ISSN 1756-3240
August 2023

GMC

Linked in YouTube

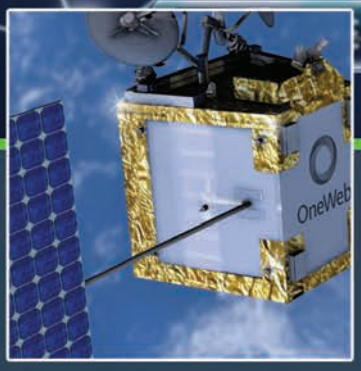
Global Military COMMUNICATIONS

OneWeb resiliency

Q&A SpiderOak

Private 5G networks

Navigating cyber threats in space



Front cover photo courtesy of Shutterstock

SATELLITE Evolution Group

Global Military Communications is part of the Satellite Evolution Group portfolio

COMTECH™

Fluent in the Future™

At **Comtech,** we're building the future of hybridized connectivity, with technology that integrates **terrestrial and satellite communications networks**.

Relentless pursuit of a better way: empowering people to connect everything and everyone.

www.comtech.com

Executive Editor
Crispin Littlehales
crispin@dsairpublications.com

News & Social Media Editor
Nicole Lewis
nicole.lewis@dsairpublications.com

Marketing and Business Development
Belinda Bradford
belinda@dsairpublications.com

Marketing Production Manager
Jamaica Hamilton
jamaica.hamilton@dsairpublications.com

Circulation Manager
Elizabeth George

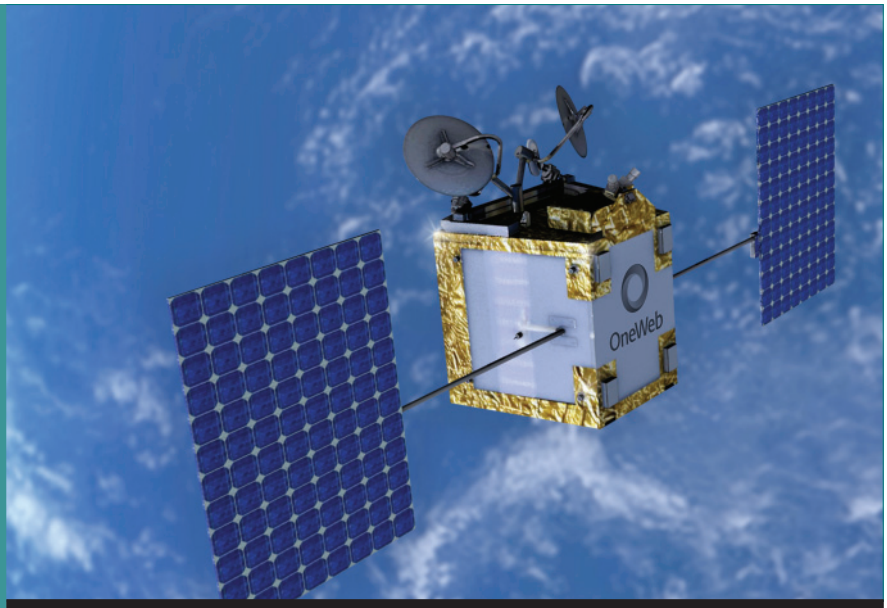
Publisher
Jill Durfee
jill.durfee@dsairpublications.com

Publishing Director
Richard Hooper
richard@dsairpublications.com

Managing Director
David Shortland
david@dsairpublications.com

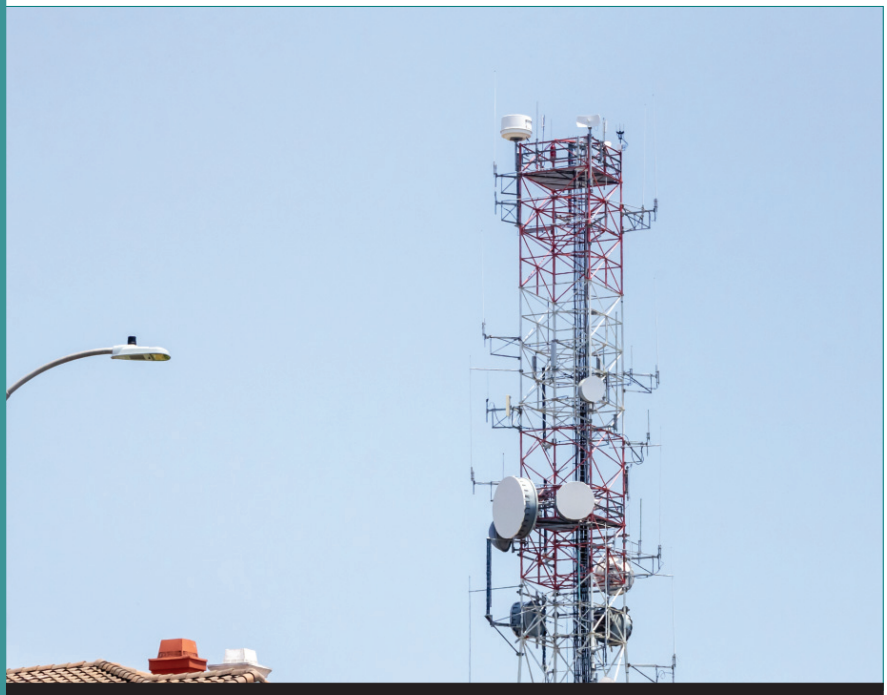
DS Air Publications
1 Langhurstwood Road
Horsham
West Sussex, RH12 4QD
United Kingdom
T: +44 1403 273973
F: +44 1403 273972
admin@dsairpublications.com
www.globalmilitarycommunications.com

GMC



Q&A Chris Moore CBE, VP of Defence and Security for OneWeb - page 8

Contents



If you would like to supply information for future issues of GMC please contact Crispin Littlehales

Photo courtesy Illuminate

Elbit Systems awarded a $55 million contract to supply a counter UAS solution to the Netherlands

Elbit Systems has been awarded a contract worth approximately $55 million to supply multi-layered ReDrone Counter Unmanned Aerial Systems (C-UAS) to the Netherlands. The contract will be performed over a period of four years.

As part of the contract, Elbit Systems will supply several mobile, stationary and deployed configurations of the ReDrone integrated Counter-UAS solution along with a logistic support package and training.

The ReDrone Solution is comprised of Elbit Systems' advanced DAiR Radar, signal intelligence (SIGINT) sensors, and COAPS-L electro-optical (EO) payload which provide an enhanced integrated aerial picture, along with high-end electronic attack capabilities, all fully controlled by a unified Command and Control system.

The ReDrone system provides functionalities beyond the common active and passive sensors that enable it to rapidly detect and locate multiple drones simultaneously within the protected area. The system can detect, identify, locate, track and neutralize hostile UAS during day and night, both in urban and rural environments and under various weather conditions.

Oren Sabag, General Manager of Elbit Systems ISTAR & EW: "The growing threat of drones creates an increasing demand for our Counter UAS solutions. We have leveraged our technology of advanced radar, signal intelligence, electro optic and electronic warfare technologies to develop an advanced, open and future ready solution for this emerging requirement of our customers. We are very proud to have been selected by the Netherlands to supply this solution and further strengthen our long term partnership."

GMC

Photo courtesy Elbit Systems

HII's Ingalls Shipbuilding launches guided missile destroyer Ted Stevens (DDG 128)

HII's Ingalls Shipbuilding division has successfully launched the Navy's third Flight III Arleigh Burke-class guided missile destroyer Ted Stevens (DDG 128).

"The translation and launch are always important milestones for our shipbuilders and the life of a ship," Ingalls Shipbuilding DDG Program Manager Ben Barnett said. "Our team has put in a tremendous amount of work leading up to the launch, and I am proud to see them bring DDG 128 one step closer to completion."

Prior to launch, DDG 128 was translated from land to the dry dock using translation railcars to support the ship. Once in the dry dock, the ship is prepared to launch.

Ted Stevens is the 76th Arleigh Burke-class ship, and its name honors former US Sen. Ted Stevens, who served as a pilot in World War II and later as a US senator representing Alaska. At the time he left office in 2009, he was the longest serving Republican US senator in history.

