2, 2020

www.spacefoundation.org/events/space-symposium

SMi Group proudly presents...

SMi
LINKING BUSINESS *with* INFORMATION

Military Space USA

11th – 12th JUNE 2019

Providing a Holistic View of the US Space Enterprise

THE RENAISSANCE HOTEL, LOS ANGELES, USA

CONFERENCE CHAIRS:

Colonel Russell Teehan, Portfolio Architect, SMC, AFSPC, **US Air Force**

Mr. Jay Santee, Vice President, Strategic Space Operations, **The Aerospace Corporation**

SMC SPEAKERS INCLUDE:

Lieutenant General John Thompson, Commander, Space and Missile Systems Center, **US Air Force***

Mr Joseph Vanderpoorten, Chief, Advanced Concepts Division, Space and Missile Systems Center, MILSATCOM/Advanced Concepts, **US Air Force**

Lieutenant Colonel Gary Thompson, Chief, Future Concepts Team, Space and Missile Systems Center, **US Air Force**

SPEAKERS INCLUDE:

Major General Stephen Whiting, Commander, 14th Air Force and Deputy Joint Space Component Commander, **US Air Force**

Colonel Nickolas Kioutas, PM - Positioning, Navigation, and Timing, PEO IEW&S, **US Army**

Captain Michael Mattis, Space Lead Commander, Third Fleet, **US Navy**

Colonel Patrick Williams, Commander, 2nd Weather Group, 557th Weather Wing, **US Air Force**

Colonel Jeremy Raley, Chief Integrated Experiments and Evaluation Division, Space Vehicles Directorate, AFRL, **US Air Force**

Colonel Jack Fischer, Vice Commander, 50th Space Wing, **US Air Force**

Colonel Kapil Jaiswal, Director, Directorate of System Applications, Directorate General of Signals, **Indian Armed Forces**

Lieutenant Colonel Yun Kyong Sung, C4I Interoperability Officer, J6, **ROK JCS**

Dr Michael J Starks, Space Environment Mission Lead, Space Vehicles Directorate, Air Force Research Laboratory, **US Air Force**

Dr Jaime Stearns, Space Control Mission Lead, Space Vehicles Directorate, Air Force Research Laboratory, **US Air Force**

Mr Arlen Biersgreen, Space Systems Engineer, AFRL Sensors Directorate, **US Air Force**

Mr Richard Cobb, Professor of Aerospace Engineering, Department of Aeronautics and Astronautics, **US Air Force Institute of Technology**

Ms Demaryl Singleton, Infrastructure and Development Division Chief, **DISA**

Dr Grant Stokes, Head of the Space and Technology Division, **MIT Lincoln Laboratory**

Ms Andrea Loper, Acquisition Program Manager, Space Vehicles Directorate, Integrated Experiments & Evaluation Division, AFRL, **US Air Force**

INDUSTRY SPEAKERS:

Senior Representative, Lockheed Martin

Dr Douglas Hendrix, CEO, **ExoAnalytic Solutions**

Dr Natalya Bailey, CEO and Co-Founder, **Accion Systems**

Mr Lars Hoffman, SVP Launch, **Rocket Lab**

Mr. Mike Lewis, Chief Innovation Officer, **NanoRacks**

Mr Kevin Coggins, Vice President, VP, Resilient PNT Platform Systems, SIG/Cyber & Engineering, **Booz Allen Hamilton**

* Subject to Final Confirmation

KEY REASONS TO ATTEND:

- Listen to key updates on how **procurement** and requirements setting for US space acquisition is **being reformed through SMC 2.0** and how delivering at epic speed is set to change the industry landscape
- Explore how **industry disruptors** and incubating vendors – are delivering the new 'agile space' sector **within the Silicon Valley & internationally**
- Build partnerships with key representation from across the **APAC region**
- Develop a comprehensive understanding of how the US Space Enterprise is developing across mission areas including **SSA, PNT, SATCOM and more!**

GOLD SPONSORS

LOCKHEED MARTIN

ExoAnalytic SOLUTIONS

SPONSORS AND EXHIBITORS

HUGHES An EchoStar Company

OFFICINA STELLARE

XTAR Satellite Communications

www.milspaceusa.com/MilSatMagazine

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

CPD CERTIFIED

@smigroupdefence
#MilSpaceUSA

SUPPORTING GLOBAL HUMANITARIAN EFFORTS

Saving lives with SATCOM

By Gwenael Loheac, Group Chief Operations Officer, IEC Telecom

Displaced, disorientated, on the brink of death — when faced with a humanitarian crisis, many of us would be unable to cope with the magnitude of the operational tasks needed to help when disaster strikes.

Not so for the world's international aid agencies who leap into action and put into place their well-established plans and procedures.

IEC Telecom's satellite communication solutions are at the heart of these activities. Thanks to the company's 24-hour service and globally responsive capabilities, IEC Telecom can activate hundreds of satellite phone SIM cards within two hours, while urgently dispatching stocks of handsets, modems and hardware to aid agency teams loading planes ready to fly out to disaster zones.

Satellite communications (SATCOM) are a central necessity for disaster management strategies, helping aid workers in the field to communicate as they establish the infrastructure needed to undertake recovery operations, rescue hundreds of victims or accommodate thousands of refugees.

This is a logistically challenging and exhausting, but ultimately fulfilling, role. "*We are proud to work with many international aid agencies, NGOs and governmental organizations throughout the world,*" said ***Gwenael Loheac***, Managing Director of IEC Telecom. "*We understand that they are working in difficult conditions, we know how hard they work and the levels they go to in order to help devastated people, and we believe we are privileged to be part of this global sector. It's a special business to be able to help people who are undergoing very difficult situations in hostile conditions.*

Using IEC Telecoms solutions, aid workers are able to establish offices in the field, however remote or challenging their location may be. Using the best SATCOM solutions available enables those field locations to operate at levels on a par with regular offices, meaning data can be transferred at high speed allowing for real-time conversations and discussions.

Large bandwidth facilities, which IEC Telecom provides via L-band modem services using all the leading satellite provisions from companies such as Inmarsat, Iridium and Thuraya or VSAT super modem services using C-, Ku- or Ka-band, allow for the transfer of data and communication via email, telephone, social media platforms, etc.

Pictured below is the Akcakale Tent Camp in southeastern Turkey.
Approximately 28,000 Syrian people reside in Akcakale Tent Camp in Urfa. Syrians started to take refuge in Turkey in April 2011. The first camp was established in Yayladağı-Hatay on May 1, 2015.

High speed file transfer including large file formats such as video footage allows for services such as telemedicine to be used in actual time, helping to save more lives.

Field operations are supported by IEC Telecom's 24/7 global technical helpline services which are available all year round. Following competitive tendering processes, the company provides its services on an optimization system, ensuring high levels of provisioning for its customers.

Careful registration of allocated SIM cards means that activation can be achieved at the click of a button in rapid time — sometimes as quickly as 10 minutes — and in large volume when needed.

Need is growing, as well — as data capabilities increase, so does the range of uses for SATCOM. "*Ten years ago the majority of business was mostly voice calls*," explained Mr Loheac, "*Today, data transmission accounts for the biggest use and we see this growing at a fast rate.*"

It's not just aid workers who can benefit from telecommunications provision —– millions of refugees around the world are able to stay in touch with the outside world using satellite phones — often using a voucher system to access airtime.

In many parts of the world, there are long-established refugee camps which are the size of small cities. The average sized camp houses more than 11,400 people. With the average stay amounting to around 15 years, many youngsters are born and raised in refugee camps. Satellite communications benefit education by enabling online e-learning tools to be used or providing access to broadcast learning resources.

The United Nations refugee Agency (*UNHCR*) reports that the world is witnessing the highest levels of displacement on record. An unprecedented 68.5 million people around the world have been forced from home, among them nearly 25.4 million refugees, more than half of whom are under the age of 18.

Mr. Loheac noted, "*A refugee camp is in many senses an artificial environment. Satellite communications can provide a window to a wider world, enabling access to social media, online resources and communication with friends and family.*"

As the need for satellite communications grows within the humanitarian sector, IEC Telecom is at the forefront of progress. Having its own in-house engineering team, IEC Telecom is able to develop innovative solutions, both to meet customer's unique requirements and to anticipate future demands.

For example, IEC Telecom recently signed an agreement with **Iridium** to become a commercial partner to supply the ***MissionLINK***™ by **Thales** — a state-of-the-art product which enables instant and critical operation global communications coverage regardless of the landscape — particularly valuable in remote areas.

MissionLINK meets unique challenges through a simple, adaptable and robust design which comes with an intuitive, user-friendly interface and can be quickly integrated into vehicles. Also included is a built-in upgradeability to extend the life of this investment and to ensure peak speed and performance.

IEC Telecom Group has been providing communications solutions to aid workers for more than 20 years. The company offers a broad range of products and humanitarian solutions that are highly suited to the emergency phase following any disaster or crisis: satellite phones, mobile devices to deploy WiFi connectivity / "***Bring Your Own Device***" or portable and fixed modems.

Instant communications in the field are achieved thanks to lightweight and compact equipment, providing workers with enhanced mobility and shorter reaction times during a crisis first response phase.

Once the disaster recovery phase is entered, IEC's telecommunications systems assist aid agencies to consolidate their relief efforts over time, establishing temporary offices using semi-fixed modems such as **Inmarsat** ***BGAN*** range or ***Thuraya IP+*** to enable them to access corporate applications, manage logistics or even use low bandwidth videoconferencing solutions.

Multiple team members can share the same WiFi connection, establish a temporary office as well as benefit from prepaid vouchers for voice communications to stay in touch with their friends and family while being in the field.

For longer term deployments and sustainable development missions, IEC Telecom Group can meet any specific needs and offers high broadband data connectivity for teams to access and share high data volume, get a Virtual Private Network connection, join videoconferencing, etc.

The company offers VSAT services (Ku- and Ka-bands), mobile, fixed or vehicular equipment and a large choice of options to provide the best solutions based on a team's specific requirements and constraints. All equipment is made to last and designed to resist the hardest climatic conditions, to maximize performance and long-term durability.

Rescue environments and refugee camps can be hazardous locations. To ensure personal safety, IEC Telecom offers advanced tracking solutions that allow a complete view of the positioned, front-line staff in real-time.

Gwenael Loheac pointed out, "*Every disaster is different. We provide adaptable, flexible and targeted solutions to enable humanitarian teams to use the latest satellite communication technology wherever they are in the world. We are proud of our customer-focused approach which, backed up by our 24-hour global helpline, means we can guarantee high levels of satisfaction.*

"***When you are saving lives the last thing you want to be worrying about is your communications network — that's our job.***"

iec-telecom.com

Gwenael Loheac is Group COO – Europe and Managing Director of satellite communications specialist IEC Telecom and is based at the company's office in Cergy, France. Gwenael has a strong background in the satellite industry and specializes in purchasing processes and vertical applications. Having joined IEC Telecom in 1997, he now leads business development for the group in the Americas, West Africa and Europe.

DRONING ON

Ground technology implementation by GMV for the MQ-9 Predator B UAV

The World ATM Congress, held in Madrid in March of this year, was a showcase for the latest air-traffic-management (ATM) advances, both in the civil and military field.

Among them, the Spanish technology multinational **GMV** has developed for the Spanish **Ministry of Defense** (*MoD*) the ground segment systems for capturing, storing and distributing information from the unmanned aerial vehicles MQ-9 Predator B, to be used from this year onwards for **Intelligence and Surveillance** (*ISR*) missions.

