GMC

Linked in YouTube

November/December 2021

Global Military COMMUNICATIONS

Challenges in US border security

Cyber security

Q&A ND SATCOM

Space debris

Front cover photo courtesy of oksana.perkins / Shutterstock

Sign-up now for your **FREE** digital copy...visit www.globalmilitarycommunications.com

SATELLITE Evolution Group

Global Military Communications is part of the Satellite Evolution Group portfolio

FlexAir & FlexMove for Government

When Moments Matter

FlexAir and FlexMove are complete, end-to-end managed service solutions, specifically designed to provide high data-rate connectivity to global teams engaged in land mobile, littoral, and airborne operations.

Intelsat gives teams the connectivity vital for mission success.

IMAGINE HERE™

Learn more at
flexmovegov.com

INTELSAT General

Editor
Amy Saunders
amy.saunders@dsairpublications.com

News & Social Media Editor
Laurence Russell
Laurence@dsairpublications.com

Marketing and Business Development
Belinda Bradford
belinda@dsairpublications.com

Circulation Manager
Elizabeth George

Production
production@dsairpublications.com

Publisher
Jill Durfee
jill.durfee@dsairpublications.com

Publishing Director
Richard Hooper
richard@dsairpublications.com

Managing Director
David Shortland
david@dsairpublications.com

No part of this publication may be transmitted, reproduced or electronically stored without the written permission from the publisher.

DS Air Publications does not give any warranty as to the content of the material appearing in the magazine, its accuracy, timeliness or fitness for any particular purpose. DS Air Publications disclaims all responsibility for any damages or losses in the use and dissemination of the information.

All editorial contents
Copyright © 2021 DS Air Publications
All rights reserved

DS Air Publications
1 Langhurstwood Road
Horsham
West Sussex, RH12 4QD
United Kingdom
T: +44 1403 273973
F: +44 1403 273972
admin@dsairpublications.com
www.globalmilitarycommunications.com

GMC

Trusted Computing Group - page 16

Contents

If you would like to supply information for future issues of GMC please contact Amy Saunders, Editor.

Photo courtesy of Space Data Association

Milrem Robotics led iMUGS consortium demonstrates deployment of unmanned systems

The iMUGS Consortium, in charge of a euro 32.6 million project developing the European standard unmanned ground system (UGS), demonstrated how defence forces can use tactical 4G/5G communications networks and UGS' equipped with ISR and signal intelligence payloads, jammers, acoustic sensors, and various other technology to conduct missions.

The demonstration that was performed in September in Latvia, was led by LMT, a member of the integrated Modular Unmanned Ground System (iMUGS) consortium, with the support of the project coordinator Milrem Robotics and featured an ensemble of different technology.

Latvian National Armed Forces used two Milrem Robotics' THeMIS Unmanned Ground Vehicles (UGV) during two scenarios to display the benefits of teaming up manned units with unmanned systems.

One THeMIS UGV was equipped with an Intelligence, surveillance, and reconnaissance (ISR) payload, Signal Intelligence antenna (SIGINT) provided by The Electronic Communications Office of Latvia, Rheinmetall's Rapid Obscuring System (ROSY) Smoke Grenade Launcher, Bittium's Vehicular Software Defined Radios (Tough SDR Vehicular), and FN Herstal's deFNder Light Remote Weapon Station (RWS). The RWS integration was part of the demonstration, but not of the iMUGS project itself.

The second THeMIS, used as a mule for transporting the squad's equipment, was equipped with Rantelon's Improvised Explosive Device (IED) Jammer and Bittium's Tough SDR Vehicular.

The units and UGVs used Bittium's tactical communication network TAC WIN combined with LMT's commercial 4G and a tactical 5G-SA bubble provided by Bittium and Cumucore.

In addition, Krauss-Maffei Wegmann's (KMW) Dingo infantry mobility vehicle was used as the command centre from where UGVs were operated in Line of Sight (LOS) and Beyond the Line of Sight (BLOS) mode using Bittium's SDR radios and to where the ISR and Signal Intelligence sensor feed was relayed and incorporated into LMT's Battle Management System Viedsargs.

"The displayed scenarios showed that unmanned systems, enhanced with innovative communication systems and various defence technology, can be used for collecting and sharing tactical information, improve situational awareness, decrease troops physical load, and increase force protection," explained Kuldar Väärsi, CEO of Milrem Robotics.

''For the first time ever, in a special network, a tactical network was connected with a stand-alone 5G network. This allowed communication between units and robots, as well as collecting information from sensors and placing this information into LMT's Battle Management System 'Viedsargs', said Ingmars Pukis, Vice President and Member of the Management Board of LMT.

Additional equipment used in the demonstration included: SRC Brasa's NATRIX UGV used for CASEVAC, high-speed First-Person View drone, Vertical Take-off, and Landing UAV STAR, and a gunshot detection and source recognition audio sensor by Riga Technical University (RTU).

The iMUGS project was launched in 2020 to develop a modular, cyber secure and scalable architecture for hybrid manned-unmanned systems. Its goal is to standardize a Europe-wide ecosystem for ground platforms, command, control and communication equipment, sensors, payloads, and algorithms. Addressed operational challenges include enhanced interoperability, increased situational awareness and faster decision-making.

The system will use an existing UGV – Milrem Robotics' THeMIS – and a specific list of payloads.

The project's progress is displayed during six demonstrations. "So far Milrem Robotics and LMT Innovations have set the bar very high. Which means we have some great things to wait for as the main results of the iMUGS projects are yet to be seen," said Martin Jõesaar from the Estonian Center for Defence Investments, the representative of the participating Member States in the iMUGS Project. The next demonstration will take place in Q1 of 2022 in Finland.

iMUGS is a cooperation between 13 parties: Milrem Robotics (project coordinator), Bittium, Diehl Defence, dotOcean, GMV Aerospace and Defence, Insta Advance, Krauss-Maffei Wegmann, Latvijas Mobilais Telefons (LMT), NEXTER Systems, Royal Military Academy of Belgium, Safran Electronics & Defense, Sol.One and Talgen Cybersecurity. **GMC**

Photo courtesy of integrated Modular Unmanned Ground System (iMUGS) consortium

Marlink to provide satellite connectivity solution to Irish Defence Forces

Marlink, the leading provider of smart network solutions, has been awarded the contract to equip the Irish Defence Forces with a secure and reliable satellite connectivity solution for their global military missions across land and sea.

The agreement will see the country's defence forces concentrate their communications infrastructure with dedicated expertise, consolidating traffic into Marlink's global smart hybrid network, combining relevant connectivity carriers including VSAT and L-band networks.

Marlink will enable connectivity for the Irish Defence Forces via numerous designated sites including fixed operational deployments in Lebanon and Syria as well as mobile troop deployments in Europe and Africa.

The Irish Defence Forces require connectivity via secure satellite backhaul on a 24/7 basis. Systems to be deployed include high throughput VSAT between command centres and remote locations and mobile satcom solutions for military personnel.

"The Irish Defence Forces requires a communications partner with a network that is agile and also highly scalable in both setup and operations and most importantly, the provider must support our requirements globally," said Comd John Kenny OIC Comms Section, DFHQ, Irish Defence Forces.

"Meeting the needs for military connectivity is always a challenge we look forward to, as it allows us to demonstrate our unique capabilities to provide a reliable, secure service in support of command and operational activities," says Alexandre DeLuca, President, Enterprise, Marlink. "The Irish Defence Forces recognised that as an agnostic provider of connectivity, we could assemble a smart network solution that keeps its people and assets connected anywhere, anytime." **GMC**

Photo courtesy of Marlink

Photo courtesy oksana.perkins / Shutterstock

Challenges in US border security

The world has changed immensely in the last couple of years, with the COVID-19 pandemic, huge changes in everyday life for billions of the world's inhabitants, and the knock-on effect of changing leadership ideologies causing massive disruption far and wide. The effects on border security around the world cannot be understated, with the US in particular, suffering severe impact.

Amy Saunders, Editor, Global Military Communications

Border security is of the utmost importance to every country across the world, with government agencies tasked with protecting borders to monitor and regulate the movement of people animals and goods across borders on land, in the air, and at sea. The concept of borders are ancient, but slowly they have, to some extent, been breaking down in recent years, as the world becomes more globalized and digitized than ever before.