Ingalls has delivered 35 Arleigh Burke-class destroyers to the US Navy including the first Flight III, Jack H. Lucas (DDG 125), in June of this year. In addition, Ingalls Shipbuilding has four Flight IIIs currently under construction and was awarded an additional six destroyers earlier this month. Ted Stevens will be christened Saturday, Aug. 19, while Jeremiah Denton (DDG 129), George M. Neal (DDG 131) and Sam Nunn (DDG 133) are also under construction at Ingalls.

Flight III Arleigh Burke-class destroyers built for the US Navy incorporate a number of design modifications that collectively provide significantly enhanced capability. DDG 125 includes the AN/SPY-6(V)1 Air and Missile Defense Radar (AMDR) and the Aegis Baseline 10 Combat System that is required to keep pace with the threats well into the 21st century. Arleigh Burke-class destroyers are highly capable, multi-mission ships and can conduct a variety of operations, from peacetime presence and crisis management to sea control and power projection. Guided missile destroyers are the backbone of the US surface fleet and are capable of fighting multiple air, surface and subsurface threats simultaneously. **GMC**

Photo courtesy HII's Ingalls Shipbuilding

Satcom Direct Avionics awarded a three-year agreement to provide aeronautical connectivity

Satcom Direct Avionics has won a competitive bid to deliver multi-band aeronautical connectivity services for Shared Services Canada (SSC) and its clients for a period of up to seven years. This represents the first signing of such an agreement between the two entities, which will see SD Avionics provide appropriately secured high-speed broadband and datalink services, hardware, hosting, and infrastructure services to support global aeronautical missions for SSC and other federal Canadian government bodies. The deal will be supported by value-added services, including training and customer support, as well as regular upgrades of the technology.

Through SSC, Canadian government users will benefit from easy ordering access to quickly establish worldwide connectivity delivered through multiple band airtime services, including Ka, Ku, and L-band options.

As an Inmarsat Tier 1 Distribution Partner and Value-Added Reseller, SD will support the full range of Inmarsat aviation services including Global Xpress (GX) airtime powered by the Ka-band Global Xpress constellation, SwiftBroadband and Classic Aeronautical services; Ku-band services will be powered by the Intelsat FlexAir network. As an approved Tier 1 Value Added Reseller for Iridium SD will also support Iridium Airtime, Voice and Low Data Throughput services as well as Iridium Short Burst and Short Message Service (SMS) services and Iridium Certus Airtime services. The aggregated group of services and optimization of multi-orbit capabilities will ensure SD facilitates enhanced high-speed broadband connectivity solutions to provide airborne users with seamless, continuous, and reliable worldwide mobile connectivity.

The aeronautical services will be supported by SD's comprehensive terrestrial network to ensure appropriately secured transmission of all SSC customers' data from aircraft to the Canadian federal government specified locations. Combined, the services will ensure always-on global connectivity, even in the most geographically challenging environments.

"We have an extensive understanding of how connectivity is used by these customers, who are often operating critical missions in extreme environments. With an agnostic approach to technology and partners, we already deliver multi-orbit connectivity services that optimize the combination of GEO, LEO and HEO satellites. This in-depth knowledge, expertise, and proven capability of managing requirements and exceeding expectations, even in the most difficult of circumstances, has enabled SD to win this contract. Our team worked extremely hard to win this contract, and we are looking forward to developing our relationship with the Canadian government," said Joanne Walker, general manager for Satcom Direct Avionics.

The contract is confirmed for an initial period of three years with four additional one-year options. SD Avionics is responsible for fulfilling the acquisition requests, delivering consistent connectivity, and providing customer support as and when needed by SSC representatives and clients.

The SSC mandate is to provide modern, appropriately secured, and reliable information technology (IT) services to government entities. It also supports Canadian citizens' access to government benefits and services from anywhere, at any time, from any device.

GMC

Photo courtesy Satcom Direct Avionics

EARTH CALLING...

When 'Long Distance' takes on a whole new meaning...

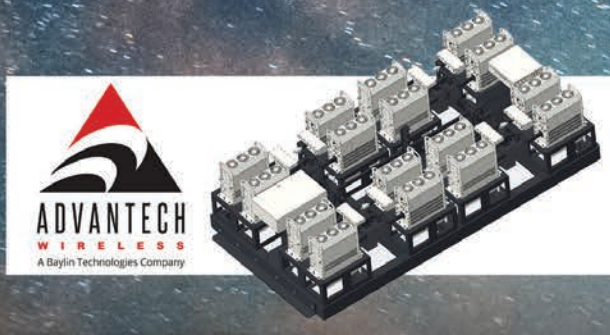
Advantech Wireless Technologies

SUMMIT

for Near and Deep Space applications.

HIGH POWER Solid State Amplifiers and Systems

- 800W to 16kW of transmit power in L/S, C, Low X, Std. X and Ku-Bands
- Communications and Ranging
- Antenna-Pad, Work-Platform and Side-Arm Mounting Configurations
- Gateway Earth Stations, Deep Space, DTH, Satellite Tracking



advantechwireless.com

Chris Moore CBE, VP of Defence and Security for OneWeb

GMC Q&A

OneWeb resiliency - when and where it's needed most

Whether it is disruption through hostile action or natural disaster, OneWeb can help by providing additional connectivity to keep communications going when all else fails. We sat down with Chris Moore CBE, VP of Defence and Security for OneWeb and a former 2* Royal Air Force officer, to find out more about the company's mission critical offerings to militaries and governments worldwide.

Crispin Littlehales, Executive Editor, Satellite Evolution Group

Question: The changing face of war requires that militaries embrace new strategies for communication. How can OneWeb help today's warfighters stay connected on the battlefield?

Chris Moore: Communication systems have always shaped the way militaries fight and advancements in technology have challenged commanders to think differently about how they can gain operational advantage. From smoke signals, flags on ships, telegraph lines in the trenches, to radio and now satellite, these technological innovations have had a profound impact on the ability to synchronize and project the diverse components of military organizations, ultimately enhancing a country's ability to operate in more effective and efficient ways.

Although satellite-enabled communications have been widely available for some time, there exists the challenge of getting large amounts of bandwidth at very low latency to the tactical edge, be it on the front line in a trench, in a cockpit, on a ship, or even an autonomous platform. Over my military career, the model has been largely built around large amounts of bandwidth into headquarters in the rear, and as information flows forward towards the front line it's compressed and constrained through a series of ever more tactical systems. By the time you get to the tactical edge there tends to be a paucity of bandwidth and high latency induced by the complexity of poorly integrated system of systems architectures.

Where OneWeb and low Earth orbit (LEO) satellites help is that they are enabling some of those blockers to be overridden. You can now get high bandwidth with low latency directly to the tactical edge. Not only does that offer militaries the ability to operate more effectively with extant organizational structures, in turn it also offers the opportunity for commanders to organize and fight their force elements differently, for example in a de-centralized way. The best recent example of this is the Ukrainians using LEO constellations in a highly mobile and agile fashion against a superior—at least in terms of mass—opposition.

Question: What about the welfare of soldiers, aviators, and sailors—including their ability to stay connected to their families—how does OneWeb fit in?

Chris Moore: I was in the military for 31 years. In those early years, I was lucky if I could write a letter back home and get one in return. In the three decades since, we've gone from handwritten notes to full streaming connectivity so there's been a massive change in welfare for our deployed forces. This is not only critical for morale, but we now have a generation that demands WiFi and connectivity as a theater entry standard. Using LEO will enable real time video calls, social media, and gaming which is very important if you want to sustain and retain troops for the long haul and keep them and their families happy.

Question: Are there other benefits that OneWeb's LEO constellation can deliver to military users?

Chris Moore: One major advantage is that we offer true global coverage. For better or for worse, the changing climate is making places such as the High North and Antarctica more accessible. Sea lanes are opening up and there are lots of mineral resources in those areas, which is creating competition alongside economic growth and, of course, helping to generate data on climate change. Currently, OneWeb is the only LEO that is designed to operate globally and offer coverage at the polar regions.

Photo courtesy Shutterstock

Another big advantage is low latency. It is not only important for how the military operates today, but it will be even more important in the future when we have widespread use of autonomous and semi-autonomous platforms where you need to perform real-time connectivity, alongside command and control at global reach. This is crucial to ensure these systems have the right oversight to make sure they're operating in both a legal and safe manner. Low latency also unlocks the delivery of cloud services across the final mile, bringing super compute power and AI to the tactical edge...that will be a gamechanger.