Drones, notably, now have a growing world market value in the military sector. The latest *ASD Reports*, analyzing the markets of the United States, Europe, Asia and the Pacific, the Middle East and Latin America, places the current value at more than seven billion euros.

In late 2015, the Spanish MoD bought from **General Atomics** two ground control stations and four aircraft, worth 158 million euros.

The first two drones and the two ground control stations will be received this coming summer; the third drone will arrive at the end of 2019 and the fourth and last in 2020.

The MQ-9 Predator drones were selected by the Spanish MoD as they are already in operation in other NATO countries such as the UK, France, Italy and the Netherlands; that incorporation by those nations will make it easier to train pilots and share equipment on international missions, as the need arises.

These **Remotely Piloted Aircraft Systems** (*RPASs*), generically known as drones or **Unmanned Air Vehicles** (*UAVs*), will come into operation at the airbase of Talavera la Real (Badajoz).

Unlike the many tactical RPASs currently flown by the Ministry of Defense, these four new vehicles are the first of the strategic type.

The MQ-9 Predator B will be supporting permanent missions on national territory, such as strategic monitoring in the areas of intelligence, surveillance and maritime security or defense, aerial operations, humanitarian crises, border control and surveillance, firefighting, the fight against terrorism and organized crime, and so on.

The MQ-9 Predator B drones are 11 meters long with a wingspan of 20 meters; they can reach a speed of 444 kph.; their service ceiling is 15 kms. and they can operate 24 hours a day, seven days a week, without being seen from Earth, transmitting information in real time.

The MQ-9 Predator B carries no air-to-ground missiles. These capacities will be covered by the **Euromale** system, a European, long-endurance, remotely piloted aircraft project that involves Germany, Italy, France and Spain.

Ricardo Sáenz Amandi, GMV's Defense & Security Programs Manager, explained how the MQ-9 Predator B drones will work as an unmanned aerial system and their use calls for certain infrastructure: satellite communications and information equipment, **ground control stations** (*GCS*), electro-optical assemblies, radars, identification systems, a de-icing system and flight-collision avoidance systems, as well as specialists in intelligence and image analysis. The GCS has two posts wielding direct control over the aircraft: the pilot and sensor operator.

For the **Directorate General of Armaments and Material** (*Dirección General de Armamento y Material: DGAM*) of the Spanish MoD, GMV has developed the ground segment systems in charge of capturing, storing and distributing information from unmanned aircraft used on surveillance and intelligence missions.

These systems, known as **Coalition Shared Databases** (*CSDs*), receive images, real-time videos plus radar tracks and GMTI tracks and enable all this information to be distributed in real-time to the armed force's intelligence and surveillance centers.

The solution developed by GMV, going under the name of ***CSD-SIERRA***, is now in service with the Spanish MoD and NATO's intelligence centers.

The CSD-SIERRA systems are compliant with all NATO interoperability standards and have been validated on several multinational exercises with multi-vendor UAVs, including those with the highest performance features, such as **Global Hawk**.

To prepare for the arrival in Spain of the first MQ-9 Predator B drones, GMV has already rolled out part of the CSD-SIERRA system network, enabling information from these aircraft to be used by the armed force's intelligence centers and distributed in real time to other surveillance and security support organizations.

www.gmv.com

Predator B RPA image is courtesy of General Atomics Aeronautical.

DISPATCHES

CopaSAT and Kymeta launch a new, flat panel satellite antenna

The disruptive SATCOM-On-The-Move (SOTM) solution delivered through CopaSAT and Kymeta Corporation partnership brings connectivity to commercial and military vehicles and vessels that have, until now, been cut off from such services.

The custom-engineered CopaSAT STORM delivers reliable tactical communications to small, fast-moving vehicles and vessels operating in remote, communications-severed and inhospitable environments.

The CopaSAT STORM is a mission-ready, ruggedized, fully-integrated, Ku-band flat-panel terminal that includes a Kymeta u7 antenna, iDirect 950mp satellite router and a 25 Watt block upconverter (BUC).

The CopaSAT STORM is a mission-ready, ruggedized, fully-integrated, Ku-band flat-panel terminal that includes a Kymeta u7 antenna, iDirect 950mp satellite router and a 25 Watt block upconverter (BUC). It is available in three different configurations including commercial, military and transportable. Advanced options are available that make it possible to add LTE capabilities, a WiFi access point, MANET radio, Newtec modem, as well as numerous mounting options for MRZRs, vehicle luggage racks and more.

Steve Carpenter, General Manager, CopaSAT, said there are so many places, vehicles and vessels where you can't use Commercial-Off-The-Self (COT) SATCOM solutions today. For example, MRZRs, 11meter, rigid, hull inflatable boats (RHIBs) and special operations craft. Legacy solutions don't fit and cannot track fast enough to remain connected with a satellite while the vehicle or vessel is moving at high speed. This has always been a challenge. The CopaSAT STORM addresses the challenge, making all of these applications possible for the first time. It truly redefines situation awareness.

Paul Mattear, VP of Business Development and Sales at Kymeta noted that the CopaSAT team has built an impressive solution that meets the mission critical situations its customers operate in. It is tremendously exciting to see Kymeta™ u7 satellite antenna technology being deployed in highly mobile environments to support data, voice and video across military and government applications that have never been connected before.

www.copasat.com

www.kymetacorp.com

DISPATCHES

How the private sector can help Britain's Skynet-6 program

What do the UK's new aircraft carriers, stealth fighters and active duty military personnel all have in common?

The need for ubiquitous, high speed, secure and resilient connectivity.

The British military is fielding an impressive array of new weapons, from Queen Elizabeth-class carriers and F-35 fighters to upgraded armored vehicles.

All of these projects, as well as an increasing number of legacy systems, share a voracious appetite for connectivity.

Without access to sufficient connectivity, even the most sophisticated weapon will be left at a substantial disadvantage — potentially putting warfighters in harm's way.

"*The UK has an enormous opportunity to make the most of new capabilities being driven by private-sector SATCOM providers, including Viasat,*" said ***Ken Peterman***, President of Government Systems at Viasat.

The UK Ministry of Defence (MoD) recognized the importance of connectivity more than a decade ago when it began the Skynet-5 program, a public-private contract in which the MoD outsourced satellite communications (SATCOM) services to a commercial organization, as a fully managed service.

This included the provision and operations of satellites, upgrades to ground stations and the delivery of user terminals and support.

The Skynet-5 contract is ending in late 2022, and the final shape of Skynet-6 isn't clear.

What is clear is that the world has changed over the past decade. The UK's commitments continue to span the globe from the Baltics to the Pacific, even as multiple defense priorities compete for scarce funding.

As threats from adversaries evolve, coalition operations have now become the norm, which in turn demands access to an advanced SATCOM network to improve collaboration and enhance mission effectiveness.

As adversaries move to develop sophisticated space weapons, including anti-satellite capabilities, demand for a robust, secure and high-speed SATCOM network is soaring.

Which leaves the question: ***How will Skynet-6 respond to this mix of peril and promise***?

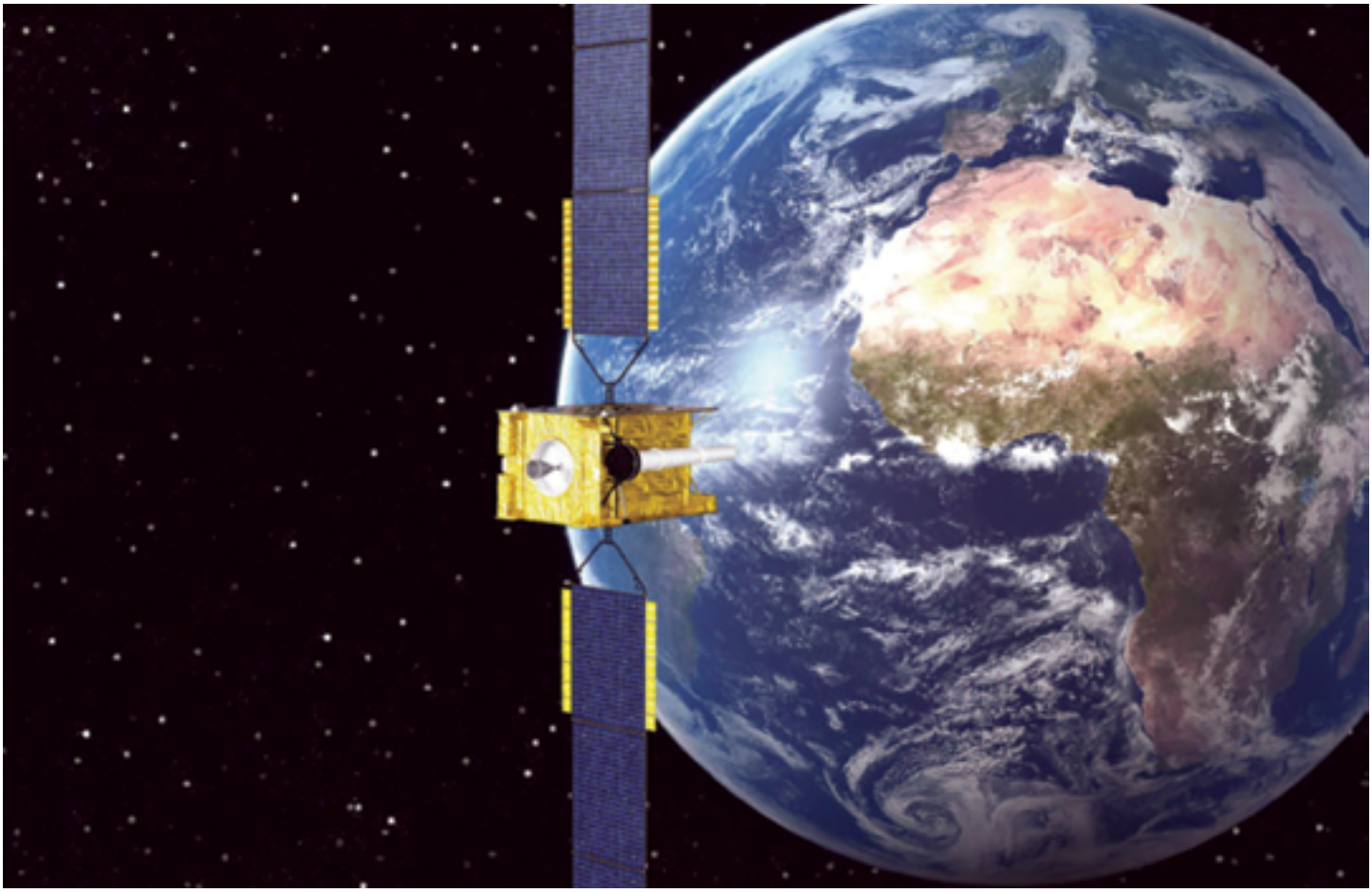
One option is for the UK government to build on its experience of outsourcing SATCOM and move to a service-based interoperable network.

This approach leverages the best of private-sector innovation to ensure the MoD can meet the connectivity demands required to deter adversary threats — all at reduced cost and reduced risk to the UK government.

Ken Peterman has been meeting with a number of MoD and coalition senior leaders to advocate for such a system.

"*By moving to an interoperable network that combines the power of government purpose-built systems with the rapid technological advancements being driven by the private sector, the MoD can easily transition to the high-speed, secure, resilient and ubiquitous system required to adopt new and emerging technologies and deter both current and future threats,*" Peterman said.

Viasat believes that if the MoD were to empirically analyze commercial SATCOM services in a defense context, the results would reveal that the most reliable, secure, user-friendly and cutting-edge services available to meet the needs of defense forces are readily available today.