In the US, however, there is no doubt that borders are borders. The United States Border Patrol is the armed and uniformed federal police that secures all US borders, detecting and preventing undocumented migrants, terrorists, weapons, goods, and people from entering the country illegally. With tens of thousands of agents and costing billions to support annually (reportedly US$3.81 billion in 2017), the Border Patrol means business. How well it's actually getting the job done amid challenging circumstances and drastic changes in ruling ideology in recent years, is another matter.

Southern border crisis wages on

Whatever your politics, it's been a tough year for President Joe Biden, who turns 79 this month. Faced with droughts, wildfires, climate activism, increased political tensions with certain factions, and the first global pandemic in modern times, he's also facing severe border control difficulties.

The United States Border Patrol recorded almost 1.7 million migrant apprehensions at the southern border in the last 12 months alone, the highest number ever on record. September 2021 saw 192,000 apprehensions, compared with 57,600 in September 2020 and 52,500 in September 2019.

Back in 2000, the year of the previous migrant apprehension record, the flow of migrants was very different – far fewer people were caught, and the Department of Homeland Security estimates that there were almost four million illegal border crossings that year, with 1,643,679 apprehensions. Some 98 percent were from Mexico, mostly single men.

In 2021, the number of families and children trying to enter through the southern border has boomed, with many turning themselves into Border Patrol to claim asylum or other protections.

Some 40 percent originated from Central America this year, with a growing number coming from South America, the Caribbean and Africa. It's been widely reported that the COVID-19 pandemic has exacerbated gang violence in the world's poorest regions, prompting increasing numbers making attempts to escape.

"I've never seen it as bad as what it is right now," reports Brandon Judd, President of the Union that represents Border Patrol agents. Agents spend hours handling paperwork for migrants who are allowed into the country to ask for asylum, distracting them from trying to stop smugglers from bringing drugs and other contraband into the US. "We just don't have the manpower and resources to do what we need to do to both detect and apprehend everything that's crossing the border."

A new Customer and Border Protection lead came one step closer to confirmation with a hearing in October; Tuscon Police

Chief Chris Magnus informed senators that he would seek to balance border security with humane treatment of migrants. "First and foremost, we need to enforce the law. And secondly, we need to have a process that's humane and efficient," said Magnus. "How we engage with the public - even the public we may be arresting - is what defines us as professionals. And this is something we have a moral obligation to do." The unusual choice to lead the Border Patrol could prove invaluable in battening down the hatches at the southern border, should he be empowered in time.

COVID-19 strikes at Biden's borders

Further complicating the influence of the pandemic on national security, back in September, President Biden announced that federal workers (and private sector workers in businesses with more than 100 employees) must either be vaccinated or take a weekly COVID-19 test, in a move expected to effect more than 100 million Americans.

"We've been patient, but our patience is wearing thin and your refusal has cost all of us," said President Biden in a statement. "This is not about freedom or personal choice. It's about protecting yourself and those around you."

The new requirements have angered a great many Americans, who claim that they are damaging to business and unconstitutional.

Indeed, Arizona's Attorney General has filed a request for a temporary restraining order to stop the Biden administration implementing a controversial vaccine requirement as a lawsuit filed last month moves forward.

"Once a vaccine has been administered, it can never be undone," said Attorney General Mark Brnovich. "The COVID-19 vaccine mandate is one of the greatest infringements upon individual liberty, federalism, and the separation of powers by any administration in our country's history."

The deadline for the first vaccine dose has already passed, with all relevant personnel requiring full vaccination by 22nd November. One of Attorney General Mark Brnovich's complaints is that only the Pfizer vaccine has been approved by the FDA to date, limiting uptake rates in the country. Moreover, market reports state that 85 percent of businesses expect the vaccine requirements to make it harder to retain employees, and 89 percent expect some employees to quit.

In November, a group of 62 House Republicans led by Rep Elise Stefanik, R-NY and Rep Brian Babin, R-Texas, warned President Biden that the vaccine mandates could cause the loss of thousands of Border Patrol agents, exacerbating the ongoing crisis at the southern border.

"We have serious concerns about your vaccine mandate for Federal employees and how it will impact the already understaffed and overworked United States Border Patrol and our overall national security," said the Republicans in a letter to President Biden, obtained by Fox News.

The Republican group stated in their letter that conditions might deteriorate further given the vaccine mandate. "Despite these staffing issues, thousands of Border Patrol agents are at risk of losing their jobs because of your ill-conceived policy," they argued. "This mandate is wholly incongruent with the principles of individual choice and medical freedom, puts families in our districts at risk of financial ruin, and threatens our national security by flooding our communities with undocumented, unvetted migrants."

They describe forcing mandates on Border Patrol agents at such a time, as "not only irresponsible, but is a dereliction of your duty as Commander-in-Chief."

The Republicans concluded that "…punishing these agents for their personal medical choices would constitute a full-frontal assault on our border agents and further reinforce your utter abandonment of our southern border." They have called to suspend the vaccine mandate for any first responder 'tasked with securing our border and addressing the ongoing border crisis.'

Former Border Patrol Chief Rodney Scott, who left his post involuntarily in August, shared his concerns with the Washington Examiner. He estimates that approximately 1,000 of the 19,000 Border Patrol agents "are probably going to get fired" because they won't get vaccinated, hurting Border Patrol's ability to defend its borders further.

A ticking clock

The future of border security in the US and the world at large is a tricky one to gauge. Certainly, more funds, more bodies and more solid plans are needed to ensure the safety of nations. Possibly even more walls. However, with the trend towards increasing digitization, border security forces may soon face an even bigger challenge, from adversaries they cannot see or physically touch. As with much of modern life, it's something of a ticking clock to see whether security forces will respond to changing realities early enough to stay ahead of the rapidly changing game. **GMC**

Low orbit satellite concept. Photo courtesy Shutterstock

How the US Intelligence Community is driving new security protocols in satcom

When you think about today's software-defined and AI-infused terrestrial networks, you could be forgiven for seeing RF traffic and networks as a little unsophisticated. Satellites have been in use since the 1950s, after all. Yet, as global governments' use of satcoms continues to diversify, and their reliance on data increases, the technology behind it has scaled up its capabilities accordingly – meaning present-day RF network architecture is anything but simplistic.

Bill Pryle, Government RF Consultant, ETL Systems

Satellite technology enables secure data transmission across vast areas of land and sea. It can be deployed quickly and operated remotely, without the need for massive investment or prior infrastructure on the ground. It's for these reasons that the technology has long provided vital communications capabilities to both the US Intelligence Community and Department of Defense (DoD): The two key customer groups I deal with.

Setting a new security standard

The need for new precautionary security measures came first from the Intelligence Community, who introduced a new mandate that any device connected to their network had to use secure protocols, namely SNMPv3 and HTTPS. The defense side followed suite, requesting secure communications protocols for any networked device operating at a government facility.

The new mandate was driven in part by a series of high-profile cyber-attacks: Russian attempts to impact the 2016 and 2020 US election results, for example. So, while RF devices in themselves aren't vulnerable to attack and wouldn't make particularly fruitful hacking targets, in the current climate, anything that touches the network must be doubly secure.

In the simplest terms, HTTPS (Hypertext Transfer Protocol Secure) is used for secure online communication and works by encrypting data in transit, safeguarding against eavesdropping and tampering. SNMPv3 (Simple Network Management Protocol Version 3) is an interoperable, standards-based protocol used for authorisation and access control.

Our recently released products carry additional features such as the option to disable unused protocols, password complexity enforcement and a restriction on the number of login attempts.

With a reach that extends far beyond the US, the Intelligence Community has long been one of the drivers advancing remote communications.

Take-up of products using the new secure protocols has been high and we're already seeing a trickle-down effect: While North America remains the largest market, our products are shipping worldwide.

We fully expect that commercial satellite operators will soon request the same enhanced network security and that worldwide adoption of the technology will increase exponentially.

The proliferation of data and increase in remote capabilities

Of course, data-security concerns aren't the only reason to invest in a more sophisticated, future-proof satcom infrastructure.