OneWeb tends to use distribution partners who are experts in their fields. Those experts can combine our strengths with their specialisms to meet the needs of end users. In the case of Defense & Security, we are dealing with a few distribution partners who have a strong and longstanding pedigree of understanding what end-user requirements are and tailoring their services accordingly.

Our terminals are also a plus for military users. As the technology progresses, they are coming down in size, weight, and power, whilst increasing in utility. Our first batch of flat panel terminals are being delivered even as we speak. Some of them are the size of a small table and some are the size of a pizza box. In the very near future, we'll be taking delivery of our person-portable terminals that will provide that link to the tactical edge in the land environment as well as on aircraft and ships. These small terminals are highly capable and represent a step change over what militaries have previously had.

A lot of OneWeb's lineage has emerged from the mobile phone industry. As a result, we've learned a lot about how people relate to their mobile phones. Our packages are tailorable, flexible, and adaptable so that you can actively and dynamically configure that service through an app on your phone or laptop.

The final big benefit is mobility. Of course, this has always been possible with traditional SATCOM, but as we know from GEO and MEO, the beam sizes tend to be fixed within a specified geography. When assets such as ships or planes go beyond the geographic boundaries, you then must swap satellites or beams to make sure that the planning associated with that is both commercially and operationally in place. One of my last jobs in the military involved operational planning for a carrier strike group when it deployed from Portsmouth to the other side of the world—the South China Sea. The satellite planning exercise for that took the better part of a year because of the number of commercial, military and government agreements that needed to be struck with different providers and agencies to make sure the journey was supported and coordinated, especially across the electromagnetic spectrum.

There are no geographical boundaries with our constellation because it covers everywhere. As a result, you don't have that same degree of complexity in the planning and provision of satellite services as with traditional approaches.

Question: What about a multi-orbit architecture; how is that superior?

Chris Moore: Each orbit has its strengths and weaknesses. Looking ahead, we'll have high altitude platforms, terrestrial

connectivity, network of networks, and so forth. The architectures and the technology are converging because interoperability is not just a military need, it's a societal need. So, we need an architecture that's not just multi-orbit, or as I prefer multi-layered, but also multi-domain. That's why OneWeb is merging with Eutelsat so that we can look towards a coherent LEO/GEO architecture in the first instance. As OneWeb evolves our horizontally integrated model, we can see scenarios where we could do LEO to MEO interoperability with other industrial partners and in time LEO to ground.

Question: How does OneWeb stack up against other MilSatCom offerings?

Chris Moore: The obvious comparison is StarLink, but we are not a one-for-one comparison because we are clearly differentiated from them. I would say that OneWeb's solution is optimized for community WiFi or 5G backhaul—things that require Quality of Service, Service Level Agreements (SLAs), and guaranteed bandwidth. We also have the advantages mentioned previously over other MEO and GEO suppliers.

It's not just about the technology of course. Licensing and spectrum come into the equation as well. OneWeb has advantages in the electromagnetic spectrum. For example, we have the priority LEO filing at Ku-band, which means that other LEO operators must coordinate with us. We also have very high priority in Ka-band, and we have other frequency bands that we have access to. Then there is the fact that each country where you offer services requires that you go through a licensing process. Again, OneWeb is very advanced in reaching agreements with certain countries to allow services to be consumed. It's a multi-dimensional challenge involving political, commercial, and technological elements as well as timing.

And, of course, it's not just about comparison to MilSatCom. It's about augmenting terrestrial and subterranean networks. With less than 20 percent of the globe covered by terrestrial cellular networks it's critical that connectivity becomes available to enable those living in under-served areas to communicate and function effectively. We are putting LEO services into disconnected or poorly connected areas and by doing so, will tap into an estimated 4 billion people who haven't yet got decent internet services.

Question: Historically, militaries have been slow to adopt newer methods of communication, often hanging on to their legacy systems. Does OneWeb have a way of addressing this?

Chris Moore: You must work with the militaries of all nations to understand their procurement process, figure out what they need, and convince them that your solution is right for them. In my experience, when it comes to revolutionary technology, it's about getting that into the hands of the users as quickly as possible so that they can experience the benefits for themselves and see how that new technology changes the game.

The war in Ukraine has shown the utility of LEO, as has the recent earthquake in Turkey and Syria. That's where we can quickly deploy these new technologies and demonstrate the benefits compared to conventional means. OneWeb, alongside our distribution partners, hopes to increase adoption by being at the forefront of what the world throws at us.

Question: What do you see are the pitfalls if a military or government doesn't embrace and adapt to new technologies?

Chris Moore: Quite simply, if militaries don't adapt to new technologies, they'll lose their competitive advantage. It's interesting to note that the US has been at the forefront of shifting into multi-orbit and a big uptake of LEO. But it's not just the big powers that are following suit. Some of the up-and-coming powers want to leap a generation of learning by adopting new technologies. Indeed, there are lots of smaller militaries that are seizing the opportunity to gain competitive advantage, having seen what has happened in Ukraine.

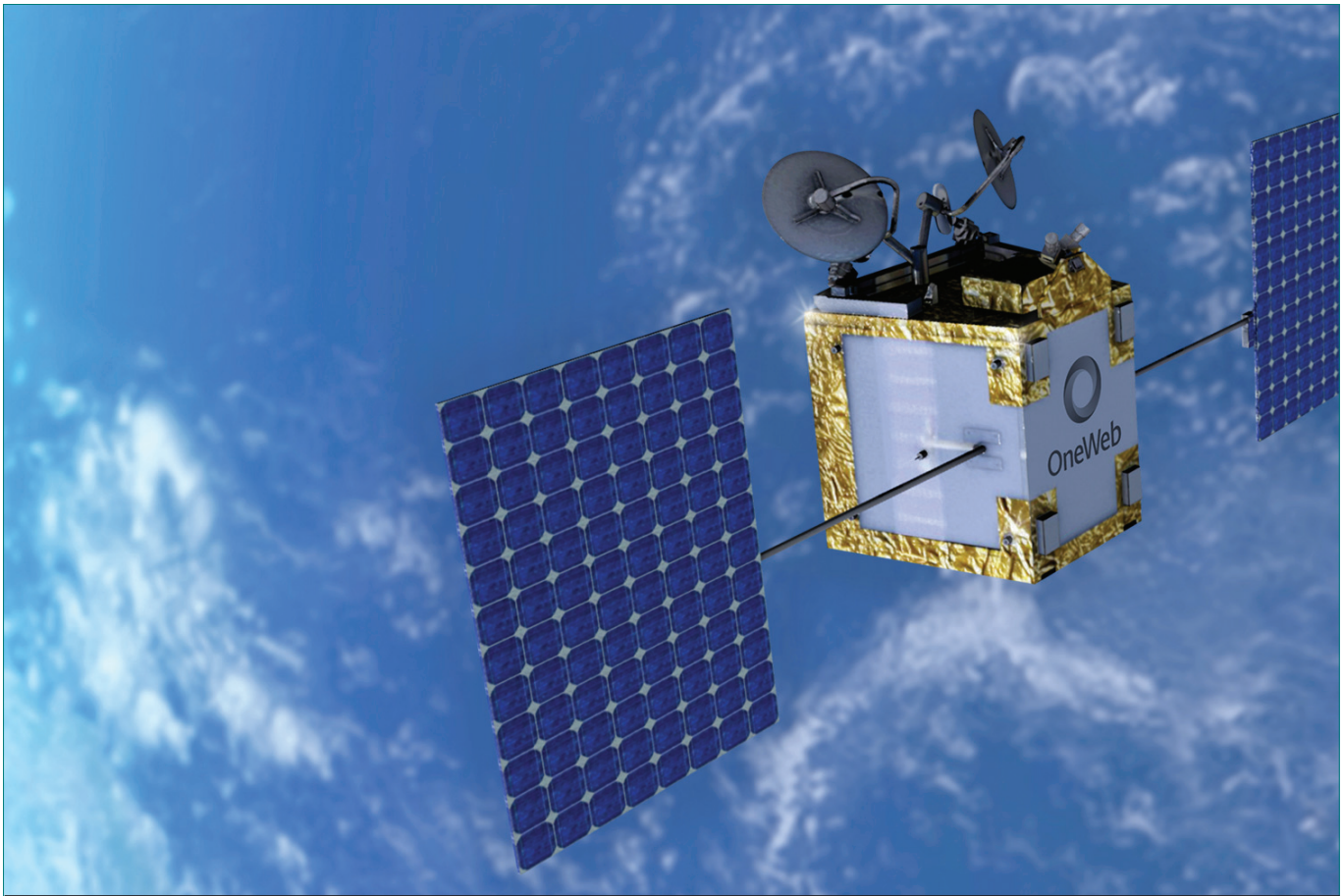


Photo courtesy OneWeb

RF, fiber optic, and low frequency interconnectivity solutions for land, sea and air

Visit us at DSEI London #H7-626

For over 50 years, HUBER+SUHNER has been trusted to solve the defense industry's most difficult design challenges spanning RF, fiber optic, and low frequency communication. As a recognized leader in materials engineering and rugged connectivity design, HUBER+SUHNER is proud to serve industry leaders across the globe with enabling solutions that meet stringent requirements for performance and safety in the most demanding of severe environments.