Artistic rendition of the SkyNet-5 satellite. Image is courtesy of Airbus.

This means offering capabilities such as network layering and resiliency, rapid scalability, cybersecurity, real-time awareness of network threats, and the ability to quickly incorporate the latest technology and practices.

"*The UK has an enormous opportunity to make the most of new capabilities being driven by private-sector SATCOM providers, including Viasat*," Peterman added.

"*These private-sector advancements will satisfy emerging mission requirements, optimize existing assets and provide access to a wide range of new technologies — all at lower cost and lower risk to the MoD.*"

As an example of adaptability, he points to Viasat's Hybrid Adaptive Network (HAN) satellite architecture concept — a flexible, scalable system not locked to any single vendor.

HAN architectures can simultaneously work with government and private networks as well as multiple satellite orbital regimes and frequency bands to significantly enhance the capabilities of armed forces.

Steve Beeching, managing director of Viasat UK, echoed the need for the MoD to move to a HAN based SATCOM architecture.

He said, "*In an era where the threats to the UK and its strategic partners have become so diverse, working closely with industry is going to offer the UK government the ability to provide effective integrated platform solutions — which remain at the forefront of technology — into the hands of our armed forces with unprecedented speed.*

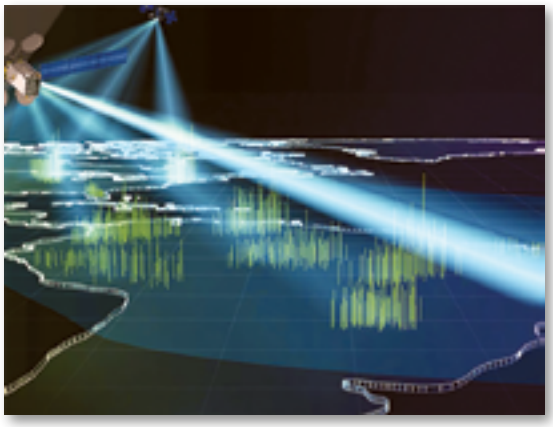
Peterman believes that ultimately, MILSATCOM must offer the same reliability and ease of use that commercial civilian customers have come to expect.

"*We have a new generation of warfighters who have grown up accustomed to an always-connected civilian way of life*," he said.

"*The private sector is capable of deliver HAN networks today, which will create a nearly seamless transition to Skynet-6 as well as provide access to a range of advanced capabilities.*"

"*We have the opportunity to work with the MoD and partners to develop the most sophisticated SATCOM system ever built, and we're looking forward to what the future has in store for Skynet-6*," Beeching added.

Story by Kim Hampson, Marketing Director, Viasat Government Systems.



THE GOVERNMENT SATELLITE REPORT

Connecting military satellites to the cloud

By G. Ramos Carr, Account Director, SES Government Solutions

The federal government has heard the siren's call of the cloud. Since the original "Cloud First Initiative" almost a decade ago that encouraged agencies to explore using cloud solutions for new infrastructure needs instead of building new data centers, government organizations have increasingly been embracing FedRAMP-approved cloud solutions as an alternative.

However, not all communities and sectors within the federal government have been as bullish about cloud adoption. While civilian agencies and the intelligence community have all worked to move data and workloads into the cloud, the defense community has been reticent to go "all in" with cloud solutions – often citing security and other concerns.

But that's starting to change.

Increasingly being heard are senior leadership across all of the branches of the military talking about a need to move to the cloud. These discussions recently culminated in the Pentagon's release of the ***Defense Enterprise Cloud Strategy*** earlier this year, which referred to the cloud as an essential part of defense IT infrastructure that would, "*empower the warfighter with data and is critical to maintaining our military's technological advantage.*"

Chances are, this new desire to aggressively move the **Department of Defense** (*DoD*) into the cloud isn't a result of some top-down mandate.

Rather, this ia a result of the military sitting back and seeing the benefits that the intelligence community and civilian agencies are reaping from their cloud initiatives. And now they want those benefits for themselves.

The Cloud's Positive Impact on Government

Within the Intel community, the cloud has made information sharing much easier and more effective — which was no small feat, considering that intel agencies often struggled with information sharing in the past.

The cloud has also made it faster and cheaper for intel and civilian agencies to develop and roll out new applications and IT solutions — effectively eliminating the need to provision new physical servers and data centers for applications.

While the cost savings and increased speed of execution has certainly been attractive, there have been other, fringe benefits that have resulted from their cloud migrations.

The cloud has enabled these agencies to experiment more and implement innovative IT programs with less concern about failure. As little physical infrastructure investment is necessary to execute on new IT programs, there are few ramifications if a program fails or an application doesn't gain traction within the agency.

The wide reach and geographic spread of cloud providers also creates benefits for government agencies. Emergency and disaster situations are less likely to knock out applications and services since they can be moved from one of a cloud provider's data centers to another in a location that wasn't impacted – something that would be impossible without significant cost for an agency operating using only brick and mortar enterprise data centers.

This also allows data and applications to be housed and hosted geographically closer to where they're needed, since most cloud providers operate a massive number of data centers in various different geographies.

The military has seen these benefits in action for the intel and civilian agencies and they understandably want access to them, as well. But they face a unique challenge that they're going to have to overcome if they're going to migrate necessary applications, IT services and tools into the cloud.

Connecting Military Personnel

The DoD has civilian personnel, senior leaders and active duty warfighters deployed across much of the globe. The organization is extremely large, and extremely distributed.

At home within the United States, on military bases and in office buildings, high-speed, broadband connectivity is almost taken for granted. It's ubiquitous and available to deliver the most bandwidth-hungry applications and IT services to anyone who needs to access them.

However, when you start to cross outside U.S. borders, when you leave military bases, when you operate outside of allied nations with stable and reliable infrastructure, that connectivity can evaporate. That's a massive problem when all of the applications and IT services that military personnel rely on are hosted in the cloud — and a reliable, high-bandwidth connection is necessary to access them.

The fact is, the experience for military personnel on a military base is nothing like the experience for personnel in a forward operating base. Should there not be consistent, reliable network connectivity, should networks not be secure, or should terrestrial networks simply not exist, deployed military personnel will not have access to cloud-hosted tools and applications. That's probably where they'll need them the most.

Thankfully, there is a solution in the form of satellite communications.

Satellite: The Military's Key to the Cloud

In places where terrestrial networks are nonexistent, unreliable, insecure or lack the necessary bandwidth for military applications, satellite communications can fill the military's connectivity requirements.

Needing little ground infrastructure to operate and available from space to practically anywhere on the globe, satellite is an adept alternative for delivering the connectivity warfighters need to access cloud applications and tools. This is especially true thanks to recent innovations and advancements in commercial satellites and satellite constellations.

Today's innovative **High-Throughput Satellites** (***HTS***) are now available at orbits closer to the Earth, including **Medium Earth Orbit** (***MEO***), which drastically reduce latency and deliver an experience on par with high-speed terrestrial fiber networks. This is essential for delivering access to advanced cloud solutions that may require low latency environments, including cloud applications that require less than 200 milliseconds of latency.

In addition to their ability to deliver immense bandwidth, high throughputs and low latency, these MEO HTS satellites are also more secure. Comprised of moving satellites using small spot beams, communications sent via MEO constellations — such as the ***SES O3b MEO*** satellite constellation — are more difficult to jam and intercept.

As military operations continue to become more network-enabled, and as military IT solutions and applications continue to make their way into the cloud, connectivity for the warfighter is only going to increase in importance.

MEO satellites are the most available, reliable and secure solution for giving deployed military personnel and warfighters access to the cloud regardless of where they are on the planet.

The post How satellites can connect the military to the cloud appeared first on GovSat.

This article first appeared on GovSat and is republished with their permission. To read additional, informative articles, please visit ***ses-gs.com/govsat/#***

BRIEFING: LEPTON GLOBAL

COMSATCOM solutions for the Pacific region

By Lyuda Promyshlyayeva, Director of Marketing, Lepton Global Solutions

The attack on Pearl Harbor in December of 1941 turned the world's eyes to the Pacific and began a new west-ward facing chapter in American history.

We often think of the Pacific as the gateway to East Asia: China, Japan, and the Koreas are the region's most formidable economic and military powers and it is not unthinkable that a hot war could take place in that theater in the future.

The Pacific is also, notably, a gateway to Russia via the Bering Strait and the Aleutian Islands further to the west. As relations with North Korea teeter, and Russia continues to engage in overt hostilities toward U.S. domestic affairs, there has been a notable increase in activity and, therefore, requirements for satellite communications in this region of the world.

As the most pelagic region on Earth where humans regularly operate, the Asia-Pacific theater has been highly reliant on satellite communications since the technology's arrival. Its vast area, diverse climates, and relatively small population density limit the extent to which the terrestrial networks popping up elsewhere around the globe will be developed. Yet, multinational businesses, national defense and environmental agencies, commercial shipping conglomerates, and aviation communications customers exist all the same.

Without fiber optic network access in remote Pacific locations, users rely heavily on satellite communications to establish a digital connection between headquarters and remote end-points, boost operational efficiency, and improve employee safety and morale. This need increases demand for bandwidth in the Pacific, which is coupled with a renewed U.S. military focus on the region and has led to an increase in **Lepton**'s activities in the area.

Since the company launched their first managed services in the Pacific using a Eutelsat Americas satellite in 2016, Lepton has increased capacity and customer usage fifteen-fold. Lepton customers in the Asia-Pacific region now enjoy broad coverage throughout the region on multiple satellites.

Today, Lepton manages Ku-band networks on Eutelsat 172 B (172 degrees East) and 70B Asia (70 degrees East), and new, managed networks will launch on E174 (174 degrees East) in Q2. The company provides Ka-band services through **Inmarsat**'s ***GlobalXpress***® offering.

Also added is networking infrastructure to a second teleport that covers the Pacific in order to offer redundant ground entry points. Among the chief infrastructure advancements is the establishment of a terrestrial Point of Presence at the secure, state-of-the-art **CoreSite Data Center** in Northern Virginia, which enables the firm to provide a "native" U.S. Internet experience to government and commercial customers from the Washington, D.C. area.

A Pacific Partnership

Lepton's long-standing partnership with **Hawaii Pacific Teleport** (*HPT*), located on the island of Oahu, continues to develop, with new satellite offerings and their expansion to Guam. HPT offers satellite and fiber-based communications, connecting the continental United States with the Pacific region. In selecting global teleports to host Lepton's network infrastructure, the company selected HPT for due to the teleport's robust fiber connections, a wide range of orbital visibility as well as access to the Pacific.

Since HPT's expansion to Pulantat, Guam, Lepton's satellite service offering extends even further west into the Pacific. The presence of an American, state-of-the-art teleport in the heart of the Pacific provides another landing station and access to additional satellite footprints not visible from Hawaii or the U.S. mainland. Lepton is already developing solutions for PACOM military customers with new requirements using HPT's Guam teleport.

As the company's network infrastructure grows, the ability to support the diverse (and interesting) requirements of Pacific region customers increases.

Alaska and the Aleutians

With the lowest population density in the country, and perhaps the harshest weather conditions, Alaska has been the slowest of the 50 states to adopt state-wide fiber communications.

City of Utqiaġvik (Point Barrow), Alaska.

In addition to commercial land-based customers in the state's mainland, Lepton also supports government sites on both the continent and in the state's remotest reaches, the Aleutian Islands chain. Located up to 1,500 miles west of Anchorage, these islands are home to U.S. naval and U.S. Air Force (USAF) stations that date back to WWII.