Satcom plays a vital role in military communications, meaning many advancements in the technology have been driven by forces' ever-growing data requirements. Just this year, we saw how the military's data demands heralded a movement to Ka-

Deploy High-Performance Ruggedized Intelligent BUCs Wherever the Action is.

Now with SNMPv3 & cyberhardening features.

Explore all **IBUC** models at TerrasatInc.com

band satcom with its higher frequencies, larger bandwidths and increased spectral efficiencies. As the rate at which our society generates and consumes data continues to surge, device capabilities must increase in parallel – not just to transmit that data, but also to process it into usable information. Securely, and in real time.

Another factor driving the demand for satcom – and the uptake of secure RF technology – is the increase in remote capabilities, such as secure video applications that allow groups to communicate from separate locations. Demand for remote methods of communicating has only increased in the wake of the COVID-19 pandemic, and the challenge for organisations now is to enable remote connectivity at scale and without compromising security.

Let's remember, too, that the ground stations where RF signals are received, converted, and redirected are growing in complexity, with the majority now remotely operated and controlled via Ethernet – another key driver in the widespread adoption of secure protocols like SNMPv3 and HTTPS.

LEO satellites and the future of RF connectivity

There's another big reason why our remote capabilities are set to increase, and that's the advent of LEO satellites: huge 'constellations' of low Earth orbit satellites, usually at altitudes ranging from about 700 to 3,000 km above the Earth's surface. Since the satellites orbit relatively close to the Earth, with a limited field of view from the on-board antennas, large numbers are needed to achieve global coverage. Accordingly, more tracking antennas are needed on the ground to ensure seamless connection between satellites.

We've all read about the likes of OneWeb, LeoSat and SpaceX: Next-generation tech businesses clamouring to deliver low-latency, high-speed broadband worldwide. But as well as helping the world get closer to 100 percent Internet access, LEO constellations can also offer 100 percent worldwide surveillance and imaging coverage. The US Department of Defence (DoD) has already contracted Elon Musk's SpaceX Corporation to develop a prototype rocket propulsion system and has also already started a project using LEO for communication purposes.

In a world where we're all more connected than ever, satellites continue to play a vital role in global intelligence and defense.

As remote operations become the norm, and the RF ecosystem grows in size and complexity, the security of our communications is paramount. We expect enhanced security features, such as HTTPS and SNMPv3 protocols, to become more and more widely used. **GMC**

LEO IOT network. Photo courtesy iStock

MISSION MICROWAVE

THE NEW SHAPE OF SOLID STATE

X-, Ku-, and Ka-Band GaN BUCs
and SSPA's from 12 to 400 Watts

CONTACT US

6060 PHYLLIS DRIVE, CYPRESS, CA 90630

(951) 893-4925 | SALES@MISSIONMICROWAVE.COM

Alexander Mueller-Gastell, CEO of ND SATCOM

GMC Q&A

Pushing the envelope of durability and performance

Following the announcement of ND SATCOM's new FlyAway terminal, the company is exhibiting the product to show off its adaptability across bands and applications. Alexander Mueller-Gastell, CEO of ND SATCOM, walks us through the new terminal and the logic that went into its design, and how the company plans to build on its success.

Laurence Russell, Assistant Editor, Satellite Evolution Group

Question: How has ND SATCOM responded to the digitization boom under the pandemic?
Alexander Mueller-Gastell: Given ND SATCOM's global presence, we already had strong use of digital technology before the pandemic. One area we did adapt was to create an online training platform for any clients who sought this option, with a secure video classroom interface and actual access to hardware/software.

Question: ND SATCOM recently introduced the multi-band FlyAway terminal MFT 1500 and presented it live at CABSAT. Could you tell us a bit about it?
Alexander Mueller-Gastell: The FlyAway terminal is a 'made in Germany' product that pushes the envelope of durability and performance in wide-ranging environmental conditions. Our expertise gained over 20 years in this industry has been incorporated in its design and construction. It is a rapidly deployable terminal that can be loaded into TULBs and used in many civil and military frequency bands.

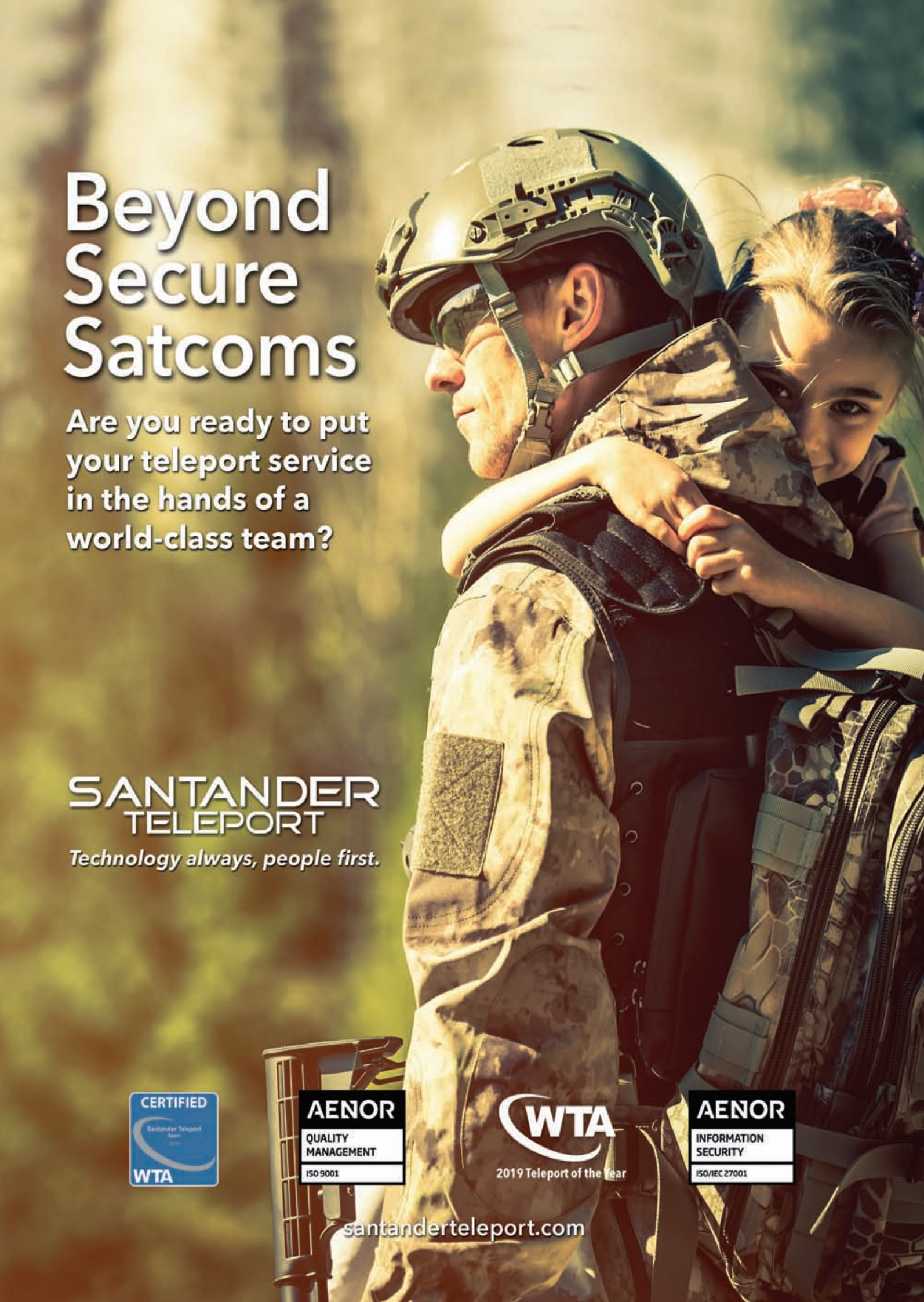
We combine 'field usability' benefits, such as easy set-up and dismantling, with the robustness of a deployable ground station, which is unique in the current market. Furthermore, the components are specifically adapted to our SKYWAN 5G modem, and the requirements for climate resilience are reflected in the new software release, which includes ACM (adaptive coding and modulation).

