GMC

May/June 2021

Global Military COMMUNICATIONS

Front cover photo courtesy of Ghost Robotics

Automation and AI in defence

Managing government data

Quantum technologies

Cybersecurity

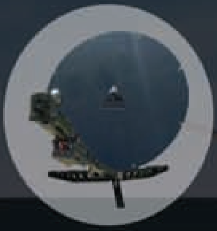
Sign-up now for your **FREE** digital copy...visit www.globalmilitarycommunications.com

SATELLITE
Evolution Group

Global Military Communications is part of the Satellite Evolution Group portfolio

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

Editor
Amy Saunders
amy.saunders@dsairpublications.com

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

Sales
Sam Baird
sam@whitehillmedia.com

Circulation Manager
Elizabeth George

Publisher
Jill Durfee
jill.durfee@dsairpublications.com

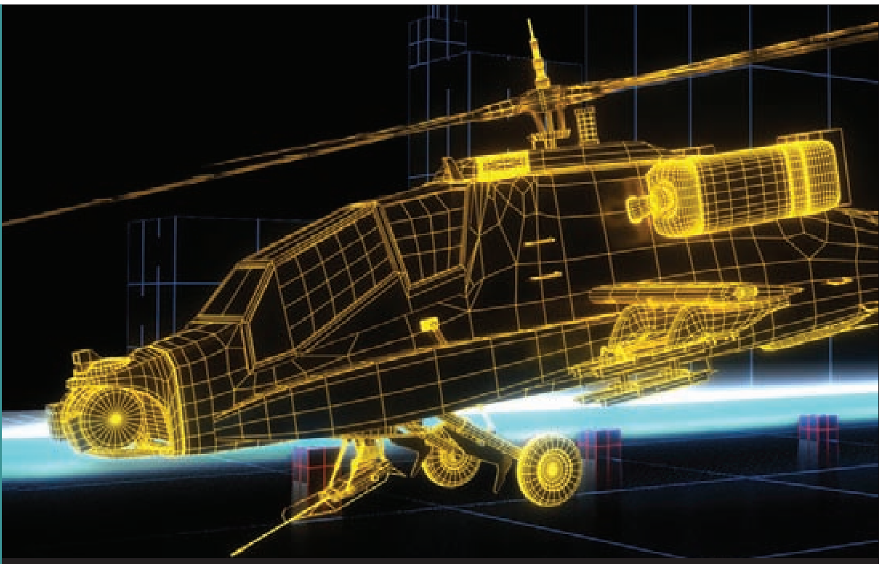
Marketing and Business Development
Belinda Bradford
belinda@dsairpublications.com

Publishing Director
Richard Hooper
richard@dsairpublications.com

Managing Director
David Shortland
david@dsairpublications.com

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

GMC



There has been a move toward integrating sensors into equipment to monitor the forces and environmental factors acting upon it throughout its service life. Photo courtesy QinetiQ. See page 24

Contents

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

Photo courtesy of Shutterstock

Silent Sentinel provides rapid delivery of Jaegar systems to East African customer

British threat detection specialist Silent Sentinel has signed a contract with Counter-UAS solution provider SKYLOCK to provide swift delivery of its Jaegar Ranger 225 uncooled LWIR, and Jaegar Searcher 700 cooled MWIR thermal camera platforms for use by an East African government, with a delivery time of six weeks. SKYLOCK is part of the Israeli Avnon Group.

In order to fulfil an unprecedented immediate operational requirement, Silent Sentinel will provide a Jaegar Ranger 225 LWIR uncooled thermal camera as well as a Jaegar Searcher 700 cooled MWIR thermal camera. The Jaegar Pan and Tilt unit (PTU) will form part of both systems.

The cameras will be mounted on vehicles and are well suited to drone detection missions. The Jaeger's unique through-shaft allows a radar to sit above the PTU enabling uninterrupted 360° continuous rotation, ideal for drone detection and tracking applications. The radar will be supplied by Observation Without Limits and C-UAS software provided by MyDefence, a subsidiary of SKYLOCK.