In spite of the harsh environment of the extreme North and its isolated location, Lepton Global proved for one defense customer a wide beam geosynchronous satellite connection as far as 71 degrees North.

Point Barrow, Alaska

Environmental operations located in some of the most remote areas of Alaska provide the monitoring of various geological behaviors such as

volcanic activity, ice characteristics and movement analysis, seafloor profiles, and long-term weather forecasts. The teams of scientists located in this region rely heavily on satellite communications to transfer their findings back to mainland headquarters. As missions can be short-term regional studies, or 24/7 year-round research, Lepton offers highly flexible service options.

Defense in the Pacific

Satellite communications also play a role in critical defense infrastructure to protect American shores from the west and across the Arctic.

SATCOM often serves as the only communications link for American military personnel on land and at sea in the region and also provides a transmission medium for seismic and missile sensors situated in-theater.

Defense communications requirements in the Pacific are vast and growing. Over the past 12 months, Lepton has supported military communications-based exercises on the JSAT 2B satellite, provided new communications links for increased service member presence at key islands in the Pacific, developed short-term service solutions with quick deploy terminals for sites only accessible during warmer months, and responded to several large government Requests for Information to bring hundreds of megabits per second (Mbps) to previously neglected military outposts.

In addition to the Defense agencies, the U.S. Coast Guard (*USCG*) plays an essential role in the Pacific with search and rescue missions, enforcement of maritime borders, and spearheading environmental protection studies. The USCG also participates in various missions in the Bering Sea alongside the International Maritime Organization partners, including Russia, Japan, and China[1]. All of these activities require robust satellite network support.

Lepton has provided services to the USCG since the 2017 disaster recovery missions in Texas, Florida, and the Caribbean, following hurricanes Harvey, Maria, and Irma. Today, the company also supports west coast-based units that deploy to the Pacific for emergency response support throughout the region.

Shipping and Science

In addition to military and defense activities, the Pacific is full of maritime vessels transporting cargo.

Key trade routes run from Shanghai, Singapore, and Hong Kong to the California coastline. In 2017, more than 284,000,000 metric tons of cargo were transported by ships to and from the Pacific ports[2].

In any given week, more than 100 cargo liner services operate routes across the Pacific Ocean from North America to Asia and Oceania[3]. Lepton's Ku-band networks support cargo ships roaming across the entirety of the Pacific Ocean and may support up to 80 vessels sailing in and out of the firm's networks in the region at any given time.

Lepton also supports organizations promoting scientific and humanitarian missions throughout Alaska and the Aleutians, on Wake Island and as distantly as Micronesia. These customers collect data in often unmanned remote locations or provide support in emergency response situations, and they all rely on satellite communications as a fundamental part of their mission.

Customer Support Mission

The global SATCOM market has increased in the Pacific Ocean area due to increased military activities and international collaborations, commerce, digital growth, and IoT expansion.

Connecting customers in this region often poses challenges, whether it be traveling to the remotest points of the ocean to install an antenna, or working across many time zones to provide technical support.

Lepton's goal is to provide every customer, regardless of the obstacles, with the highest quality network service and customer support possible. Lepton's team delivers the same award-winning level of support to all customers, from U.S. military users calling home to the scientific community providing critical research data.

To the company, every customer deserves to achieve their mission, share their discoveries with the world as well as stay in touch with their families and loved ones. Lepton is looking forward to the continued growth that 2019 will bring to the firm's networks and customers in the Pacific.

leptonglobal.com

References

[1]*U.S. Center for Strategic & International Studies Maritime Futures and the Bering Strait Region November 29, 2017, 14:00-15:00*

[2]*U. S. Department of Transportation MARAD Maritime Administration Report U.S. Waterborne Foreign Container Trade by U.S. Customs Ports 2000-2017, "Container-Ports-2000-2017.xlsx"*

[3]*World Shipping Council Trade Routes*

Ms. Promyshlyayeva has experience in B2B and B2G business environments. She previously worked for manufacturing and distribution companies and joined Lepton Global in early 2016.

AIS ship tracking snapshot of marine traffic in the northern Pacific. Credit: ***Vesselfinder.com****.*

CYBERSECURITY: NEXGEN DEFENSES

The threat of cyber-attacks continues to grow

By Tore Morten Olsen, President, Marlink

In 2017 alone, cyber-attacks cost the maritime industry hundreds of millions of dollars. Preparing and implementing stringent cyber security standards is essential to reduce the effects and potential loss.

Marlink's role in helping customers to defend against cyber threats is taken very seriously and provides a range of solutions to reduce the risk of a cyber-attack and mitigate the consequences of such an intrusion. While technology is important, education and understanding are key.

In this article, the aim is to explain the challenges, the methods that cyber criminals use, and the solutions and technologies in place to prevent cyber-attacks.

Ultimately, successful cyber security is a collaborative approach. Worth noting is that, so far, most known large-scale cyber-attacks in the Maritime sector have been untargeted (including *WannaCry* and *NotPetya*). However, it is widely expected that cyber attackers will increasingly "discover" the Maritime Industry and launch targeted attacks which are much more dangerous and can only be detected using next-generation cyber security measures.

Rapid Satellite Capacity Growth and Vessel Digitalization

For many decades, ocean-going vessels were connected via voice and low-bandwidth communications which were used exclusively for business purposes e.g. communication with shore office and port authorities.

Thanks to the large scale deployment of **High Throughput Satellites** (*HTS*) in the Maritime Sector, the available bandwidth has increased manifold while the cost per transferred megabyte (MB) has decreased.

As a consequence, it is widely expected that cost will no longer be an entry barrier leading to twice as many broadband connected vessels in the next six years (***see figure 1 on the following page***).

Already, crew on vessels expect to use communications for welfare purposes (*e.g.*, browse the internet, chat with their families and friends) and according to recent surveys, for 78 percent of seafarers this has a strong influence on their choice of employer (***Source: Futurenautics Crew Connectivity Survey***).

Technically impossible just a few years ago, according to the same survey, nearly half of the respondents see 1 Mbps as the minimum acceptable crew bandwidth.

In addition to enhancing existing applications such as crew welfare, the higher available bandwidth will allow vessel operators to connect their various vessel systems to shore at negligible cost.

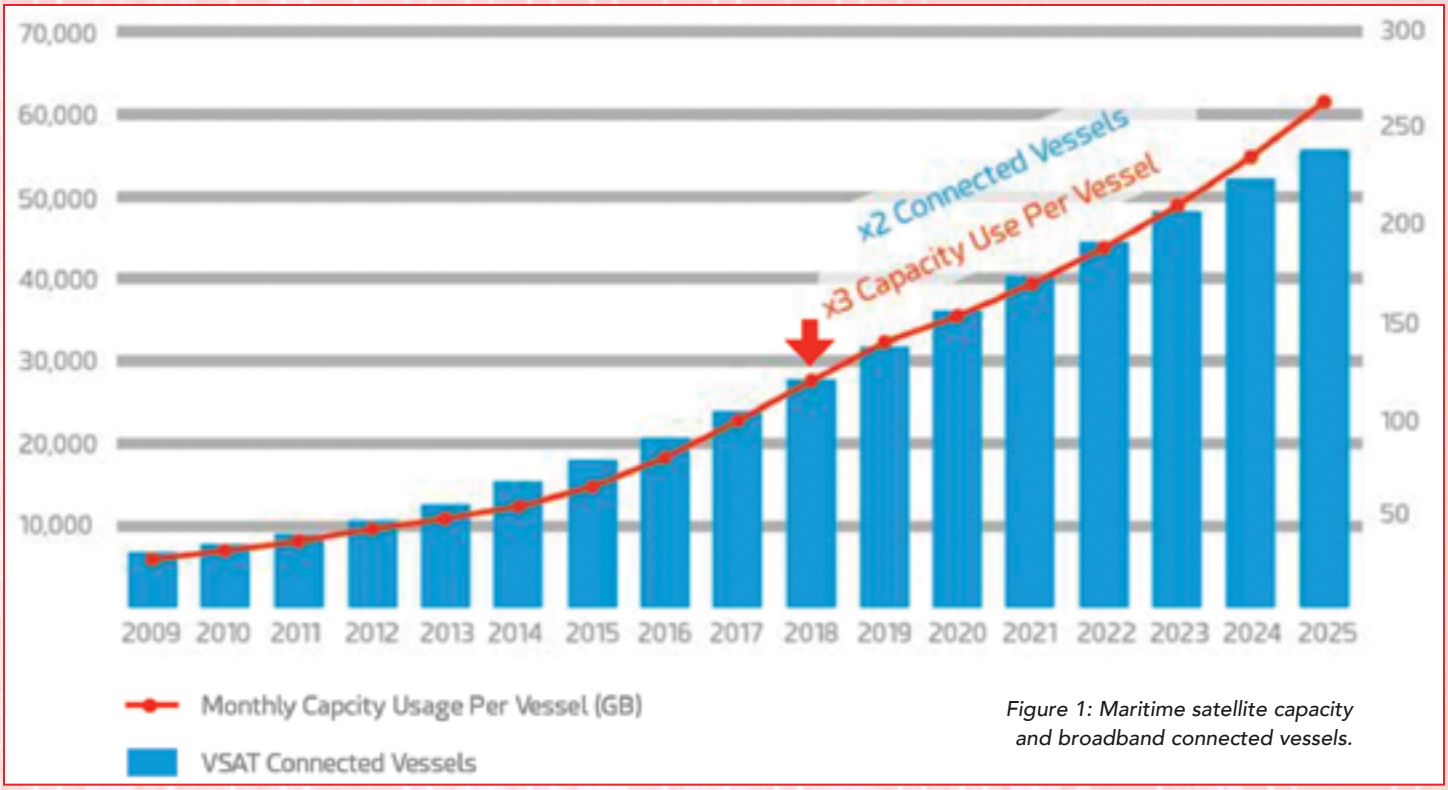


Figure 1: Maritime satellite capacity and broadband connected vessels.

This will enable digitalization applications offering increased operational efficiency and optimizing processes, such as:

Fuel and Energy Efficiency
Transfer vessel sensor data onshore to specialized analysts in order to recommend the most efficient operating processes.

Environment and Reporting
Automate emissions data collection and reporting to authorities (e.g. MRV in the EU).

Smart or Predictive Maintenance
Manufacturers could detect potential equipment failure in advance and perform corrections via remote connection or schedule an intervention at the next port visit.

E-Navigation
Update navigational charts automatically into the ECDIS or remote planning of vessel navigational routes.

E-Learning
Update learning material automatically and synchronize crew certificates to the shore HR office while still at sea.

Cyber Security State of Play

Maritime Cyber Awareness
The increasing inter-connectivity of vessel systems combined with the growing penetration of broadband communications (***e.g.***, VSAT) and multi-bearer services (*e.g.*, 3G/4G) enables operational efficiency gains, but also increases the vulnerability to cyber-attacks.

Although historically not considered part of the critical infrastructure sector, given the fact that more than 90 percent of global trade is carried by sea, shipping companies may increasingly become a cyber target. In fact, the Maritime Industry is particularly vulnerable for the following reasons:

1) *Information Exchange Across Many Stakeholders at Different Time Zones*
Vessel staff regularly communicate with different stakeholders, such as the ship owner, charterer, origin port, destination port, consignee, customs authorities and bunker providers. This significantly increases the vulnerability of the communications systems and enhances the likelihood of a cyber-attack.

2) Vulnerability of Legacy Systems Onboard
While the modern IT system life cycle is two to three years, the lifetime of a vessel is 25-30 years. Security was not a concern when many legacy Operational Technology (OT) vessel systems (e.g. navigational computers, engines) were developed and many are using vulnerable practices such as outdated protocols, default password and static public IP address.