RF/Microwave Connectivity

These assemblies include the SUCOFLEX 100, MULTIFLEX CT, SPUMA RS and MINIBEND® coaxial cable families and are all MIL qualified. We also offer configurations utilizing stainless steel 316L connectors, delivering outstanding mechanical durability.

Antennas

Covering the digital TETRA, ultra-broadband and professional LTE bands, we offer mobile communication services enabling the combination of voice and data in critical situations to ensure reliable coverage when it is needed most - in the air, on the ground, and at sea.

Fiber Optic Connectivity

A broad range of fiber optic cabling solutions that meet the stringent requirements of ground and naval applications. Light, robust, halogen-free and self-extinguishing cables are available to ensure the highest level of safety for field personnel and equipment.

Data & Power Connectivity

Extensive expertise in data communication and power connectivity, utilizing our renowned RADOX® cable technology, featuring electron-beam-cross-linked material to ensure reliable performance in high-temperature applications and harsh environmental conditions.

hubersuhner.com

HUBER+SUHNER

You might be surprised by the list of countries who have been slow on the uptake. But there is one thing that will spur them on and that's competition. When they see not only their peers, but also lower tier nations taking up the service, it's likely they'll catch up.

There is, however, a bit of a gold rush going on since there is only a finite amount of capacity as we grow the network. If a country's military is late to the party, it will likely miss out and be less competitive in a rapidly evolving world.

Question: How can OneWeb help if an existing communications infrastructure such as an undersea internet cable, is sabotaged?

Chris Moore: Some state actors have allegedly disrupted undersea cables, which is a critical vulnerability to national and international infrastructure. It is how 21st century modern digitized society runs in a globalized world. The cables provide enormous capacity and solely relying on that connectivity is an incredibly dangerous position in which to be.

If an undersea cable is compromised, OneWeb doesn't have the ability to take on all of what undersea cables have to offer, but we can provide resilience for the highest priority traffic, be that of governments, financial systems, or high-priority industrials. That resilience can be available in an instant should these links go down and it will keep the critical national infrastructures, the political dialogue, and the intergovernmental relationships going on, so there won't be a breakdown of communication at scale.

Having a resilient path that will mitigate some risk if sabotage or an accident interrupts mission critical communications is vital. OneWeb is positioned to offer resilience to terrestrial and subterranean systems that impact the supply chain, energy, and all the other things that are critical for our militaries and our society to continue to function.

This is not just terrestrial in terms of the hard wires and fibre, it's about mobility and our logistics chain around the world, 24/7. We offer the opportunity to ensure tracking in real-time, regardless of geography. This can allow for dynamic rerouting and give decision makers options on how to do things differently because they know where things are.

The old military comms mantra of primary, alternate, contingency, emergency (PACE) absolutely applies to industry and defense alike so it's critical that OneWeb offer an alternative, and sometimes the primary solution to enable militaries and governments to keep their competitive advantage.

In June, we saw connectivity cut in several rural towns of Alaska when a 1,200-mile undersea fibre cable was damaged due to an ice scouring event. Using our vital network of satellites, we were able to work with our local partners to restore connectivity to affected communities whilst month-long repairs to the sub-sea system were made.

Question: What makes High North NATO Integrated Air Missile Defence a good use case for a low latency LEO constellation?

Chris Moore: Although fiber and line of sight radio links are the primary choice for an integrated air missile defense system, OneWeb offers resilience. We offer connectivity to support NATO's efforts, and, as LEO constellations evolve, there is the potential to add ancillary payloads to our constellation to better see what's happening in real time. That would be useful for measuring the environment, tracking wildfires, and in identifying and helping governments understand nefarious activities. But all of that is in the future.

What is happening now is that information technology and digital capabilities are becoming part of the front line and therefore a direct target. We see this with Ukraine. There is a blurring of the traditional transactional relationship between industry and defense. This is becoming a lot more integrated and interdependent than we've previously seen because the cutting-edge technology does not exist in the military as it exists outside. I think that may well force governments and societies to rethink what competition and conflict means across the whole of society and the industrial base. **GMC**

Terminal in Alaska. Photo courtesy of OneWeb

TERRASAT
Communications, Inc.
Engineered to Endure

BE PREPARED FOR THE UNEXPECTED

Protect your critical SATCOM applications with the unique CYBER HARDENED IBUCs.

C-Band | X-Band | Ku-Band | Ka-Band

- Cryptographic network protocols with SSHv2, HTTPS, & SNMPv3
- Secret-Key Authentication
- Multi-Level Access Control
- Hardened Physical Ports with ASCII
- Timeline History Logs
- Enhanced Management & Control

Learn more at Terrasatinc.com

Photo courtesy Bits And Splits/Shutterstock

Navigating cyber threats in space in the age of commercialization

The rapid commercialization of space has ushered in an era of unparalleled opportunities for technological advancement and innovation. Breakthroughs in lightweight composites and advanced materials have enabled the design and construction of more efficient spacecraft and satellites, while reduced costs have led to a significant surge in satellite deployment. However, amidst this significant progress lies a pressing challenge that demands our attention - the complex world of cybersecurity.

Neil Sherwin-Peddie, Head of Space Security at BAE Systems Digital Intelligence

As private companies, start-ups, and governments venture into space, the intricacies of space operations and the interconnectedness of space systems have become fertile ground for potential cyber adversaries, and these continue to loom in the space sector. The implications of these attacks are self-evident; however, it is crucial to address these challenges to ensure the resilience and protection of galactical systems through a mass team effort.

The rise of cybersecurity threats in space

In general, the space industry has been significantly slow to adapt to the changes brought about by rapid commercialization, leading to vulnerabilities in the system. Some spacecraft still rely on outdated software, like Fortran, and operating systems that haven't been updated for decades. Each satellite and ground station now represents a potential target, making robust security measures throughout the space supply chain an absolute necessity.

Additionally, cybercriminals are becoming bolder than ever before. The allure of the space sector to these criminals stems from the fact that satellites function as platforms with embedded systems and interfaces, akin to enterprise networks. Recent incidents, such as attacks on Viasat via supply chain vulnerabilities and threats against Starlink low earth orbit (LEO) satellites, underscore the vulnerabilities inherent in existing satellites. Therefore, the urgency to enhance cybersecurity measures and fortify the resilience of space systems against potential threats cannot be overstated.

The biggest threat in the space industry: supply chain management

The most significant threat facing the space industry currently lies in supply chain management and attacks. The commercialization of the sector, coupled with complexities in its supply chain, has led to concerns over cybersecurity vulnerabilities. According to global research, supply chain attacks surged by over 50 percent in the second half of 2022, further emphasizing the urgent need for action to mitigate these threats.

Additionally, organizations that rely primarily on off-the-shelf purchases from third-party suppliers face even more complexities in verifying security measures. The Viasat attack was a great example of this as it exposed supply chain vulnerabilities and highlighted the need for organizations to consider manufacturing certain components in-house, such as third-party modems and encryption platforms.

In light of the evolving threat landscapes, organizations must proactively address supply chain risks, by implementing robust supply chain security measures and forging strategic partnerships with trusted suppliers.