Question: What were the challenges involved in the terminal's development?
Alexander Mueller-Gastell: Optimization led us to bundle our capabilities through integrated systems that include core ND SATCOM products as components - such as our SKYWAN 5G modem here. Usability is always a priority, and we considered our solutions' user-friendliness and 'field usability' upfront in the design phase. In addition to focusing on and achieving outstanding performance parameters, this solution met military grade standards through our commitment to very high levels of robustness and resilience.

In addressing flexibility and customization, we adopted a modular component approach to creating a terminal product family. Our multi-prong approach to solving challenges in providing superior solutions has firmly established our reputation among customers.

Question: When do you hope to have it available on the market, and what

SKYWAN 5G modem. Photo courtesy of ND SATCOM


Beyond Secure Satcoms
Are you ready to put your teleport service in the hands of a world-class team?
SANTANDER TELEPORT
Technology always, people first.
CERTIFIED
WTA
AENOR
QUALITY MANAGEMENT
ISO 9001
WTA
2019 Teleport of the Year
AENOR
INFORMATION SECURITY
ISO/IEC 27001
santanderteleport.com

are your expectations for the product launch?
Alexander Mueller-Gastell: The FlyAway terminal was presented at CABSAT as a non-motorized version initially designed for Ku-band capability. This solution will be market-ready in 2022. The X- and Ka-band-capable versions are in the pipeline, as is a motorized version.

Question: Reliability is often the golden ticket in communications. How does ND SATCOM approach that goal?
Alexander Mueller-Gastell: ND SATCOM has been a reliable partner for satellite communications with a proven track record for over 20 years. With our value proposition of installing reliability, we have been providing customers reliable solutions with high availability and outstanding performance, complimented by highly intuitive interfaces and a well thought out logistics concept. By marrying innovation, performance, and dependability throughout our portfolio, customers trust the substance and quality that our brand represents.

Question: The accessibility of hardware is a strong goal for developers too, is that a similar priority?
Alexander Mueller-Gastell: Hardware accessibility in terms of usability and streamlined processes for allowing customers to get up and running are indeed integral to our development as we continue to grow and innovate as a company. The FLYAWAY's ease of deployment and dismantling reflect this.

Question: What else is ND SATCOM working on these days?
Alexander Mueller-Gastell: This new FlyAway terminal is the cornerstone of a complete family of deployable ground stations. In the future, we will increase performance through modularity by using up to 2.4m antennas. The basic concept will always be the same. Future plans beyond a motorised version include an integrated ACU (antenna control unit) in SKYWAN.

In addition, ND SATCOM is developing together with a partner an AIRBORNE SATCOM solution for rotorcraft based on the SKYWAN modem platform in order to expand its position in the military SATCOM market. **GMC**

ND SATCOM MFT 1500 Terminal. Photo courtesy ND SATCOM

Protect Your
Earth Station Antennas
From Ice, Snow, Rain, and more

WALTON DE-ICE

Antenna De-Ice Systems:

- **HOT AIR**
- **Ice Quake**
- **Snow Shield**
- **Portable Radome**

Walton Advantages:

- Uniform surface heating
  - Minimizes reflector distortion loss
  - Maximizes accuracy
- Most powerful and cost-effective system on the market
- 40+ years field-proven leadership
- 24/7/365 Support & Field Services

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

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

Keeping military satellite communications secure

With the threat of cyberattack increasing at astonishing rates in recent years, priorities must shift to protect one of the military's most critical assets. Satellites have become more vulnerable as Earth station access points have rapidly grown, rendering astonishing amounts of secure data open to attack.

Thorsten Stremlau, Trusted Computing Group (TCG) Marketing Work Group Chair

There is no doubt that cyber warfare is increasing, with recent research finding that 80 percent of companies have experienced at least one firmware attack in the past two years. Despite this, just 29 percent of their security budgets are allocated to protect firmware. As cyber-attacks become increasingly frequent and sophisticated, securing this must be high on the agenda for organizations. This is especially true for those in the defence sector, who are often a priority target for hackers looking to extract sensitive data and information. The rise of satellites being used in military and government operations has taken the risks to a new high level, as space-based assets are more difficult to protect due to the size, scope, and number of Earth station access points.

The challenge is that specialized electronic communications are rooted in tradition and as such, are often developed in a proprietary way. This makes it difficult to establish best practice security standards and specifications that protect stakeholders across the entire defence ecosystem. Military security has particularly unique considerations, but the implementation of well-tested, established technologies will drive forward secure military communications on a global scale.

Thorsten Stremlau, Trusted Computing Group (TCG) Marketing Work Group Chair

The role of satellite in the military

Satellite technology now plays a key role in military communications and is used for a range of purposes, including gathering intelligence and carrying out surveillance. Satellites are used in ongoing military conflicts or tense situations, as well as for navigation and logistical purposes as they can flag movements or redeployments without needing to have troops physically on the ground. We can only imagine the highly

Trusted computing architectures, specifications and standards can significantly enhance the security of global military communications. Photo courtesy TCG

SPACEBRIDGE

ALL THINGS CONNECTED

CONNECTING PEOPLE TO THEIR MISSIONS

Government & Military | IIoT, ATM, SCADA, Oil & Gas | HTS Broadband Consumer & Enterprise | SATCOM On The Move | Cellular Backhaul | Managed Services

For over 30 years, SpaceBridge has striven to eliminate the global digital divide as an innovator, leader and trusted provider of services and solutions that keep people connected to their missions, everywhere.

We live on the cutting edge of what is possible, challenging ourselves to adapt with our ever-changing world and deliver ultra-reliable, high-performance GEO and NGSO Extreme Broadband Gateways, VSAT Terminals, Modems, and Services for mission critical applications.

As we venture into the future, we invite you to join us in our mission. Connect with us at spacebridge.com and learn how you can achieve greater connectivity.

ALL THINGS CONNECTED

spacebridge.com | info@spacebridge.com | +1.514.420.0045

APAC | USA | CANADA | LATAM | BRAZIL | EMEA

sensitive data that is communicated back down to Earth and used to inform military operations, so it is no surprise that space-based assets are now a prime target for hackers looking to compromise vulnerable information. If this data was to fall into the wrong hands, the consequences would be severe.

Alongside the advancement of satellite technology, the sophistication of cyber-attacks has also developed. We have seen several attacks that have targeted deferral government networks and organizations, such as the attack on SolarWinds last year, where the hackers remained undetected for months. This means that not only do hackers have the knowledge to access highly sensitive information, they can do so in a way which makes it difficult to know they are there, track them, or confirm exactly how much data has been compromised.

Despite this, military communications are not always as secure as they need to be. When a company develops a satellite, they develop all of the algorithms, software and components in a siloed environment. The benefit of this is absolute security control of that satellite with no dependencies, but on the other hand it prevents the implementation of standards-based technologies that enhance security across the defence industry as a whole.

Space obstacles

Due to the size, scope and number of Earth station access points, there are a number of challenges that come with securing military satellites. Space-based assets form large communication networks that are collecting and sharing huge volumes of sensitive data, and just one weak link can bring down the entire network. Every single component and device in the network must have the correct security measures in place to ensure it is not vulnerable to an attack.

There is a similar concern in regard to supply chain security challenges, as the highest level of security will come from all devices and stages of the supply chain following the same secure standards. If one component does not have the same stringent testing and protection in place as others, hackers may find a way in.

The isolation of space means it is vital that a level of trust is established between devices on Earth and satellites that last for the entirety of the satellites' lifetime. Of course, we cannot send people up to upgrade or maintain each and every satellite, so the right solutions and infrastructure need to be in place before a satellite goes into orbit. Weak encryption and old equipment are key vulnerabilities for satellite networks and are common targets for hackers. With the right technologies built into satellites at the start of development, they will be protected for years to come.

Trusted computing technologies are not just for computers

Trusted computing technologies have been widely adopted for equipment such as PCs and servers, but they can play a critical role in protecting satellites too. With well-established and proven architectures, specifications and standards followed, global military communications security can be enhanced significantly. Trusted computing technologies act as the building blocks to creating secure systems and ensure trustworthiness of devices, device identity and security validity. Communications can be authenticated at every stage of data transmission, acting as a firewall as no unchecked data will reach the satellite. Trusted computing technologies can also encrypt communications at the networking level, protecting data even when it is travelling across the satellite ecosystem.