The Jaegar has a rapid release mechanism that allows for a range of interchangeable payloads to be mounted on the PTU making the platform extremely modular. The Jaegar is IP67-rated meaning that its ruggedized housing will ensure high performance even in the harsh conditions of East Africa. Suitable for mobile and vehicle-mounted applications, the Jaegar's through-shaft allows the camera to continuously rotate through 360°, offering effective long-range detection of small aerial targets whilst the vehicle is travelling over rough terrain.

Silent Sentinel was able to perform rigorous Factory Acceptance Tests remotely and will deliver the system less than six weeks after it was ordered, meeting the immediate needs of the customer rapidly and efficiently and demonstrating their ability to respond to exceptional orders.

James Longcroft, Sales Director at Silent Sentinel said: "This contract represents an opportunity to showcase the durability and accuracy of the Jaegar camera in Counter-UAS operations, as well as the agility and efficiency of Silent Sentinel in delivering the system despite such an unusually quick turnaround. This vehicle-mounted C-UAS solution is indicative of Silent Sentinel's position as a supplier of versatile threat detection in a broad range of climates and conditions."

Ofer Kashan, CTO of SKYLOCK said: "This first phase of delivery required an agile supplier with the ability to provide versatile and durable equipment within a short timeframe, and we are pleased to announce this partnership with Silent Sentinel, whose high-performance systems will operate seamlessly alongside our Counter-UAS expertise to meet the unique needs of our customer in this harsh environment."

GMC

Jaegar Searcher 700

SPACEBRIDGE
ALL THINGS CONNECTED
CONNECTING PEOPLE TO THEIR MISSIONS

Milrem Robotics' THeMIS UGVs used in a live-fire manned-unmanned teaming exercise

Photo courtesy Milrem

The Estonian Defence Forces Artillery Battalion used Milrem Robotics' THeMIS UGVs in a live-fire exercise to provide advanced situational awareness, conduct casualty evacuation (CASEVAC) and to support units manoeuvre while providing direct fire support from various positions.

During the exercise held in April, two THeMIS UGVs were used by the Artillery Battalion: the THeMIS Combat Support integrated with FN Herstal's deFNder® Light Remote Weapon System (RWS) with a 7,62 mm machine gun and the THeMIS Observe with Acecore's tethered drone.

The THeMIS Combat was tasked with supporting an advance force that consisted of an antitank weapons team and a forward observer's team. The main task of the UGV was to provide covering fire and support the retreat of the two teams to main positions as well as transporting their anti-tank weapons. At the main battle position the UGV was used for casualty evacuation.

The THeMIS Observe provided overwatch and enhanced the battalion's situational awareness. The use of a tethered attachment to the THeMIS UGV provides tactical units with 24 hours of constant observation of the operational area that is essential in the situational awareness prospective as well as peace time live-fire safety perspective.

"Taking part in the live-fire exercise of the Artillery Battalion was a great opportunity for us to validate our new infantry support UGV with end users in an actual combat scenario," said Jüri Pajuste, Director of Defence Research at Milrem Robotics. "The THeMIS Combat Support as well as other unmanned ground systems will enhance various combat capabilities and help reduce loss of life during combat operations," Pajuste added.

"We found several benefits in including UGVs into our battle scenario," said Lt Mari-Li Kapp, Commander of operations and training section (S3) in the Artillery Battalion. "Having UGVs as a part of the reconnaissance force that prepares the arrival of the main unit, the UGVs could secure the indirect fire and anti-tank teams by providing direct fire support during an engagement and whilst some units are withdrawing. UGVs could also act as front guards all by themselves since they can provide situational awareness and act as forward observers for indirect fire," she added.

GMC

General Dynamics Mission Systems delivers 500th radome for F-35 aircraft

Wideband radomes provide critical protection

General Dynamics Mission Systems has delivered the 500th wideband nose radome to Lockheed Martin for installation aboard US Air Force, US Navy, US Marine Corps and international military F-35 aircraft.