However, many vessel OT systems may not be modified for regulatory reasons and may no longer be supported by the manufacturer. It is therefore crucial to isolate and protect these systems to avoid spreading any OT vulnerabilities to the entire IT network.

3) Low Crew Awareness
Most crews and onshore staff are insufficiently prepared for cyber-attacks, resulting in behavior that fails to contain the damage. Crews need to be made much more aware of what are typical cyber-attacks, how to prevent them and how they can contribute to raise cyber security onboard.

Captain, officer and crew frequently face a high workload with vessel operational tasks and cannot necessarily treat IT Security as a priority. Furthermore, they are more and more bringing their personal devices with them onboard, accessing the internet more frequently while at sea, and consequently increasing the chance of infection on the vessel network

4) Dynamic Cyber Environment
Cyber vulnerability has been increasingly exposed at recent industry conferences and is now seen as an organization wide concern for IT technicians, ship managers and C-level executives at shipping companies.

Cyber security threats are dynamic by nature and protection against threats is a continuous game of catch-up. There are more than 500,000,000 known malicious malware programs, with over 390,000 new variations of attacks and new malware detected each day[1] . This mainly covers untargeted attacks with malware indiscriminately sent to as many machines or

services as possible, hoping that some of them might become infected.

In addition, targeted attacks by sophisticated organizations with significant resources are becoming more common for businesses. Based on extensive intelligence on the target IT system and the unaware users, the attackers use a blend of customized intrusion methods with the objective of staying undetected in the network as long as possible.

State Regulation

With the **European Union General Data Protection** (***GDPR***) being in force since May 2018, all shipping companies based in the EU, traveling to EU ports or transporting cargo for EU customers have to stay compliant with the data protection.

This new regulation forces organizations to take responsibility for data protection and legal liability towards the owner of the data, mandating the notification of a cyber incident to public authorities as well as to the third-party data owners within 72 hours. This regulation requires organizations to improve both their cyber security and develop specialist forensics capabilities or face significant penalties.

Specific to the Maritime sector, the **Baltic and International Maritime Conference** (***BIMCO***) has already issued a set of cyber security guidelines, the **International Maritime Organization** (***IMO***) has made it mandatory to include cyber risk into each vessel's **International Safety Management** (***ISM***) ***Code***.

The **U.S. Coast Guard** (**USCG**) has created a dedicated **Cyber Command unit** (***USCGCC***) and published its cyber strategy in June 2015. While there is currently no obligation to adhere to its recommendations, many industry observers believe that required documentation to enter U.S. ports may soon include an assessment of the vessel's cyber resiliency. A public notification obligation of cyber incidents has been in place for several years in many American states.

Other regions and organizations are expected to follow adopting similar legislation.

Maritime as a Target

Actors

The profiles of cyber-attackers have profoundly changed in the last ten years from isolated individuals or small groups operating without a defined strategy to professional criminal or military groups.

Criminal Organizations

Traditional organized crime groups (e.g., mafia) have recognized cyber as an opportunity to support illegal trade or to enable financial gain.

Hacktivists

Political organizations, underground activists (*e.g.*, ***Anonymous***, ***LulzSec***) and terrorists are using cyber-attacks to support their political agenda.

Sponsored by Nation States

Nation-states are directly engaging or sponsoring cyber-attacks as a means of warfare and/or (economic) espionage.

Insider Threat

An insider threat happens when a person who is close to an organization or has authorized access, misuses that access to negatively impact the organization's critical systems.

Hacktivism

Political groups are increasingly using cyber-attacks as a tool to extract confidential data which is then disclosed to the public to raise public awareness / outcry or damage reputation *e.g.*, publishing compromising photos taken on super yachts.

In addition, political groups may use operational disruption to 'retaliate' against the target's practices *e.g.*, deactivating or destroying vessel systems.

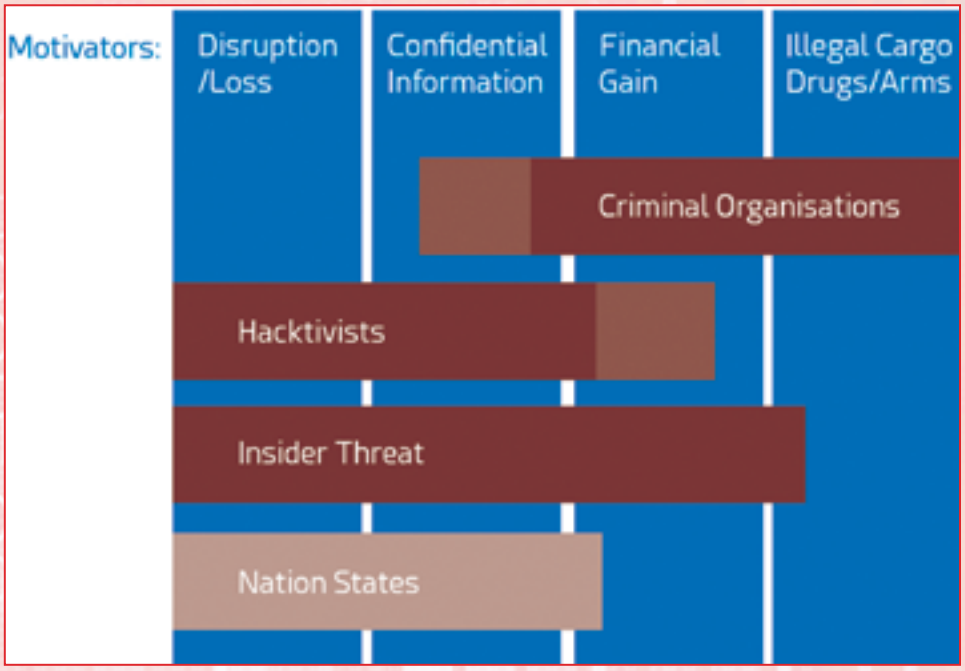


Figure 2. Overview of actors & motivators of cyber-attacks.

Motivations

Financial Gain

To obtain financial gain, cyber-attackers may use '*ransomware*,' a malicious software rendering a PC inoperative with a demand for ransom payment to unblock it. While most cases are kept silent, it is believed to be the most common type of cyber-attack today. Fleet Managers may feel inclined to give in to the blackmailing as any disruption to business continuity causes direct financial loss and the IT competency of the vessel crew is very limited, however, there is no guarantee that the attackers will actually unblock the computers following a payment.

Another type of information valuable for attackers are bank details, which may be used to initiate payments to their accounts e.g. from super yacht passengers, or by counterfeiting bunker fuel invoices. Such attacks are facilitated by the fact that the stakeholders are scattered across multiple time zones and cannot always communicate rapidly. Criminal organizations or insiders such as malicious employees with network privileges, are the most likely authors of such attacks.

Common political targets include the Oil & Gas Industry, high-net-worth individuals and certain fishing segments such as whaling. Organizations could also potentially make use of cyber-attacks to cause damage or even loss of life to support their objectives. Hacktivists are not typically interested in financial gain.

Mafia / Smuggling

As opposed to the previous two motivations, criminal organizations aiming to transport illicit goods (*e.g.*, drugs, arms, etc) are generally aiming to stay undetected. An interesting example is the Antwerp port cyber-attack[2] in which drug traffickers recruited hackers to gain access to the IT systems controlling the movement and location of containers. This attack demonstrates the sophistication and resources of organized crime related to cyber-attacks.

Piracy

While there has not yet been any reported cases of physical piracy supported or prepared by a cyber-attack, theoretically a vessel could be led off course or taken over by pirates through an engine shut down or by taking over the navigation systems on board.

Cyber-Attack Impacts

Safety Risks

While most current vessel systems are not yet connected to external networks, it is widely assumed in the maritime industry that in the decade ahead the optimization of processes and operations will drive the digitalization of the maritime sector. This evolution may result in additional vulnerabilities, caused by human beings.

Critical Systems Interruption

Piracy attacks could be facilitated by deactivation of vessel engines and falsified navigation charts.

Vessel Hijacking

By controlling a vessel remotely, attackers could try to provoke vessel collisions, shore accidents or move containers e.g. using the vessel's crane.

A glimpse of the potentially disastrous possibilities is offered by a 2015 attack on a **Remotely Operated Vehicle** (*ROV*): a hacker was able to override the controls sent from the mothership to the ROV, causing the ROV to sink to the seabed[8]. The cost of the resulting salvage operation was $500,000.

Fines by Authorities

In the past, national data protection agencies' maximum fines for non-compliance used to be a very limited deterrent *e.g.*, 100k euros in France and 900k euros in Spain. However, under the new EU GDPR regulation, noncompliance can lead to potentially substantial fines of up to 20 million euros or 4 percent of annual global company revenue (whichever is greater).

Moreover, the EU has indicated that penalties will be particularly severe if a cyber-attack was facilitated by negligence *e.g.*, insufficient protection mechanisms, unencrypted sensible data, untrained staff.

Insurance

Maritime insurance companies have recognized the risk of cyber-attacks and refuse to provide coverage if the damage was a consequence of it. Therefore, virtually all maritime insurance policies contain the Institute **Cyber-attack Exclusion Clause** (*CL380 — see Annex 1*). Many shipping companies are probably unaware of this financial risk and would be unable to absorb this potentially huge liability.

Taking the case of the 2007 loss of the MSC Napoli as an example (although not caused by a cyber incident), overall liabilities linked to hull loss, cargo loss, environmental damage, personal injury and removal of the wreck came to more than $1 billion[3].

Business Disruption

Business disruption as a result of a cyber-attack is another source of potentially considerable financial impact. The 2011 attack on the **Islamic Republic of Iran Shipping Lines** (*IRISL*) gives an idea of the potential scale: the cyber-attack caused an outage on the entire internal network, meaning rates, loading, cargo number, date and place were not available[4]. Consequently, a number of vessels had to stop operating as cargo manifests were inaccessible; in a number of cases, cargo was sent to the wrong destination and had to be recovered, causing additional losses. Such an outage affecting the entire 115 tanker fleet might have caused direct losses of over $1 million per day[5].

The financial risk for cargo operators is even higher; in 2017 the average cargo operator's capacity was 100,000 TEU; meaning that the potential direct loss of an IRISL-like fleet-wide attack would be $100 million per day[6]. Considering the strained financial situation and cyber exclusion clause in most insurances (*see Annex 1*), many cargo operators might not be able to financially sustain such an attack. Connectivity outage resulting from a cyber-attack may also cause disruption on a smaller scale, *e.g.*, by non-timely reporting of **Notice Of Arrival and Departure** (*NOAD*) forms for port entry:

- *Delays for entering into port*
- *Fines by authorities for non-timely / non-electronic reporting*
- *Late cargo delivery penalties*
- *While waiting for port entry: additional fuel burnt, additional crew working and vessel charter days*
- *If the issue cannot be resolved remotely: travel expenses to send IT technicians onboard*

Company Reputation

Less immediate than the previously mentioned consequences, the negative impact of a cyber-attack on a company's reputation can however be substantial in the longer term. In a survey by the Economist Intelligence Unit in 20167, C-suite members of large companies were asked about the greatest risk of a cyber-attack; the majority responded: damage to "*our reputation with our customers.*"

While it may take decades to build trust in a brand, media coverage about a cyber incident establishes a negative association, which can severely damage the public reputation for a long

period of time. Consumers and businesses are particularly sensitive to cyber breaches because it exposes the confidential data they have entrusted the company with identity, bank details, business information and may lead to financial losses.