This is critical to bolstering cybersecurity in the space sector. As per the DCMS 2022 Security Breaches Survey, only 13 percent of respondents reported reviewing the cybersecurity of their immediate suppliers, while only seven percent went deeper into their supply chains. Ensuring that security measures are embedded and followed throughout the contract lifecycle is imperative.

By prioritizing this transparency and accountability across the supply chain, the space industry can strengthen its resilience against cyber threats and safeguard the integrity of space missions.

MISSION MICROWAVE

Family of X-, Ku- and Ka-Band BUCs from 8-800 Watts

STINGER

25 W Ka-Band

55 W Ku-Band

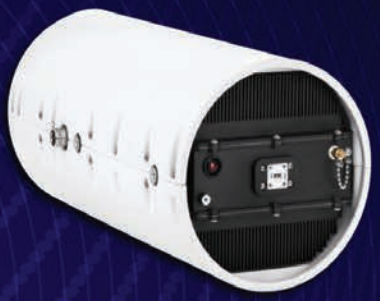
50/80/100 W X-Band

JAVELIN

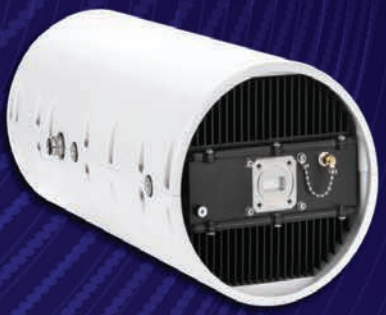
50/100 W Ka-Band

100 W Ku-Band

TITAN



200 W Ka-Band



200 W Ku-Band

The New Shape of Solid State

Available with Full Ka-Band Coverage for LEO/MEO/GEO Terminals and Gateways

Neil Sherwin-Peddie, Head of Space Security at BAE Systems Digital Intelligence

Mitigating supply chain risks through emerging technologies

To begin making the right steps in addressing supply chain risks, organizations are currently exploring technologies such as blockchain, artificial intelligence, and machine learning, to enhance supply chain visibility, traceability, and security. Regular security assessments and the application of these technologies greatly help to identify vulnerabilities and provide real-time monitoring of the space supply chain.

For instance, at BAE Systems Digital Intelligence, we embrace the DevSecOps lifecycle, promoting an agile approach to integrate the penetration test components regularly. This constant review cycle when bringing components together supports regular integration and penetration testing to ensure that operations are running as efficiently as possible. Multi-sensor satellite clusters, such as Azalea, also provide a more secure and innovative solution to conventional, single-purpose satellites. Existing space-based sensors require multiple terabytes of data to be transmitted to Earth before processing, a method that takes a significant amount of time and can be quite inflexible. Utilizing innovative technologies that exist in these multi-sensor satellites allows organizations to prioritize which data to analyze and also boost their ability to understand any emerging threats.

Another critical part of the Azalea program is the development of the Cyber Security Operations Centre (CSOC). To ensure effective cybersecurity defense, it's crucial to have a holistic understanding of data and processes in their entirety. The CSOC will serve as a single platform for consolidating information from different sources like the Space Operations Centre and Enterprise Operating Centres. This collective platform will help to detect potential threats and maintain a clear understanding of the overall health and security of the entire infrastructure.

Encryption also plays a pivotal role in safeguarding sensitive data and ensuring the effectiveness of its security even in the event of breaches. Continuous monitoring of network activity and data transmission can identify suspicious activities early on, mitigating potential risks thus acting as a powerful ally for organizations.

The bigger picture - looking at innovation in the space race

The space race is continually driving innovation, and multi-sensor satellite clusters present a pivotal opportunity to enhance cybersecurity in space. Among them, the Azalea multi-sensor satellite cluster stands out as a trailblazing example of cutting-edge technology, set to launch into low Earth orbit in 2025.

Azalea's advanced design incorporates a diverse array of sensors, including visual, radar, and radio frequency, allowing it to collect comprehensive and real-time data from space. The onboard machine learning capabilities are the key to Azalea's capabilities, as they enable the satellite to process and analyze the gathered data on edge processors while still in orbit, cutting processing times down from days to near real-time. By performing data analysis on board, the need to transfer massive amounts of data back to Earth for processing is eliminated. This not only saves valuable time but also reduces the vulnerability associated with data transfers between space and ground stations. This near-instantaneous data processing and intelligence delivery empower space missions with faster and more accurate insights, essential in today's fast-paced space environment.

As space missions become more complex and data-driven, Azalea and similar multi-sensor satellite clusters pave the way for a more secure and efficient space environment. The fusion of advanced sensor capabilities and machine learning technologies represents a paradigm shift in space exploration, offering unprecedented opportunities to tackle evolving cybersecurity challenges. With Azalea and other innovative satellite clusters leading the way, the space industry can bolster its cybersecurity resilience and stay ahead in the space race.

The space race is a team sport

Regardless of how innovative the solution is, the key to tackling threats lies in doubling down on collaboration. In the face of dynamic cyber threats and the new space race, the space sector must foster collaborative partnerships for information sharing. Sharing threat intelligence, best practices, and security information among key industry stakeholders, governmental agencies, and international partners can undoubtedly strengthen the overall security of the space supply chain.

UK agencies, alongside BAE Systems, the UK Space Agency, European Space Agency, and the wider ecosystem are already coming together to gain better visibility and address

Photo courtesy sdecoret/Shutterstock

security concerns. As we enter a new era in space exploration, we're met with many opportunities to adopt more agile and adaptable best practices to counter any upcoming threats and these can only be successful with effective cooperation and collaboration, not only in the UK, but globally.

Emerging cybersecurity trends in space exploration

As the commercialization of space continues to evolve, emerging cybersecurity trends have begun to shape the industry's future. Artificial intelligence and machine learning are finding applications in threat detection and anomaly identification. Autonomous response mechanisms can neutralize potential threats in real-time, reducing human intervention.

Moreover, quantum-resistant encryption is gaining attention as a way to protect data from potential future quantum computing attacks. Such encryption ensures that even with the power of quantum computers, hackers cannot breach the security of sensitive space data.

Additionally, space agencies are investing in improving the cybersecurity posture of their personnel through rigorous training programs. These programs help employees understand the evolving threat landscape and instill best practices for protecting sensitive information.

Looking ahead, the number of cyber threats in space will only continue to grow and become more complex. The ongoing cyber threats in the space sector demand a proactive response. By adopting cutting-edge technologies, integrating encryption, and monitoring, and fostering collaboration, the UK space industry can effectively navigate evolving cybersecurity challenges, stay ahead in the space race, and build a safer future.

With the increasing commercialization of space, organizations must strengthen their supply chain security through the adoption of best practices and emerging technologies. Through collaborative efforts and a keen focus on cybersecurity, the space sector can protect its advancements, explore further frontiers, and ensure the secure and prosperous future of space exploration. **GMC**