The implementation of trusted computing technologies can play a key role in securing the supply chain too. According to a report from Sonatype, supply chain attacks grew by 430 percent in 2020, but the sheer number of stages, organisations and individuals involved make it difficult to protect against hackers. A satellite is the end product of a lengthy design and manufacturing process, so it is critical that these technologies are implemented across the chain as a whole to ensure enhanced security. Some stakeholders in the supply chain may have the tools, knowledge and expertise to ensure all devices and stages are kept secure, but others may not. The implementation of trusted computing technologies across the ecosystem as a whole will best protect military communications from cyberattacks by guaranteeing the reliability and integrity of satellite networks. **GMC**

Due to the size, scope and number of earth station access points, there are a number of challenges that come with securing military satellites. Photo courtesy TCG

Proven Performance for Mission Communications

Proven performance translates into reliability, scalability, adaptability and optimized space segment for mission communications. With Comtech, you have all of that and more. Our product portfolio of satellite modems, digital IF, data optimization, network and bandwidth management and RF products are supporting government/military applications above and below the sea, on the ground, and in the air. We offer both branch and agency support with solutions engineered to meet a range of standards for changing mission requirements. As a result, the Comtech brand is utilized in the majority of the U.S. Department of Defense's tactical terminal program.

Let's discuss how the proven performance of Comtech solutions can support your mission communications. Contact us today.

COMTECH EF DATA™

+1.480.333.2200
sales@comtechefdata.com
www.comtechefdata.com

Image courtesy of DoD

Phil Mar, CTO for Government Systems at Viasat

GMC Q&A

Defining the cutting edge

Viasat has proven itself a highly intuitive commentator on emerging technologies in defence. As a developer on the frontlines of technical movements, it's often Viasat's solutions defining the cutting edge. Phil Mar, CTO for Government Systems at Viasat, discussed contemporary challenges, as well as the company's recommendations for the most sensible strategies moving forward.

Laurence Russell, Assistant Editor, Global Military Communications

Question: What have the last few years taught us about the nature of the cyber domain?

Phil Mar: In the past few years, we have learned that political and diplomatic efforts to curtail cyber-attacks have not worked. The number and severity of attacks persisted, as illustrated by some notable and high-profile attacks including SolarWinds, Microsoft and Colonial Pipeline to name a few. So, while diplomatic and political solutions will no doubt continue to be explored, we shouldn't expect this to deter or prevent future attacks.

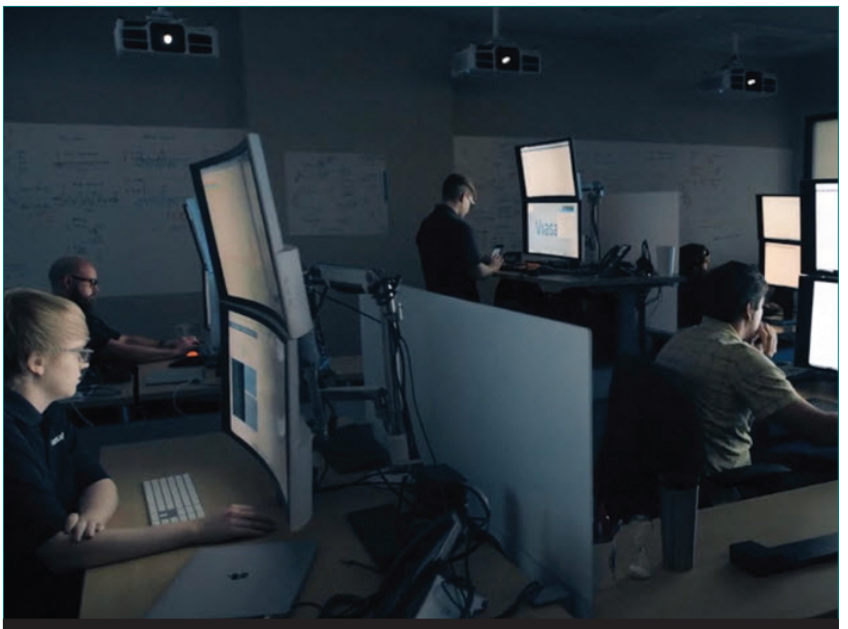
The US and allied nations need to have a cybersecurity strategy that addresses adversaries' emerging capabilities instead of intention. This means continuing to evolve and expand capabilities from end-to-end, with the ability to identify threats, protect sensitive data and mitigate risks amid an increasing pool of potential threats that could target a vastly expanded attack surface.

Question: How is electronic warfare being used in engagements today, and how will it be deployed in the future?

Phil Mar: Electronic warfare (EW) has been an integrated part of warfare for many years. But the deployment and sophistication of EW is undoubtedly growing with greater reliance on advanced microelectronics in C5ISR in weapon systems.

With the proliferation of software-defined radio (SDR) and standardization of waveform and protocols, EW capabilities are no longer only available to near-peer threat actors. Smaller nation-states and groups can acquire, deploy, or even develop EW capabilities at scale. So, with EW engagement becoming more common, we will see a continued increase in both defensive and offensive EW capability.

Question: Quantum technology often compels conversations about cybersecurity, both in quantum computing decryption and 'unhackable'



Cybersecurity Operations Center Viasat

ORBAN MICROWAVE

SYSTEMS BUILT TO SPECIFICATION
WHERE NO STANDARD SOLUTION IS
AVAILABLE ON THE MARKET

SHAPED BEAM GPS ARRAYS
LOW NOISE AMPLIFIERS
ANTENNAS WITH HEMOSPHERICAL COVERAGE
L AND S-BAND ANTENNAS
X-BAND ACTIVE & PASSIVE ARRAYS
HIGH-EFFICIENCY DC/DC CONVERTERS
POWER AMPLIFIERS
AND MORE!

321-200-0080

11333 LAKE UNDERHILL ROAD | SUITE 104 | ORLANDO FL, 32825

ORBANMICROWAVE.COM

quantum security. How do you anticipate quantum technologies realistically influencing cybersecurity?

Phil Mar: It is still too hard to predict the timing, but quantum computing will significantly impact security as we know it. Quantum computing will make the current generation of public key cryptography, such as RSA (Rivest-Shamir-Adleman) and ECC (elliptic curve cryptography), vulnerable to attack. These security concerns are certainly things governments and militaries need to be aware of as quantum computing grows.

The National Institute of Standards and Technology (NIST), part of the US Department of Commerce, has been working the past few years to come up with quantum resistant cryptography (QRC) to protect against this future. So, if you have information that needs to be kept under secrecy for the next few decades, it is important to start migrating data protection capability with QRC or at least begin to plan for it now.

Question: With several examples of high profile cyberattacks being strongly alleged to have been committed by near-peer states as the cyber arms race accelerates, do you think entire engagements can be fought on digital battlegrounds?

Phil Mar: The real answer depends on the nature of the operations and the definition of battlegrounds. Most military operations involve many contingencies, which means it is unlikely for an entire engagement to be fought just on digital battlegrounds. But, as we look ahead, what is most vulnerable is critical infrastructure in the civilian world that supports military operations, such as electric grids, communications systems, etc.

We should expect an increase in the number and severity of these cyber-physical attacks on critical infrastructure targets. It's important to understand the impact these attacks could have on military operations, as well as recognize that civilian lives are likely to be disrupted.

Question: In prior conversations with Viasat, we discussed the culture of military technology R&D changing to match the speed of the commercial sector. What are your thoughts on the topic?

Phil Mar: The mindset of development needs to move toward what we see across commercial. The speed of innovation from near-peer adversaries is like the competition you can see within western commercial sectors. In many cases, these peers have much simpler acquisition processes, allowing them to constantly explore the use of new capabilities and look for an asymmetric advantage.

The US, UK and allied governments must innovate the same way to bring forward technologies at the speed of relevance before they are outdated. This is critical not to overtake or surpass what adversaries are doing, but to keep up with the constant evolution and emergence of new threats. Many nations, particularly as it relates to offensive cyber and EW, are fully adopting this model.