Maritime Risk Assessment and Protection Solutions

The Maritime industry has only recently started to understand the risk to its assets and the need to protect critical systems. Cyber-attacks to critical systems as outlined may disrupt business continuity (*e.g.*, connectivity outage) and paralyze a vessel.

The direct and indirect cost factors of any such delay to the voyage are extensive. Rather than being an isolated IT topic, all concerned stakeholders (including finance, fleet operations and commercial departments) need to draft a contingency plan with response procedures in case of a cyber-attack.

A risk assessment of the vessel's critical systems and contingency plans need to be established. For instance, the GPS position and ECDIS charts are fundamental to the ship's navigation and safety, yet experts have demonstrated that many systems suffer from cyber vulnerabilities.

Moreover, the cargo manifest can be of high value to attackers seeking to read or modify the information to enable illicit trade. Secure network architectures are emerging which isolate systems identified as critical to vessel operations (ECDIS, ERP Systems, etc) from directly facing external networks. Implementing a back-up communication system which could be non IP-based and has a different entry point would allow business continuation in case of a major infection of all IP communication systems.

Cyber-Attacks and Security in a Nutshell

Methods of Intrusion

Untargeted Attacks: Every cyber-attack is composed of multiple phases, the first one being intrusion into the network. The following untargeted intrusion methods are indiscriminately sent to as many machines as possible.

Email Threats: Many of the most prolific viruses distribute themselves automatically by email. Any attachment received by email could carry a virus, and launching such an attachment can infect a computer. Even an attachment that appears to be a safe type of file, *e.g.*, a file with a .txt extension, can pose a threat. The amount of email spam and viruses is rising constantly and are estimated to represent more than 70 percent of global email traffic.

Malware Apps on Personal Devices: With more and more personal devices of seafarers (**Bring Your Own Device** = *BYOD*) being used on a vessel's network, apps containing hidden malware can provide a backdoor for cyber criminals. There are currently at least 7,000 free apps proven to contain aggressive adware that can lead to an infected IT network. 80 percent of them are still available on app stores. The potential for infection is high as over 10 percent of these have been downloaded a million times.

Worms: Rather than direct infection, a PC could also become infected by a worm creating exact copies of itself and using connectivity between computers to spread within a network.

Keylogger: Using a hardware device or covert software to record every keystroke and mouse movement made by a user, cyber-attackers may extract confidential information or passwords to gain access to IT systems.

Password Attacks: A trial-and-error method using automated software to guess a user password by systematically trying all possible passwords. Such attacks may be prevented by limiting the number of attempts to enter a password, introducing time delays between attempts and strong passwords (minimum of 12 characters using both alphanumerical characters and symbols).

Targeted Attacks: In a targeted attack, attackers initially perform extensive intelligence on the specific configuration of the IT system as well as its vulnerabilities or on the people using the systems and then tailor malware specifically to an organization. Most conventional cyber security measures (*e.g.*, Anti-Virus, firewall) will not detect such specifically targeted malware.

Pharming and Phishing (Social Engineering): All attacks can be supported by Social Engineering based on impersonation techniques, *e.g.*, using a bogus Social Network profile showing the same interests as the person and coming from the same hometown. This is very effective in tricking a person into installing the malware application, opening an email attachment or supplying confidential or personal information.

Another method consists of distributing an email that appears to come from a reputable organization, such as a bank. The email includes what appears to be a link to the organization's website, but the link directs to a replica of the website. Any details entered, such as account numbers, PINs or passwords, can be stolen and used by the hackers who created the bogus site.

Zero-day Attacks: While anti-virus programs protect against signatures of known malware in their threat database, there is a time window between the detection of new vulnerabilities, the time they are added to the anti-virus database, software patches are developed and the time the anti- virus signature update or software patch are deployed on the computer. This very sophisticated method is often used by targeted attacks and can only be detected through behavioral analysis and **Deep Packet Inspection** (*DPI*).

Advanced Persistent Threat: An attack specifically designed to be difficult to detect using conventional means, thereby allowing the attackers to remain undetected in the network for a long time: more than three months on average. APTs can only be detected using advanced Cyber Detection solutions.

Intrusion Via a Less Secure / Third-party Network: If the configuration of the target's IT system is known, attackers may attempt to first gain access to a less secure (*e.g.*, BYOD device, social network) or a third party system in order to then intrude into the corporate network. The 2014 cyber breach on the U.S. retailer Target actually started via a breach of the heating and ventilation contractor's billing system.

Malicious Software (Malware): Once the cyber-attackers have obtained access inside the network; they deploy malware in order to carry out their main mission. Malware can be classified into the groups explained below and, in some cases, actually may belong to several groups (e.g. a Trojan Horse spreading as a worm).

Trojan Horses and Remote Access Tool (RAT): A Trojan Horse appears to be legitimate software with a clear function and may even carry it out, but actually performs another task in parallel, usually without the user's knowledge. RAT is a malware program providing remote control over the target computer to the cyber-attacker (*e.g.*, to take screenshots, activate the webcam, format drivers, access locally stored files).

Spyware: Software that enables hackers to gather information without permission. It tracks activity or copies data and reports it to others, and consumes memory and processing capacity that may slow down or crash computers.

Adware: Software that displays advertisements on computers. Adware can slow down a PC and is designed to be difficult to uninstall.

Ransomware: A type of malicious software which blocks the system or encrypts data, forcing its victims to pay a ransom to the cyber-attackers in order to regain access to their system. Commonly used Ransomware programs include **Bit Locker** (not to be confused with the Microsoft product) and **Locky**.

Botnet / Zombie: A group of computers infected with a RAT which is used to carry out malicious tasks (e.g. sending email spam, DoS attacks). In most cases, the owners are not aware of the breach.

Rootkit: A piece of software that provides the attacker with maximum privileges (e.g. root privileges) on the infected machines, allowing him to perform potentially destructive tasks that are not allowed by a regular user account.

Disruption
Most cyber-attacks aim to take over IT systems for specific purposes. However, some attackers primarily intend to cause disruption to access and leak as much information as possible.

Denial of Service (DoS): An infrastructure attack aimed at making a system unavailable to its intended users by flooding a server with a large number of requests, thereby blocking the fulfillment of legitimate requests.

Sabotage / Destruction: In some cases malicious software is aimed at destroying industrial systems (e.g. Stuxnet) or making computers unusable (*e.g.*, by deleting the operating system), thereby creating a threat to business continuation or even a major infection of all IP communication systems.

Conventional Maritime Cyber Security Measures

Cyber Security Framework

In order to protect a property, one would generally first conduct a study of the grounds and the neighborhood to identify weaknesses as well as all possible entry points and then install a number of locks and shutters (PROTECT) as well as alarms and sensors (DETECT). In case of a confirmed intrusion, it important to RESOLVE it as quickly as possible.

As shown in ***Figure 3***, this is a continuous process; after an intrusion, one would generally try to understand how it was carried out and improve the means to PROTECT and DETECT.

Figure 3. Continuous cyber security process

In the same way, protecting a Maritime IT network against cyber threats requires a combination of proven tools and processes. Isolated means such as a firewall and anti-virus (**PROTECT**) need to be complemented by a strategic deployment of threat detection and response hardware and software (**DETECT** and **RESOLVE**) as well as training of the staff on board. This will help to ensure never being in a position of having to pay hackers a ransom, a fine to national bodies or suffering from a severe loss of reputation.

Staff Awareness and Usage Policy

While access to the internet has become common on shipping vessels for both business use and crew staying connected with family, crew members are not aware of cyber risks.

Therefore, in addition to technical cyber security solutions, it is essential to create awareness among the staff through regular training as well as a clearly communicated IT usage policy ('*IT Charter*'). Cyber criminals know that untrained people or those with little computing experience are an easy target. If malware of any sort does get through to a vessel's PC network, the final step for the attack is the execution by the user which may be facilitated by social engineering.

Training courses should teach best practices (*e.g.*, avoid opening suspicious email attachments), clear procedures in case of a detected cyber-attack as well as awareness about available secondary back-up systems.

Access Management

There are several technical means to implement this policy: the first, and most obvious parameter is user authentication to ensure that the user (a human or a device) is approved to be on the network. Once this is established, user access management can be set based on specific time slots according to shift patterns. Thanks to this system, it is also possible to detect any unauthorized access attempts, or keep track of usage patterns. Marlink's Integrated Communication Management Platform includes a complete User Access Management system (see

Marlink's ***Integrated Communication Management Platform*** includes a complete User Access Management system (see Marlink's "*Cyber Guard Solutions*" brochure).

Endpoint Device

Firewall

The first line of perimeter defence is the firewall integrating basic protections and being able to filter internet traffic upon defined rules (*e.g.*, based on ports, protocols, applications). A shore-based firewall at the internet gateway may be complemented by a firewall deployed at the vessel, scrutinizing requests from remote terminals to the internet. This service provides protection against untargeted internet attacks and non-customized malware.

Marlink on-board solutions include firewalls (*e.g.*, ***XChange 2-stage***, **Cisco** and ***FortiGate Firewall***, see Marlink "*Cyber Guard Solutions*" brochure). In addition, Marlink also provides shore based firewalls: ***Data Manager*** and ***@SEAwebControl***™.

Anti-Virus

Anti-virus software combats a wide range of threats such as viruses, Trojan horses and other malicious software by comparing detected programs to the signature database of known threats. Regular updates are therefore key to detect the most recent threats. Some anti-virus software providers are complementing signature-based protection with behavior-based screening; thereby even if a new ransomware software is not part of the signature database it may be detected by analyzing its behavior *e.g.*, if a process starts encrypting a large number of files.

Marlink provides a satellite optimized anti-virus package that includes both signature and behavior based screening (***SkyFile Anti-Virus***) as well as version monitoring of any anti-virus software through ***KeepUp@Sea***™ (see Marlink's "*Cyber Guard Solutions*" brochure).

IT System Configuration

Particularly on Corporate PC's, it is recommended to enforce the IT charter through management of the PC's configuration e.g. through settings in the Windows registry. Depending on the criticality of the machines, measures could include: deactivation of all USB ports, blocking of new devices to be connected or new software to be installed unless an administrator has given prior approval. IT Configuration Systems detect attempted changes to the system and automatically roll back to the latest approved configuration.

Marlink's ***KeepUp@Sea***™ operational vessel IT platform includes Configuration Management with automatic restoration.

Applications

Email Security

It was reported in April 2016 by security company Retarus that one in six of all incoming emails in the world are blocked because of positives from anti-virus software. Malware delivered via email attachments is one of the key transport mechanisms for intruders to get access to an IT network. One potential aspect of email security includes only downloading attachments when they are requested by the email recipient. Of course, this is good practice to save on satellite airtime, but is also important to reduce the number of unknown executable files coming on board a ship.

Marlink's ***SkyFile Mail*** solution includes Attachment Protection (see Marlink's "*Cyber Guard Solutions*" brochure).

Website and Content-Based Filtering

A firewall may be complemented by web filtering carried out at various different levels, using specific profiles and additional layers.