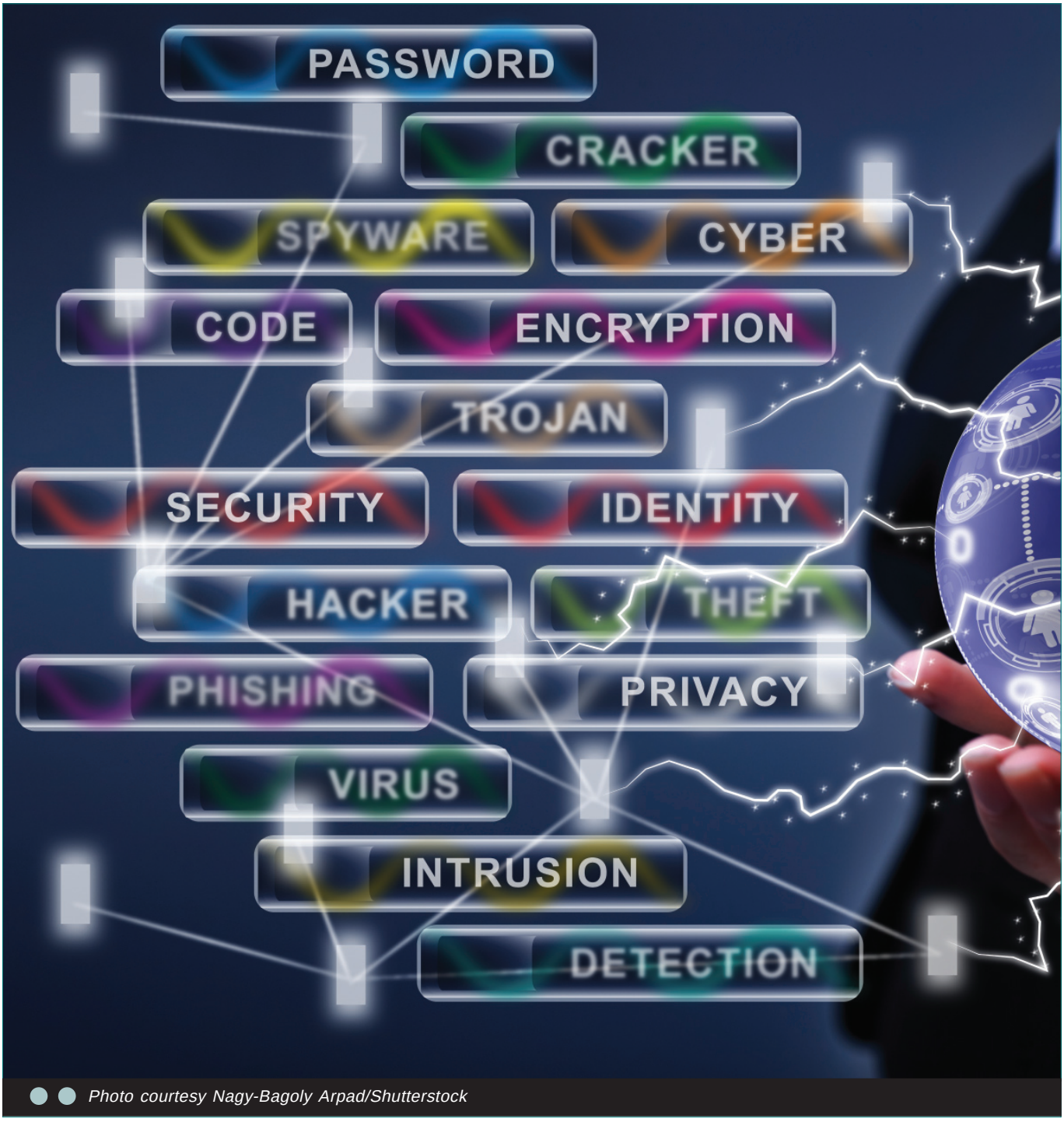


Photo courtesy Nagy-Bagoly Arpad/Shutterstock

John Moberly, Senior Vice President for Space, SpiderOak

GMC Q&A

On-orbit satellite cybersecurity

SpiderOak has partnered with leading defense contractors including Northrop Grumman, Lockheed Martin, Raytheon, and Ball to test and tweak its software-based end-to-end cybersecurity and resiliency solutions for government, military, and commercial space operations. In June 2023, the company successfully demonstrated its OrbitSecure software in low Earth orbit on a Ball Aerospace payload aboard a Loft Orbital satellite. We interviewed SpiderOak's Senior Vice President for Space, John Moberly, to find out how SpiderOak intends to deliver a disruption-tolerant space networking future.

Crispin Littlehales, Executive Editor, Satellite Evolution Group

Question: Please provide a summary of SpiderOak's expertise and evolution in the space industry. What portion of the company's efforts are targeted towards military users?

John Moberly: Just a few years ago**,** one of our existing customers challenged us with a surprising question: "Would SpiderOak be able to provide a similar, bullet proof solution for vendors and integrators who need end-to-end data protection for a space system?" The unique challenges, as compared to the others we had faced in the previous 12 years, were two-fold. First, satellite systems are intermittently connected networks and second all future architectures appeared to be on small, low-power devices connected in meshed networks. SpiderOak engineers are notorious for loving impossible challenges, so after working with potential customer experts in the space industry, we created OrbitSecure—a fully decentralized software platform for secure data orchestration (storage, transport, validation) in space. By "space" I'm not just talking about satellites. Yes, we protect the data that enters the satellite, the data that leaves the satellite, and the data that belongs to the satellite. But we are also protecting the uplink, the downlink, the ground stations, the antennas, and the terminals. In addition to securing the data in transit, we secure the data at rest.

We are bringing a software capability that is secure, distributed, and fully decentralized. We can upload it to various elements already in orbit, and we can build out new capabilities. What sets us apart is that we can update the on-orbit satellites. That is critically important. If you are not able to update on-orbit satellites and be backwards compatible with them, you're just creating your weakest link in space.

Right now, we are mostly targeting military and defense users. We just closed $16.4 million in an oversubscribed Series C round of fundraising. The OrbitSecure software with which we recently achieved flight heritage is already a minimum viable product. With this raise, we have the resources to further enhance our software and productize for the different space missions over the next year or two.

Question: The company has forged some interesting partnerships with TriSept, Raytheon, Lockheed Martin, and Ball Aerospace. What attracted these companies to SpiderOak and how are those partnerships unfolding?

John Moberly: Whether we're working with a vendor, integrator, or solution provider, it always starts with a question: how can SpiderOak help enhance my existing offering to meet zero-trust requirements in space and win contracts? Given the challenges of space – size, weight, power, connectivity – only a decentralized and asynchronous solution will actually work.

We've been told we are the only solution with a fully decentralized system for data orchestration across all domains—ground, air, sea, and space—and these partners were looking for an accelerated, proven pathway to meeting true zero-trust. All these relationships started with rigorous internal testing of our solution in their development environments, including flat sats, to confirm our small footprint, performance, and of course, security.

We do have working relationships with the satellite Primes including Lockheed Martin, Ball Aerospace, Raytheon and some who are notoriously secretive. We are also collaborating with other developers. A good example is TriSept, which is developing a secure operating system called TSEL. For all the companies with whom we work, we always aim to be the valued mission partner that can

solve secure and trusted data orchestration problems for them and their customers, typically government and military clients. So, those are true win-win partnerships in our eyes as well.

We have the OrbitSecure platform which is fully decentralized. It is built upon a foundation of zero-trust encryption and distributed ledger. It has role-based access control, identity management, and security. In addition, it has the peer-to-peer message queuing as well as peer-to-peer file sharing and storage. All of those together make up this baseline and then it's easily modifiable to suit the various needs of our customers. We don't get directly involved in sensor design or any of that, to us all those satellites are simply nodes in an autonomous network. The data going in and out of every memory stack is what we're protecting right through all the access points that we mentioned earlier.

The big goal right now is to create a fully resilient zero-trust mesh network in space so that information can be passed ubiquitously through other systems and reach the intended user, decision maker, or warfighter on the ground. Our strategic partnership with Raytheon Technologies' BBN division is all about developing and fielding a new generation of zero-trust security systems for satellite communications in proliferated low-Earth orbit (pLEO). We are combining OrbitSecure with Raytheon BBN's Distributed, Disrupted, Disconnected, and Denied (D4) secure cloud solution to ensure resilience of mesh networks in contested environments.

Many companies are talking about doing distributed architectures and on the government side, the Space Development Agency (SDA) and a couple of other groups are moving aggressively into that, but the space sector is still in the early days. Even the Starlink constellation is not a fully meshed network.

SpiderOak makes a very lightweight software protocol, a very thin client if you will, that can be uploaded onto existing systems in space. That's not easy. When you take into consideration orbital speeds and the vintage of some processors, you have a very limited amount of time to upload. On June 22, we were able to successfully deploy our OrbitSecure software and integrate it into Ball Aerospace's hosted payload in LEO, making it the first time a zero-trust application has been performed in space. That was a significant achievement for us.

At present we are continuing to validate the entire baseline platform in the operational space environment. But then, as we tailor and modify it for specific use cases, we are also creating and proving multiple product lines.

Question: An increasing number of MilSatCom satellites are in orbit today with more scheduled to be launched. What portion of these systems are vulnerable and are there ways to make all of them cybersecure?

John Moberly: Securing satellites is, in many ways, much more difficult than terrestrial cybersecurity. But in some ways, it is safer. If we assume that the supply chain and the satellite are fully secure going into orbit, then the primary ways in are through the uplink and downlink. We can secure those with our role-based access control so that when an adversary or any malicious code that doesn't meet that authority and permission tries to enter, it will be denied. That is the key part of what SpiderOak delivers at the intersection of space and cyber.

Question: How can security software be uploaded on-orbit and what are the challenges to making that option a widespread reality?