However, this doesn't mean government and military agencies need to take on all the innovation and technology development themselves. In fact, leveraging the commercial sector investments already being made can provide government users with faster access to the latest technology to keep pace, as well as remove the management and maintenance responsibility that comes with owning the R&D directly, meaning less cost for the taxpayer. The important thing, regardless of the technology, is creating a more agile process in the acquisition and deployment of solutions for the military to support the warfighter.

Question: In terms of cybersecurity, what does Viasat feel we all need to concentrate on for the best chance of global stability?

Phil Mar: Critical infrastructure needs government help to improve its cybersecurity posture, but this can't only be done through unfunded mandates. This is not going to work as near-peer adversaries are heavily subsidizing these industries to protect themselves. To keep pace with evolving threats, governments need to consider how they can encourage greater investment in enhanced cybersecurity.

Governments also have capabilities and technologies that industry can leverage. For example, the US Department of Homeland Security has a program called the Enhanced Cybersecurity Service (ECS) that enables industry participants to utilize unique threat intelligence and technologies that can prevent state actor attacks.

This program is a great example of a public-private partnership to offer supplemental cybersecurity capabilities. As cyber threats become increasingly sophisticated and widespread, continued public-private collaboration, as well as cooperation among allied nations, will be essential to combating the instability created by global cyber threats.

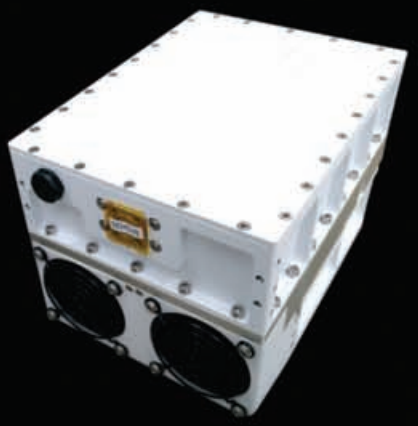
Question: How do Viasat's contemporary cyber solutions perform, and what innovations do they plan to deliver in the foreseeable future?

Phil Mar: The cybersecurity solutions Viasat has procured and developed all provide the protection needed across large networks, which today means terabytes (TBs) and petabytes (PBs) of data. This is an enormous challenge, and the path forward is to automate as much as possible. To put it in perspective, we deal with billions of cyber relevant events every day in our cybersecurity operations centre and analysts can only go over them with the help of big data analytics.

From a cyber innovation and development standpoint, we need to continue evolving by using artificial intelligence, behavioural analysis, and machine learning technologies to enhance our automated cyber capabilities. This will improve our cyber posture and allow us to better direct human resources toward the most critical threats that require greater attention. **GMC**

Photo courtesy Gorodenkoff/Shutterstock

Autoped
First motorized scooter
1915



ACTX-Ka40W-E31-V5
BUC Ka-band 40W
dual band (29-31 GHz)
2021

ACORDE

"Our task is not to foresee the future, but to enable it"

Antoine de Saint-Exupéry

Nelson Santini, CEO, Minerva Space Technologies

GMC Q&A

Inventive company with unique offering

The world of space startups is vast, particularly in the US, where an innovative tech culture stands as a leading pioneer in technology. Minerva Space Technologies is one such inventive new company, setting itself apart with a unique service offering. The company collects and analyses SDA data like many of its peers, and authenticates the information it produces with NFTs, non-fungible tokens, a popular finance trend. Nelson Santini, CEO, explains the company's strategy.

Laurence Russell, Assistant Editor, Global Military Communications

Question: Could you introduce us to Minerva Space Technologies?
Nelson Santini: We are a spaceborne infrastructure data-centric company focused on the generation, validation, and distribution of non-fungible digital assets (NFAs) that will help commercial and federal government customers, including the US Department of Defense, to achieve better command and control (C2) of their operational assets in space.

Some of the digital assets we'll use will be generated by our satellites; others will come from our space domain operational awareness (SDA) marketplace, where the space industry will be able to buy and trade resident space object (RSO) authenticated data.

Our technology solutions will help customers maximize their spaceborne infrastructure investment, elevating the user experience by using a mix of artificial intelligence (AI), virtual reality (VR), and augmented reality (AR) to analyze and assist the execution of complex space operations.

Going beyond 'awareness' or simple SDA, we are about achieving practical and meaningful command and control in space.

Question: There's a lot of mixed information about blockchain and non-fungible tokens (NFTs) in the news lately. Could you substantiate them, and describe how you use them?
Nelson Santini: Let's conceptualize these two elements first and then put them into Minerva's context.

Let's say that you have an aircraft carrier seeking safe sea transit through a narrow, a straight or a canal. Rules of safe navigation require those in command of this high-value asset to be familiar with the domain (the sea) they operate in, and more specifically, to know with certainty where they are relative to hazards to navigate in that environment. They must periodically 'fix' their position at sea.

To get a good 'fix,' ships can use a bearing to a star (celestial navigation), a bearing to a known fixed object ashore (a line of bearing), LORAN, GPS (digital navigation), radar distance to a known fixed feature, etc. Each of these data

Photo courtesy Zapp2Photo/Shutterstock

sources by themselves are good sources of navigational information and all have attached a level of uncertainty. When you compare and combine them all in a special way on a navigational chart, let's say for example at the same point in time, you reduce the impact of their individual uncertainty, and you get a more precise 'fix.'

Let's say that now, the Chief Quartermaster brings the navigational chart showing the 'fix' to the Navigator of the aircraft carrier, who reviews the data and with his special-colored pen signs the chart, to certify that the fixes shown are accurate. The chart is then taken by the Quartermaster to the Officer of the Deck and the Commanding Officer, who use it in the vessel's command and control operations, knowing that the information that they see is correct, and the C2 recommendations supported by the Navigator. *That 'special-colored' signature is a rudimentary NFT.*

So, you can see; it's not always especially exciting.

Minerva's blockchain technology will be used to help fuse and correlate petabytes of available spaceborne infrastructure data available in different formats from different sources. This correlation process will generate more accurate data (like a 'fix'), which will help the original data itself become 'more accurate' and refined. All data in the system, original and resulting, in turn will be tagged with NFTs so that the complete picture (the navigational chart) can be certified to be 'authentic' when presented to the users.

In this context, blockchain and NFT are not just cool trendy buzzwords. Minerva is using these new digital tools to ensure command and control decisions come from space domain awareness forged from factually optimized and verified data. No Commanding Officer would like to drive a warship with data that can't be trusted 100 percent.

Question: How would commercial entities benefit from Minerva's digitally authenticated space data?

Nelson Santini: Most people have no concept how much of our modern lifestyle is dependent upon the thousands of satellites orbiting above us. Broadcast TV, Netflix, gaming, and trading stocks are just a few examples of how satellites are needed daily, not for billions but for trillions of dollars moving in the global economy.

Out of sight and out of mind, satellites keep the economies of the world going 24/7/365. But what happens when a satellite fails to work? Maybe it's due to wear-and-tear that could have been identified and anticipated. Maybe it's an unexpected impact from space debris that could have been avoided. Even worse and more deeply concerning, what if it's the spaceborne version of a foreign cyber-attack on our critical infrastructure – and that high-value infrastructure just happens to be in space?

You can quickly see that an attack on our commercial space infrastructure, be it a bold direct attack or a silent stealth attack, immediately has a significant impact on our national security.

With our own satellites, Minerva will have 'eyes in the sky' collecting authenticated data to help monitor, manage, and mitigate the vast array of spaceborne risks for both our commercial and government customers, including where they overlap.

Imagine a commercial satellite experiencing unexplainable RF interference. Now let's say that one or more of our assets near this commercial satellite detects a nearby source of this interference, and a trove of other data points in the blockchain validate this 'digital asset' and observation. Developing a course of action to fix the interference would be a much faster, more focused effort, rather than what we in America call a 'SWAG,' a scientific wild-ass guess.

As the industry moves to assembly and repair in space, imagine the value of an unbiased *third-party* certifying that work on a space asset was completed and in accordance to print by using sensors like LIDAR to confirm internal connections were properly made. Again, having this fact in the form of a digitally authenticated asset would free you from future liability to the space assembler, by providing solid proof that the work was properly done.