- *Category Filtering: Restricting user's web access by blocking certain categories such as undesirable content (i.e., drugs, racism or hacking) to non-productive activity (i.e,. games) to security threats (i.e,. P2P sharing and sites with known malware).*
- *Content Filtering: Blocking certain types of content to avoid download of potentially harmful files (e.g., EXE files).*
- *Filtering policies applicable to a vessel, or groups of users can be implemented. If an attempt is made to access a restricted website from a computer on-board a vessel where content filtering is enabled, the user will be blocked or redirected to a website where information about the policy violation is given.*
- *A combination of both category and content filtering systems is recommended as even white-listed categories might contain unwanted or unsecure types of content (tracking cookies, viruses or malicious software).*

*Marlink provides website category and content filtering as part of the following two Value-Added Services: **Data Manager** and **@SEAwebControl**™ (see Marlink's "Cyber Guard Solutions" brochure).*

System Back-Up and Resiliency

Although Secure Remote Access allows remote secure intervention on a PC, this risks causing excessive satellite airtime consumption. Therefore, for cases of malware infection and ransomware but also to protect against hardware failure, it is good IT practice to implement an automatic back up process to a physical secondary system on-board. Considering the remote aspect of ships, back-up systems enable operations to be restored right away, rather than waiting for a remote technician to intervene or even wait for back-up hard disks to be delivered and installed in port.

Marlink's ***KeepUp@Sea***™ IT platform includes an automatic back-up and restoration function (see Marlink's "*Cyber Guard Solutions*" brochure).

Update Management

Software updates are published frequently to include new features, but also to fix security vulnerabilities. Although software updates consume satellite bandwidth and take time, these should be performed regularly to avoid known vulnerabilities in outdated software being exploited by an attacker as a method of intrusion.

The WannaCry ransomware outbreak in May 2017 exploited a vulnerability in the SMB protocol for which Microsoft had released a patch two months before. Despite abundant media coverage, many systems were not updated and the NotPetya ransomware used the same vulnerability in June 2017 to again cause disruption on a large scale. The likely explanation for this is a lack of centralized awareness about deployed software versions across an organization. Specialized monitoring and reporting software allows a Fleet Manager to see an overview of the deployed software versions on all PCs in their fleet, identify vulnerable versions and launch updates remotely.

KeepUp@Sea™ includes version management of deployed software onboard (see Marlink's "*Cyber Guard Solutions*" brochure).

Network Infrastructure

Network Configuration

In addition to protecting against outside threats, to avoid infection spill-overs, it is also essential practice to isolate networks used for different purposes: the business critical Corporate Network should be clearly isolated from the potentially less

secure Crew Welfare Network. Marlink prevents cross-network access by either of the following two methods:

- *Virtual Routing and Forwarding Technology (VRF): Networks are delivered to separate termination points using dedicated VRF.*
- *Physically Split Local Area Networks (LAN): Networks are physically separated requiring separate cabling. Additional security settings can be applied to physical networks to prevent non-listed computers and systems from cross-connecting between networks.*

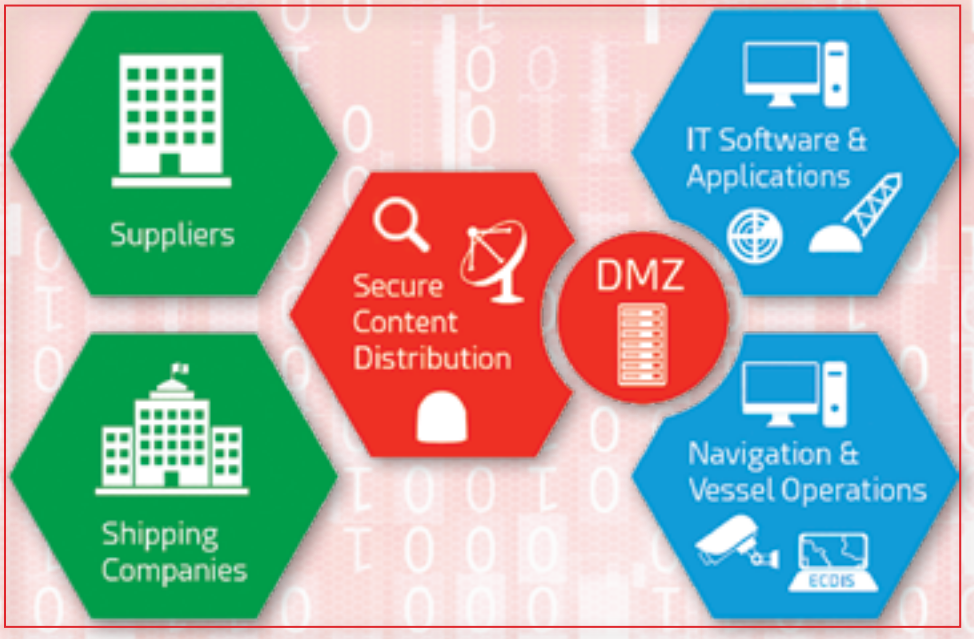


Figure 4. A DMZ-based network architecture to securely distribute content to critical bridge systems (e.g. Radar, ECDIS, ERP Systems)

Thanks to this implementation, since a Crew PC, smartphone or tablet cannot access the Corporate LAN, untargeted malware cannot spread from the Crew to the Corporate LAN. Moreover, this is a good defence against a targeted cross-network intrusion of the corporate network through a less secure network. However, such network separation can only act efficiently in combination with staff awareness: despite the separation of Crew and Corporate networks, a crew member could infect a Corporate PC by connecting an infected USB drive.

Marlink's XChange includes network isolation technology (see ***XChange*** and **Cisco** chapters in Marlink's "Cyber Guard Solutions" Brochure).

VPN Interconnect

To increase security against outside intrusion or eavesdropping when routing through the internet, an encryption protocol may be used to add another layer of security. However, an encryption method suitable for usage over satellite should be chosen, as some types of encryption are geared towards terrestrial usage and use extensive amounts of bandwidth.

Additionally, encryption for user authentication can also improve resilience.

The benefits of using a VPN are numerous. Essentially, using a pre-defined routing path along a public network, it enables a secure extension of an internal network to a remote location. This makes Corporate IT networks more coherent and easier to manage, by including the vessel into the same network as any shore office. Two types of VPN solutions are provided by Marlink:

- *HQ Interconnect: From the Marlink teleport gateway to the Customer HQ.*
- *End-to-end VPN: From the vessel via the Marlink teleport gateway to the Customer HQ.*

Secure Remote Access

There are rarely IT specialists on board a ship, so more complex software based issues may require a technician to visit, which is costly and operationally difficult to manage. It is becoming more common for IT management of on-board PC networks to be performed remotely. However, rather than using insecure means such as a Public IP, a Secure Remote Access Tool over a VPN with a single point of access should be used. Considering that for additional security Marlink is operating a private network, such tools need to be compatible with **Network Address Translation** (*NAT*) on multiple levels.

Thanks to such ***Secure Remote Access Tools***, all PCs can be accessed from shore to fix specific issues or deploy updates. For instance, should a PC require a clean install of Windows, the process can be managed remotely, without the need for any on-board intervention. Similarly, ransomware could be remedied by a reset to an earlier backup.

XChange includes the **Universal Remote Access** (*URA*) feature providing secure remote access to all on-board devices connected to it. Moreover, the ***KeepUp@Sea***™ platform allows to remotely initiate the reset to an earlier back-up or software reinstall (see Marlink's "***Cyber Guard Solutions***" brochure).

Next Generation Cyber Security Measures

Cyber Detection

While signature-based cyber solutions (anti-virus, firewall, content filtering) and a secure network infrastructure (VPN, LAN separation) are effective against untargeted attacks, in order to provide efficient defence against targeted attacks such as APTs, a cyber detection solution should be implemented.

Typically, network probes would be placed in several parts of the infrastructure performing the following functions:

- *Deep Packet Inspection (DPI): Rather than performing filtering based on a packet's meta data, a DPI system will also analyze the payload of the packet.*
- *Intrusion Prevention System (IPS): Detects common patterns of cyber-attacks (e.g., large amounts of data extracted to unusual destinations) and corporate policy violations (e.g., detection of applications which should be blocked, e.g., BitTorrent).*
- *Sandboxing: A controlled environment to test suspicious files (e.g. attachments from unknown senders) to examine for malicious behavior; effective in case of zero-day attacks.*
- *Traffic Pattern Monitoring: Raises alerts in case of deviations from usual weekly and monthly traffic patterns (e.g., applications, volume); although more prone to false alerting than the previous three functions, it is an additional source to detect abnormalities.*

Incident Alerting and Response

Alerts generated from these various systems are aggregated and assessed by a **Security Information and Event Management** (*SIEM*) system. In addition to controlling a number of automated countermeasures (*e.g.*, quarantine suspicious machines), this information is displayed in a dashboard overview to be exploited either by the Corporate Network Administrator or a third-party 24/7 **Security Operations Center** (*SOC*).

Based on their training and experience, the human analysts choose anomalies to investigate further and in case of a confirmed attack perform the follow-up actions such as:

1. **Isolate infected assets**
2. **Remediation (e.g., cleaning)**
3. **Investigate incident to determine source of attack**
4. **Improve protection systems (e.g., add attacker's DNS domain to central firewall DNS blacklist)**
5. **Raise staff awareness (training courses, bulletins)**

Rather than implementing a dedicated Cyber Detection system and operating an in-house SOC, a shipping company may achieve economies of scale by using a central system and third-party SOC service implemented at the Satellite Communication Provider's gateway.

Secure Content Distribution

Even if internet is becoming a commodity on vessels, it is recommended to block direct access to navigation assets. Smart and secure content distribution services already today — acting as DMZ between assets and the internet — can eliminate risks of attacks and infection, as shown in *Figure 4*.

Not only all of these critical systems to vessel operations (ECDIS, ERP Systems, etc) should be managed in different network groups, software updates and new content (*e.g.*, new training material, navigation charts) shall be transferred indirectly to vessels using such DMZ principles, performing integrity verification / sandboxing of files while preventing an open and direct access to hackers to these assets.

Consulting Services

As cyber security is a highly specialized and fast moving sector, many shipping operator's internal IT departments may lack the expertise to stay on top of the latest developments. It may be advisable to seek outside expertise for the following tasks:

- *Regular Penetration Tests (Pen Test): A white hat attacker attempts to perform an unauthorized intrusion into the tested system without knowing any details about its architecture. The objective is to identify vulnerabilities that could be exploited by malicious attackers, such as flaws in services and applications, misconfiguration or risky end-user behavior.*
- *Forensics / Response to Authorities: Many public bodies such as GDPR not only mandate companies to inform them in case of cyber incidents but also to analyze which data has been extracted. As attackers often try to hide their trail, this is very time consuming and requires specialized IT forensics skills (analyze network logs, recover deleted and hidden files, seize RAM data). Moreover, there are several provisions to comply with for the data to be legally admissible in court.*
- *External Audit of Back-up Systems and Contingency Procedures: It is advisable to ask independent security experts to review the secondary systems and cyber-attack response procedures.*