John Moberly: It starts with having a software-only solution – built in a memory-safe language like Rust — that can not only work on new hardware but legacy, flight-heritage hardware that many satellite systems continue to employ. But it's not just having a small memory and storage footprint, our entire platform

Photo courtesy Toria/Shutterstock

is built around an asynchronous protocol that works over slow and intermittently connected networks. We're able to upload just as we demonstrated on the Ball Aerospace payload which incorporated Ball's Open Software System (BOSS) framework, which is made for swift data processing and modification of applications on-orbit. That was just the first demonstration, we have more planned on other satellites and ground systems. Our first was challenging in and of itself because the satellite was small, so it didn't have big antennas and it didn't have big link budgets.

Question: During any military mission, secure and trusted data must move from sensor to shooter/decision-maker while traveling through many nodes of variable trust. How can warfighters trust that the data hasn't been tampered with during that entire chain of custody?

John Moberly: Since our platform is role-based access control by design, you must have the authority and permission to even get in. What's more, our software has a distributed ledger which works much like the traditional blockchains used in cryptocurrency.

You can see the full data provenance from the sensor all the way down. This makes it easy to determine whether anything has been tampered with in transit throughout the chain of custody. That's 90 percent of the battle right there.

Understanding that the warfighter who is in the battlefield needs to know immediately if the data is secure, we are developing a simple automated way for checking that the data provenance has been held throughout. We are envisioning using something like a red or green light as an indicator. We will also have a graphic user interface that enables monitoring of our software for both safety and some of the data provenance capabilities.

Question: Relying only on hardware encryption significantly increases latency while also causing a timely and complex re-keying process if there is any compromise across any node in the architecture. How can SpiderOak mitigate that particular risk?

John Moberly: Traditional authentication using just hardware involves going back to the central data center for authentication then back up to the satellite. SpiderOak's software works with any encryption, and we can decrease the latency and increase the agility of the queuing system. Since our system is fully decentralized the message queue handles all the authentication back and forth in a peer-to-peer manner continuously. Many of our partners also use hardware encryption on each link of their system, whereas we provide encryption end-to-end, regardless of the number of hops from source to destination: this provides a significant latency and power advantage over traditional approaches.

At the same time, we're changing the keys and doing what we call expert key management but without doing the encryption and without doing the ECU because we don't want to get involved with the whole NSA certification process at this point.

Question: Can your platform be deployed to satellites in LEO, MEO, and GEO?

John Moberly: To us, it doesn't really matter which orbits the satellites are in, or even how many different data paths need to be protected. Again, they are just nodes in an increasing complex network. However, we must be able to integrate into different types of hardware because of some challenging radiation environments that some processor hardware was designed for. Our software is also agnostic when it comes to encryption algorithms, we can use off the shelf commercial encryption or customer directed special purpose software – plug and play if you will. We've already worked with multiple types of processors and even have a project destined to land on the Moon. Although it was quite difficult to embed software into that operating system, we did it.

Question: Is it possible to stay a step ahead of hackers and other bad actors when it comes to cybersecurity?

John Moberly: It's very difficult. We feel that prevention is 90 percent of the cure, and you can get that from our software through the authority and permission access controls which makes it incredibly difficult to infiltrate. Our customers are especially interested in our solution because it works well in the protection of completely autonomous systems, like those out there alone in space.

Question: How do you see things unfurling for SpiderOak in the next 1 to 5 years?

John Moberly: We have the resources to continue to evolve our initial set of products that are currently at the minimum viable product and proof of concept stages. Meanwhile, we are starting to sell those products off the shelf with enhancements and some operation maintenance such as sending updates. We will then start scaling up because as we solve more of the real operational challenges our customers encounter, we'll take on even harder engineering problems, but always building from the decentralized, secure data transport platform. The goal is to create assets that will continue to matter well into the future. **GMC**

Photo courtesy SpiderOak

Focus Day:
SATCOM ON-THE-MOVE
November 6
The Royal Horseguards Hotel, London, UK

Conference:
GMSC MAIN EVENT
November 7-9
QEII Centre, London, UK

Lead sponsor
AIRBUS

Brought to you by:
SAE MEDIA GROUP

GLOBAL MILSATCOM
CONFERENCE & EXHIBITION

25TH ANNIVERSARY

Celebrate, Connect and Collaborate with the World's Biggest MilSatCom Community

1000+	80+	45+	35	4	3
ATTENDEES	CONFERENCE SESSIONS	NATIONS IN ATTENDANCE	EXHIBITION STANDS	TOPIC-LED STREAMS	EVENING RECEPTIONS

Join those who are shaping the future of MilSatCom in the arena's pre-eminent forum

Vice Admiral Dr. Thomas Daum, German Federal Armed Forces

Lieutenant General Elanor Boekholt-O'Sullivan, The Netherlands Ministry of Defence

Lieutenant General Carlos Enrique Chavez Cateriano, Peruvian Air Force

Air Vice Marshal Paul Godfrey, UK Space Command

Major General Philippe Adam, French Space Command

Cordell DeLaPena, Space Systems Command, USSF

Air Vice Marshal Dhananjay Vasant Khot, Indian Defence Space Agency

Major General Hans Folmer, NATO Communications and Information Agency (NCI Agency)

Major General Karsten Stoye, EUROCONTROL

Major General Elma de Villiers, South African Air Force

Find out more here: **www.globalmilsatcom.com** or **call +44 (0) 20 7827 6024**

Mobile infrastructure. Photo courtesy Illuminate

The emergence of Private 5G networks in US military bases for enhanced communications security

The need for secure and effective communication is paramount for military organizations, as the transfer of sensitive information and real-time data is crucial for their operations. With the advancement in technology, military bases are transitioning from traditional communication systems to more advanced networks. One such development is the adoption of Private 5G (P5G) networks in US military bases. Despite the assumption that military bases are already equipped with such advanced technology, many bases still rely on outdated equipment and methods for data transmission.

Gregg Melanson – Chief Growth Officer, Illuminate

Traditionally, military bases have relied on landlines, 2G, and 3G networks for communication and data transmission. These older methods not only lack the desired level of security but also have significant limitations in terms of speed and data capacity. The vulnerability of these systems makes them susceptible to cyberattacks and espionage activities. As such, military bases are exploring the potential of P5G networks to enhance their communication systems and improve overall operational efficiency.

P5G networks: benefits and advantages

Enhanced security: P5G networks offer a higher level of security compared to their predecessors. By using advanced encryption techniques and network slicing, P5G networks can isolate and protect sensitive data streams, making them less prone to cyberattacks and unauthorized access. The implementation of zero-trust security models and the use of end-to-end encryption methods further fortify the network's defense against potential threats.

Improved data transmission speed and capacity: 5G technology is capable of transmitting data at incredibly high speeds and in larger volumes compared to previous generations. This increased capacity enables military bases to process and share substantial amounts of information quickly and efficiently, significantly improving situational awareness and response times during critical missions. The low latency offered by 5G networks also ensures real-time communication and data sharing, enabling prompt decision-making in high-stress scenarios.

Increased operational efficiency: P5G networks can facilitate the seamless integration of various communication systems, sensors, and devices within a military base. This interoperability can streamline operations and enhance coordination among different units, resulting in improved decision-making and overall efficiency. Furthermore, the flexibility of 5G networks allows for rapid scalability and adaptability, catering to the dynamic needs of military organizations.

Support for emerging technologies: As military organizations adopt innovative technologies such as Artificial Intelligence (AI), augmented reality and autonomous systems, the need for a robust and secure communication network

Gregg Melanson – Chief Growth Officer, Illuminate

becomes increasingly critical. P5G networks can support these emerging technologies, providing the necessary infrastructure for future advancements and capabilities. The integration of 5G with cutting-edge solutions like edge computing, drone swarms, and advanced surveillance systems can revolutionize military tactics and strategies.

Enhanced training and simulation: The adoption of P5G networks can greatly benefit military training and simulation exercises. The networks' high-speed data transfer and low latency can facilitate realistic and immersive virtual reality and augmented reality-based training, preparing soldiers for various scenarios and conditions. These advanced training methods can significantly improve the readiness and adaptability of military personnel in the field.