It's not just about onboard cameras and multiple sensors in space. It's about making sure that every piece of available data 'matches' reality and can be 'authenticated.'

Photo courtesy Yurchanka Siarhei/Shutterstock

"We recognize the fact that we are not the only ones in the industry talking about AI, AR, and VR. That said, Minerva plans to use the tools in a way that truly helps the user consume data in a way that gets them closer and faster to the decision point that extends and protects their commercial asset or our national security."

Question: What would be the benefit of Minerva's services for the US Government?

Nelson Santini: Command and control of orbital space.

Ever since the space race of the 1960s, space has been foretold as the next geopolitical frontier. Enter the Chinese into space in 2003 and now we have a complex, tenuous dance in LEO and GEO space, soon to be cislunar space and far beyond, amongst three superpowers quietly bidding for control. Add in nine other countries operating satellites in space and it is quickly becoming the proverbial 'wild west' orbiting above us. That said, here are some benefits:

1. Our satellites can be commissioned to address immediate government and DoD needs and gaps. We don't need to wait for a program of record or prolonged debate. If a spaceborne asset is needed, we have the means and network to build it and provide its services to the government.
2. Our data marketplace, combined with its blockchain and NFT technology will ensure that government customers are executing command and control decisions with secure, reliable digital artefacts, validated by multiple participating data sets and collaborators.
3. The centralized data marketplace will make it easier for government and commercial customers to get access to multiple data sources in the format that they need. Rather than waiting for a standard, or committing to one format, we will have the tools to ensure reliable, quick, and secure access to the multiple datasets.

You get the special data you need; now and you know it's 'clean.' You get it in the format you need or want it. In a world of quality vs speed, having a provider deliver both at the same time is a hard value to argue.

Question: How does Minerva use artificial intelligence and augmented reality?

Nelson Santini: This is another area where the industry 'hype' can distract people from the real substance. We are talking about rapidly emerging tools that when creatively leveraged, enable a significant acceleration in new capabilities.

The simple truth is that the amount of information related to any one piece of spaceborne infrastructure is hard to comprehend. Data overload is not just a warning from a computer, it's a real operational threat. It's truly a case of missing the forest because of the trees.

Take for example AI - the simulation of human intelligence through vast, detailed, lightning-fast computing algorithms, helps us consume and process enormous amounts of complex data to produce operational decision options for us to act upon.

With thousands of satellites in orbit, the wrong anomaly or malfunction can create a serious national security situation or an economic meltdown for a given industry. Without these new technologies, expecting any group of humans to achieve true command and control of orbital space is laughable. Unless we have the right AI tools properly applied, the data that we have is almost useless, and therefore our operational command and control, our space domain awareness is shaky at best.

Let's think about it this way:

- Maneuvering a satellite to keep a station at GEO is the standard operating procedure. A qualified group of operators and solid satellite maneuvering and station keeping software will do.
- Maneuvering a satellite because a conjunction analysis suggests a collision is likely, is a form of more advanced operating procedures where AI can help minimize the 'delta V' consumed to assume a safe operational posture.
- Alerting operators of an unexpected or uncharacteristic maneuver by an adjacent satellite may require an additional level of AI. Perhaps it could prevent a collision by actions taken in a compressed timeline and under a certain level of duress.

Where AI can make a better difference is in recommending a minute orbital maneuver today, to prevent a near-miss situation or conjunction in orbit two years from now, taking into consideration not only the objects in orbit today, but the debris likely generated by launches still to take place. This is an area where more advanced AI can help extend the useful life of space-borne assets, and that is our goal.

The problem is not only the volume of data that must be analyzed but how the analysis should be presented to the user. This is where VR and AR make the difference.

The most sophisticated AI engine and pristine data ecosystem can be less effective if the delivery interface limits the user experience. If you have ever received a 50+ column, 3,000 row excel or CSV file, you know. The dynamics of space simply dictate an elevated experience that allows operators and supervisors to act effectively and promptly consuming a large volume of information imperceptibly. AR/VR would allow users to 'drink data from a firehose,' but feel like they are 'sipping knowledge from a glass.'

We recognize the fact that we are not the only ones in the industry talking about AI, AR, and VR. That said, Minerva plans to use the tools in a way that truly helps the user consume data in a way that gets them closer and faster to the decision point that extends and protects their commercial asset or our national security.

Question: Space domain awareness is becoming a buzzword in the growing space industry. What differentiators set Minerva apart in the SDA arena?

Nelson Santini: Unpopular opinion perhaps, but Minerva does not want to merely support space domain awareness or deliver SDA, we want our commercial and government customers to achieve true command and operational control of their space-borne assets.

Space domain awareness is the means – command and control, the end.

Certainly, our ability to generate SDA data from space will set us apart from other telemetry SDA data sources. But far greater than the spaceborne content we generate will be the marketplace we build to collaborate with all sources of SDA data. Our SDA data marketplace will incentivize all suppliers of SDA data to share and correlate their data to create a better end-product for the entire SDA community.

As we improve the user experience, interface to the data, and add our own valuable content to the marketplace, Minerva will become the trusted platform for all SDA to be shared, validated, and monetized.

Minerva seeks to create more opportunities for correlation of SDA data by creating a marketplace for this data that incentivizes data creators to collaborate. Six sources of data about the same object or incident in space at the same moment in time gives us a far more accurate understanding of that object or incident than one source alone.

In the end, building an NFA digital marketplace and controlling our space-borne assets generating data in space, about space objects is what will set Minerva Space Technologies apart in the industry.

GMC


37TH SPACE SYMPOSIUM
SPACE FOUNDATION
April 4-7, 2022
Colorado Springs, Colorado | USA
New Business Opportunities
World Class Networking
Space Industry Experts
Be Connected. Anywhere.
Reserve Your Space!
www.spacesymposium.org
+1.800.691.4000 | #37Space #SpaceSymposium

Are we doing enough to prevent space debris?

Space situational awareness (SSA) has been a growing topic of concern in recent years, in line with the number of proposed satellite constellations. With so much more 'stuff' destined for orbit, the opportunity for collision and debris production has never been so great.

Pascal Wauthier, Chairman, the Space Data Association

We need to see all space users contributing high-quality data to further strengthen their reliability and accuracy and create safer use of space. Photo courtesy Abobe Stock

Satellites have been used by the military for numerous years. Beyond remote sensing, communications satellites enable forces to establish effective communication networks due to their high bandwidth and ubiquitous geographical coverage. With many missions happening in remote areas with poor ground infrastructure, satellite delivers critical connectivity. Connections must be secure and robust as personnel are relying on them to remain in contact with base; a loss of contact could have dire consequences on an operation and place assets at risk.

Additionally, satellite provides military organizations with means to create systems for mission development and planning. This isn't limited to combat; natural disasters and other crises often require military input, and networks must remain resilient regardless of failing ground infrastructures. As we build our reliance upon satellite-based infrastructures and networks, the importance of these networks' resilience grows. Within the military, resilience is one of the most important aspects of communications networks, as having access to comms systems is critical to achieving missions.

Commercial use of space is increasing drastically, and the number of satellites in orbit is set to vastly increase. Is the industry doing enough to manage space debris and ensure space situational awareness (SSA) is being used appropriately in order to prevent issues which could impact on military use of satcom?

The growing challenge of space debris

Since the first satellite launch in 1957, space debris has been a steadily growing problem. ESA states that there are currently approximately 7,500 satellites in orbit, with only approximately 4,600 still functioning. However, commercial markets within satcom are growing and this is being reflected by the launch of mega constellations of satellites into lower earth orbit (LEO). The number of satellites in-orbit are set to increase quickly; we have seen the FCC provide a licence for Starlink alone to launch 42,000 satellites. When debris is added, we will soon be facing hundreds of thousands of dangerous debris in orbit.

The figures above highlight the challenges surrounding the management of space debris. Even the smallest piece of debris can have a significant operational impact on a functioning satellite, and, in a crowded space, the threat of Kessler Syndrome is increasing. Through its statistical models, ESA estimates that there are 36,500 objects greater than 10cm in orbit. Identifying and tracking these objects is becoming increasingly important.