www.marlink.com

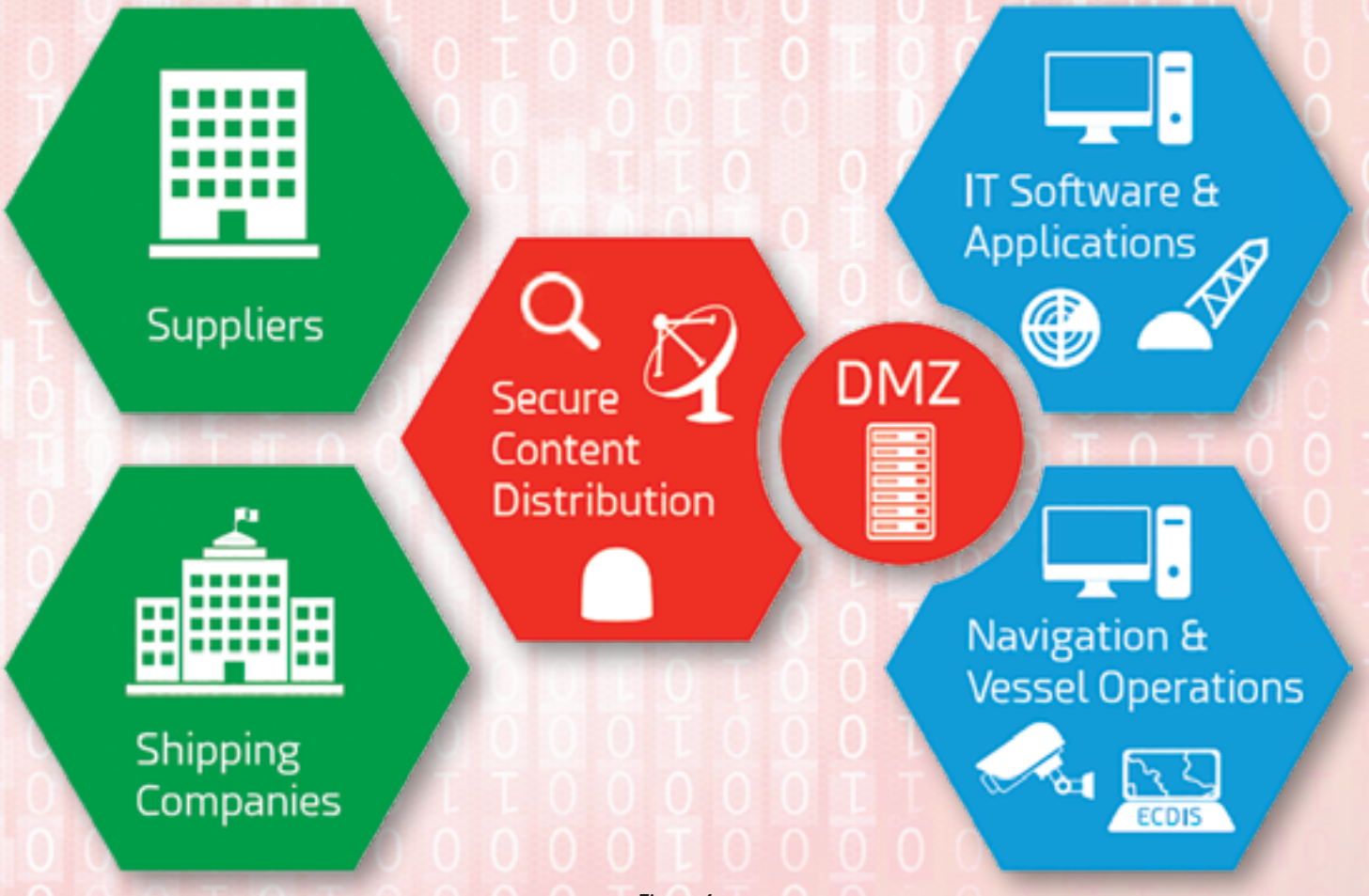


Figure 4.

Abbreviations

APT: Advanced Persistent Threat

BYOD: Bring Your Own Device

DPI: Deep Packet Inspection

DMZ: Demilitarized Zone

DoS: Denial of Service

ECDIS: Electronic Chart Display and Information System

ERP: Enterprise Resource Planning Software

HTS: High Throughput Satellite

IoT: Internet of Things

LAN: Local Area Network

MRV: Monitoring, Reporting and Verification (EU Directive)

NAT: Network Address Translation

NOAD: Notice of Notice Of Arrival and Departure

RAT: Remote Access Tool

***ROV**: Remotely Operated Vehicle*

SIEM: Security Information and Event Management

SMB: Server Message Block

TEU: Twenty-Foot Equivalent Unit (international cargo size unit)

SOC: Security Operations Center

VLAN: Virtual LAN

VPN: Virtual Private Network

VRF: Virtual Routing and Forwarding Technology

Definitions

Advanced Persistent Threat: A sophisticated attack designed to be difficult to detect, remaining undetected in a network for a long time.

Black Hat Hacker: A hacker exploiting computer security for personal gain or because of maliciousness.

Demilitarized Zone: A network architecture which only allows external access to certain hosts inside the DMZ (e.g. web services, email server) while the other hosts in the organization are not externally reachable.

Meta Data: A summary of a dataset (e.g. title, file type, size, modification date, sender, destination).

Payload: The part of the network packet containing the intended message, i.e.; excluding the Meta Data.

HELO: A command in an email message containing information about the sender which can be used to filter spam.
White Hat Hacker: An ethical computer security expert who will use information on vulnerabilities to improve the security of an organization's information systems.

Annex 1 - Institute Cyber-attack Exclusion Clause (CL380) (CL 380, 10/11/03) 1.1.

Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program malicious code, computer virus or process or any other electronic system.

1.2. Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software program or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

BROADCAST INNOVATION...

... in military environments

By David Edwards, Product Manager, Vislink

People on the edge of the SATCOM world have often viewed the industry as static and slow to change; however, when are at the heart of the action, the evolution and transformation that is occurring at an ever-increasing pace can readily be seen.

The military and public safety markets can reap numerous benefits by drawing on the fast-paced innovation occurring in the commercial video broadcast market. This market segment has decades of experience in providing high-quality, low-latency imaging within a commercial budget.

In an era where **Commercial Off the Shelf** (***COTS***) solutions are increasingly being viewed as excellent value, advances in live broadcast SATCOM technology should certainly be of immediate interest to the military and emergency services satellite community.

For more than 25 years, **Vislink Technologies** has been a global leader in the transmission of ultra-low latency, high-end full motion video, utilizing a portfolio of proven satellite ground terminals specifically designed to transmit superb quality video in the most demanding and extreme environments.

Tracking Innovation

As an industry that relies on RF technology, SATCOM is starting to integrate with the ever-increasing IP-connected world.

The rapid increase in **High Throughput Satellite** (***HTS***) and Ka-band capacity is testament to that fact, with some predictions suggesting a doubling of capacity by the early 2020s.

There are major ongoing innovations in what has been termed "New Space" — **Low Earth-Orbit** (***LEO***) constellations that promise connectivity for locations that have always been a challenge for any form of reliable communication — offering dependable, high bandwidth infrastructure to developing nations, polar regions and marine services.

As more and more bandwidth capacity becomes available to military and public safety concerns, there will be a swift increase in user requests for broadcast quality, **Full Motion Video** (***FMV***) with actionable intelligence to increased situational awareness with low end-to-end latency to support accurate decision making.

Vislink's AirPro75Ka terminal in operation in Cairo, Egypt.

Vislink's AirPro75Ka terminal in operation in Sydney, Australia

Vislink Technologies is seeing transition and growth driven by users' desires to experience more and better visual communication systems. The advent of 4K UHD resolution video is impacting TV broadcast services and could have a similar, significant influence in the military and public safety environment, as well. Forward-looking statements of intent indicate that 2019 is likely to bring an increased demand for payload capacity and antenna systems that fulfill the link budget requirements of higher bandwidth transmissions.

The Broadcast Downlink

Live broadcast-over-satellite continues to be driven by cost-per-bit economics. Uplink operators are keen to reduce OPEX costs by investing in greater transmission efficiency.

Over the past several months, Vislink Technologies has been actively innovating to deliver that next step-change for uplinkers. This includes a suite of new satellite products in the form of the ***DVE 6100*** satellite encoder and ***IRD 6200*** satellite decoder which, together, provide end-to-end video connectivity using new HEVC compression and DVB-S2X satellite modulation.

When combined, these two technologies offer as much as a 50 percent reduction in satellite bandwidth when compared to older technology while maintaining equivalent quality video. For HD resolutions, the reduction in satellite bandwidth leasing and satellite bandwidth costs associated with this new equipment can result in a return on investment within a few months.

For operations that are dealing in 4K quality video, this new technology is the key that makes a service launch a practical reality. It is not just the search for OPEX cost reduction where the new HEVC and DVB-S2X technology finds a home. With increased efficiency in use of valuable bandwidth, operators now have access to more payload capacity without transmission cost increases.

While this product offering was initially offered to commercial video broadcast applications, it offers the reliability and quality needed for MILSATCOM operations. The Vislink DVE encoder and IRD decoder products have developed a strong following in the SATCOM world by mixing high-quality video compression with low-latency processing — highly valuable when a communication channel inevitably incorporates a geostationary round-trip. The small form-factor and integrated HPA control capability delivers valuable space-savings in increasingly sophisticated uplink vehicles or for fly-away applications that must comply with airline baggage regulations.

Bringing IP to SATCOM

Where does the IP world come in to the picture? In short, everywhere! IP internet connectivity between equipment is preferred as it leads to common interfacing and lower cost installations — and for mobile operations, a valuable reduction in weight. New standards for video interconnection are now available.

In the past year, we have seen the advent of SMPTE 2110 as a mechanism to transport baseband video-over-IP, with the first, all-IP video production trucks brought into service in the commercial broadcast sector — 2019 appears to be the year that many SATCOM operators will follow suit and finally transition to all-IP internal connectivity.

IP is increasingly critical on the external communication side, as well. In today's hyper-connected world, it is unrealistic to expect remote and mobile teams to be beyond reach of IT network connectivity. This year, Vislink Technologies has been responding to this need with a brand-new satellite terminal, with IP at its heart, the ***AirPro75Ka*** antenna.

The antenna offers high-rate IP connectivity that allows ad-hoc connection to the **Eutelsat *Konnect*** (formally *Tooway*) network. The AirPro75Ka terminal is a single-click device that automatically finds the satellite and provides users on-air connectivity in a matter of minutes. The antenna system uses pay-as-you-go data bundles for general connectivity and file transfer in conjunction with the ability to book uncontended satellite time to enable live, reliable transmission.

The AirPro75Ka antenna has many fans in the SATCOM industry as it addresses the need of operators to work in newer, smarter ways, with better use of budgets. The Ka-band IP connectivity provides improved flexibility, better price-per-bit and a physically smaller antenna package than traditional Ku-band terminals. This allows it to be installed as a companion antenna on existing C2 platforms or as a sole transmission device on new smaller vehicles.

Having tested the market response to the device this year through data transmission trials — including on environmentally friendly, electric vehicles, customers like the robust, yet affordable, construction as well as the concept that Vislink is trialling the sale of the antenna and air-time as combined package. These features will enable a quick-and-easy transition to the IP-connected world. The company's expectation is to have bring this solution to the mass-market in the coming year.

With such a heavy investment and commitment within the SATCOM industry, Vislink is re-affirming its long-standing connection with the satellite community. Users taking delivery of new satellite products in 2019 will also notice improved user interfaces as well as a fresh, modern, Vislink Technologies logo that reflects the dawning of a new IP-centric satellite world.

www.vislink.com
twitter.com/vislink

David Edwards started his career as a design engineer working on the first generation of Direct Conversion satellite demodulators for Digital TV - realizing an all-silicon solution that enabled a shift in technology price points and reduction in complexity.

With a background in designing link budgets for many of the world's leading broadcasters' satellite networks, Edwards understands the balance and trade-off of video quality, network reliability and operational cost that operators require to create a financially successful satellite-based business.

SATELLITE INNOVATION

2019 SILICON VALLEY

THE MEETING PLACE FOR SATELLITE EXECUTIVES AND PROFESSIONALS

75
EXHIBITORS / SPONSORS

125
SPEAKERS

800
ATTENDEES

SATINNOVATION.COM

The ***Satellite Innovation*** Conference has become the premier meeting place for innovative Satellite Executives and Professionals. Subject-matter experts focus on imminent changes and the market forces that will propel their implementation. Meet the market leaders and pioneers of the shifting landscape of our industry.

October 8th - 10th, 2019