Challenges in implementing P5G networks

Despite the numerous benefits of P5G networks, their implementation in military bases is not without challenges. Key considerations include:

- **Cost and investment:** Deploying P5G networks can be costly, as it requires significant investment in infrastructure and equipment. Additionally, the ongoing maintenance and management of the network can contribute to the overall costs. Military organizations must weigh the benefits against the financial implications to make informed decisions regarding the adoption of P5G networks. Nevertheless, taking a long-term perspective on the investment can reveal the substantial advantages that come from enhanced operational efficiency, improved security, and the ability to integrate future technologies, justifying the initial costs, and fostering an advanced communication infrastructure.
- **Spectrum allocation and interference:** Spectrum allocation and management are crucial factors in the implementation of 5G networks. Military organizations must navigate the complexities of spectrum allocation while ensuring minimal interference with existing communication systems and civilian networks. By proactively collaborating with regulatory bodies, telecommunication providers, and other stakeholders, military organizations can successfully overcome spectrum-related challenges, leading to a more effective and secure communication network that meets both military and civilian needs.
- **Cybersecurity threats:** Although P5G networks offer increased security, they are not immune to cybersecurity threats. Military organizations must remain vigilant and adopt proactive measures to protect their networks and sensitive data from potential attacks. As they dedicate resources to continuous monitoring, regular updates, and advanced threat detection and mitigation strategies, they will significantly strengthen the security of their P5G networks, ensuring a robust and resilient communication system to counter evolving cyber threats.

The future of communications security on military bases

The growing interest in P5G networks among US military bases highlights the increasing importance of secure and efficient communications in an ever-evolving digital landscape. As these networks are adopted, military organizations must address the associated challenges and ensure the seamless integration of

SATELLITE
Evolution Group

Global content...Global coverage

Download on the App Store

GET IT ON Google Play

If your focus is the global Satellite, Space, NewSpace or Military sectors - look no further!

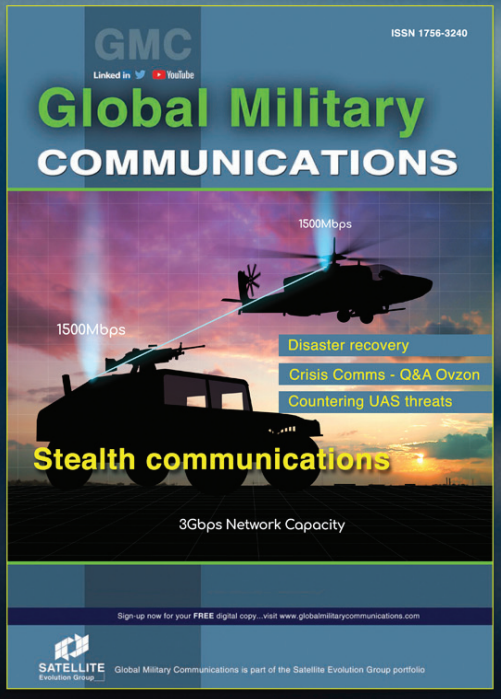


Photo courtesy Shutterstock/13_Phunkod

From print through to video, the Satellite Evolution Group has a solution to meet your company's corporate or product marketing plans

LinkedIn YouTube

www.satelliteevolution.com

these advanced systems into their existing infrastructure.

By embracing P5G networks, military bases can not only enhance their communication security but also prepare themselves for the integration of emerging technologies and advancements in the future. In turn, these improvements can bolster overall military capabilities, allowing for more effective and coordinated operations. This shift toward P5G networks has the potential to revolutionize the way military bases handle data transmission and communications, ultimately contributing to a stronger and more secure defense infrastructure.

In conclusion, the transition to P5G networks is a necessary step for US military bases to remain at the forefront of secure communication technology. By addressing the challenges associated with implementation and harnessing the advantages offered by these networks, military organizations can ensure a more robust and efficient communication system. Illuminate sees the adoption of P5G networks as a way to not only enhance the security of sensitive information and data but also pave the way for the integration of advanced technologies, fostering innovation and strengthening national security in the years to come. Military organizations must remain committed to investing in and exploring the potential of P5G networks, while recognizing their strategic value and the opportunities they present for enhancing the capabilities of the US armed forces. **GMC**

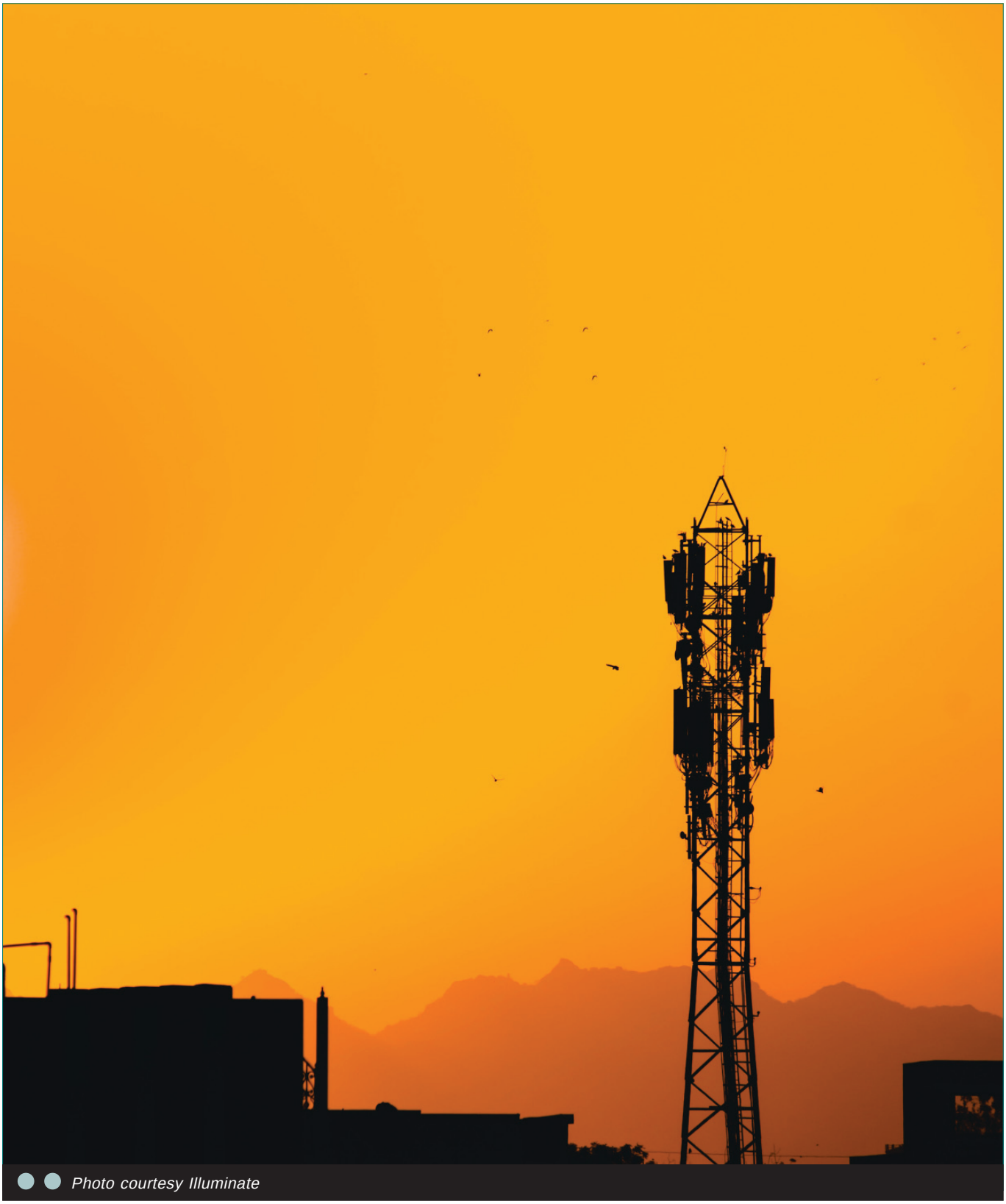


Photo courtesy Illuminate

GLOBAL CONTENT DISTRIBUTION

SATELLITE & IP | PLAYOUT & CLOUD | STREAMING & OTT | OCCASIONAL USE | CO-LOCATION SERVICES

WWW.STN.EU

SKYWAN – THE NEW DIMENSION IN AIRBORNE SATELLITE COMMUNICATION