In March 2021 we saw that a Chinese weather satellite was

Commercial markets within satcom are growing and this is being reflected in LEO; there is set to be a significant increase in the number of satellites in-orbit. Photo courtesy Abobe Stock

2 DAYS

1000 PARTICIPANTS

9000 MEETINGS

40 SPEAKERS

maxine.benacom@proximum365.com +33(0)1 70 61 46 85 www.paris-space-week.com

ORGANIZED BY ASTech Paris Region PROXIMUM365 COMMUNITIES & LEADS GENERATION FACTORY

damaged in-orbit. At the time, the 18th Space Control Squadron of the United States Space Force tweeted that it was tracking 21 associated pieces from the collision. For months, there remained a question mark over what happened to Yunhai 1-02. However, it was recently announced by the US Space Force that a piece of space debris left over from a Russian rocket launch in 1996 collided with Yunhai 1-02, causing it significant damage. Without the correct monitoring and data sharing, it is likely that we will witness more of these preventable events. Additionally, with space becoming more congested, the potential secondary effects of any in orbit collision will increase significantly. Now is the time for industry and other space users to be looking at the systems in place for space traffic management purposes.

Getting deorbiting practices right

Deorbiting and retiring satellites is key to managing space debris; space sustainability relies upon it. Retiring satellites has been best practice within the geostationary orbit for many years, with many satellites being moved to a higher graveyard orbit to ensure that decommissioned satellites will remain out of active zones for 100 years or so.

Deorbiting satellites in low Earth orbit (LEO) will not be the same. It is set to be a bigger challenge; decommissioned satellites must be positioned to descend with atmospheric drag, allowing them to re-enter Earth's atmosphere to burn-up. Due the scale of LEO, the IADC has mandated that LEO satellites should be explicitly deorbited or where appropriate manoeuvred into an orbit with an expected residual orbital lifetime of less than 25 years. Significant players in LEO, including SpaceX and OneWeb, have confirmed that they will be adhering to the FCC disposal orbit guidelines, however it is crucial that all space users obey these rules. Preventing space debris must be a priority for the satellite industry; satellites should have a de-orbiting strategy prior to launch.

Monitoring: What systems are in place?

Monitoring is a key factor within the management of space debris. There are numerous organizations, including governmental, which are willing to share data, however bringing together multiple sources, aggregating the data, and delivering it to space-users in a manner that is both timely and actionable is a significant task. Naturally, some military use of satellites is confidential and presents data sharing challenges. However, with commercial and military sectors operating in relatively close proximity, there is a need for a secure central aggregator of flight data to perform conjunction assessments and provide safety warnings. Without this, satellite operators, regardless of their sector, are at increased risk of collision.

Beyond the 'how', the industry also needs to address the 'what.' We should be looking at what data is being collected and shared. What are the satellite's capabilities? Its size and potential for manoeuvrability? Do we know its future movements, including those as a result of manoeuvres? Without this in-depth data, decisions will not be as accurate as they need to be to ensure safety of flight and the preservation of the space environment. Data sharing the correct information is critical in preventing collisions. Considering the catastrophic impact, a collision in orbit would have, this must be a priority for Space Traffic Management (STM) systems.

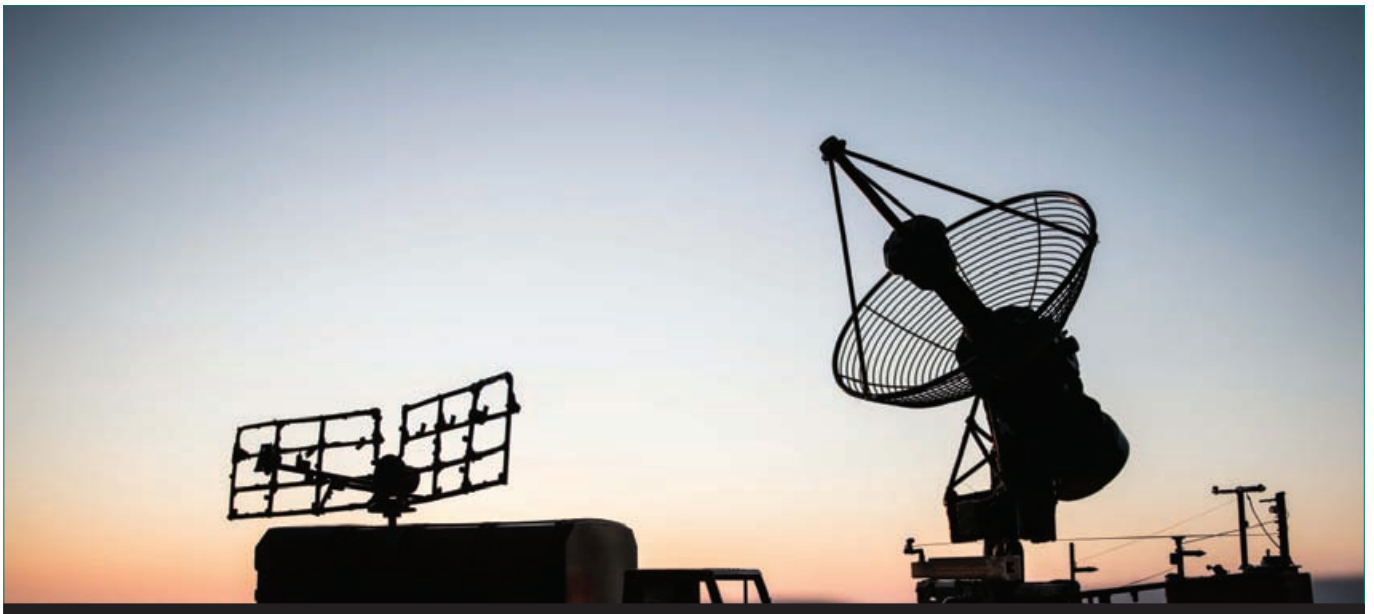
Is in orbit cohesion possible?

As an industry, we must rely on a cohesive system in which all space operators including governmental space users are able to use space safely. The Space Data Association's approach safeguards data and avoids compromising the individual operator. The SDA's platform, the Space Data Centre, utilizes the member provided ephemerides with integrated future manoeuvre information; this can be fused with SP (Special Perturbation) data from the Space Force public catalogue if required.

Rather than requiring all orbital information to be publicly available, participants can access accurate information to the extent necessary to improve conjunction assessments. This concept of 'least information release' means SDA's members can collaborate across all participating space users, civil, military, commercial, and non-profit sectors to ensure access to key data without disclosing or mis-using sensitive information.

SDA also makes member data available, at their request, to others such as the 18 SPCS, to ensure that member data is available for processing by special user communities, such as the military.

The SDA's consolidation of data benefits all operators. It has never been more important to have a strategy for space debris management; never have we relied on communication networks as much and never has the industry seen such a dramatic shift in terms of numbers. All operators, regardless of their sector or nationality, must work together to address a significant threat to the satcom industry: space debris. The systems are in place; it's now time to see everyone contributing high-quality data to further strengthen their reliability and accuracy and create safer use of space. **GMC**



With commercial and military sectors operating in relatively close proximity, there is a need for a secure central aggregator of flight data to perform conjunction assessments. Photo courtesy Abobe Stock

Advantech Wireless Technologies

Military & Government Solutions

X-Band SSPAs/BUcs
GaN & GaAs configurations

Engage Class Integrated
SATCOM Terminals

X-Band / Ka-Band
Frequency Converters

Troposcatter Products

LNAs / LNBs

Solid State
Pulsed Amplifiers

Faster & More Secure Communications for Military and Government Agencies

At Advantech Wireless Technologies, we have over 25 years of experience delivering cutting-edge innovations in communications that solve mission critical communications challenges.
We understand the challenges that government & military leaders face and our technologies empower them with the freedom to communicate quickly, reliably and securely.

ADVANTECH
Wireless Technologies

Contact us

sales@advantechwireless.com

+1 514 694 8666

advantechwireless.com

www.stn.eu
@ sales@stn.eu

STN

SATELLITE

BROADCAST

CO-LOCATION