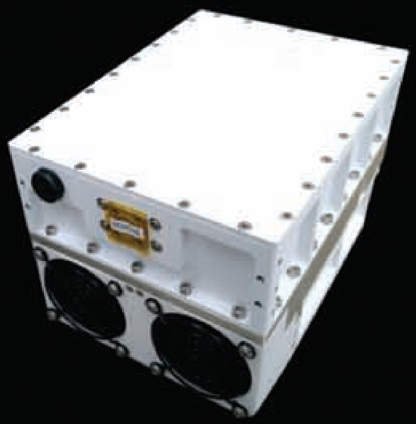
These radomes physically protect the aircraft's Active Electronically Scanned Array (AESA) radar, while minimizing radio frequency (RF) interference and reducing the aircraft's susceptibility from detection by enemy radar. The radomes were originally co-developed by General Dynamics and Lockheed Martin, with General Dynamics leading the RF design and Lockheed Martin leading the overall development effort.

"This milestone is an incredible example of our Marion team's 75-year commitment to successfully design, produce and test more than 65,000 radomes that meet the needs of more than 50 different types of aircraft," said Carlo Zaffanella, vice president and general manager at General Dynamics Mission Systems. "Our goal at General Dynamics is to make wideband radomes that protect aircraft and radar systems as they evolve and support increased functionality with as little interference as possible."

General Dynamics has designed and produced over 1,700 advanced wideband nose radomes specifically to support AESA radars on US and international military aircraft including the F-15, F-16, F/A-18 and F-35 platforms. Wideband radomes provide increased performance over legacy radomes by minimizing impact to RF performance over the much broader AESA frequency bands. This improvement enables F-35 pilots greater operating frequency space and provides maximum performance in target detection, tracking and mapping.

GMC

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*

JSTAR jet. Photo courtesy Boeing

Automation and AI in defence

With the increasing sophistication of automated mechanised assets, military effectiveness has the potential to rapidly advance in the near future, painting a picture of defence in which servicemen needn't risk their lives in the line of duty. Though the realities of automated locomotion and engagement is advanced enough, the communications infrastructure and security it requires is another massive challenge.

Laurence Russell, News & Social Editor, Global Military Communications

On 7 January, Milrem Robotics rolled out its new Type-X RCV combat vehicle, designed to support mechanized units as an 'intelligent wingman' to tanks and infantry vehicles. "The vehicle will be equipped with intelligent functions such as follow-me, waypoint navigation and obstacle detection with Artificial Intelligence being part of the algorithms," said Kuldar Väärsi, CEO of Milrem Robotics. "Milrem Robotics' software developers have taken a totally new and innovative approach to allow remote controlled operations on higher speeds."

The Type-X can be fitted with offensive measures such as various cannons, and is air droppable, making it a flexible asset. "The Type-X provides means to breach enemy defensive positions with minimal risk for own troops and replacing a lost RCV is purely a logistical nuance," Väärsi summarises.

The Type-X joins Milrem's portfolio besides the better known THeMIS platform, a smaller, more agile RCV intended to support dismounted units. When discussing a THeMIS field test conducted by the Estonian Defence Forces called Operation Barkhane in Mali, Lt Col Sten Allik, Senior Staff Officer of the Estonian Defence Forces remarked: "The possibility to detect and neutralize the enemy or an explosive device from a distance is a crucial capability. It is easier to risk the vehicle than a human life. If we can reduce the risk to life in combat situations, we can increase operational speed."

Automated assets such as these are becoming increasingly advanced, reliable, and most important of all, popular. January saw the US House of Representatives overwhelmingly pass the National Defense Authorization Act (NDAA), a US$740 billion injection which was filled with provisions explicitly aiming to stimulate the development and purchase of automated assets. The act will see automated systems continue to grow in ubiquity in the US military, likely also influencing NATO members and allied forces.

In its most idealised state, automation in defence need not exclusively shield the lives of their own personnel, but those of their enemies, by leveraging more instances of uncounterable force to motivate surrender scenarios, wishfully expanding the humanitarian scope of civilized terms of engagement.

Tom McCarthy, Vice President of Business Development at Motiv Systems Inc., one of the companies behind the InSight Mars lander, explains that US procurement decision-makers "have been leading the charge for automation as part of a multipronged approach. They want systems that play well together." This strategy can be witnessed in action across the theory and rollout of Internet of Military Things (IoMT).

Intelligence multiplication

In contemporary warfare, US forces and their NATO allies have favoured Boeing jumbo jets, known as JSTARS, as airborne control centres for C4ISR, capable of both recognising the state of an operational environment and suitably directing a joint-domain response.

Though once considered so high-altitude and well equipped with ballistic countermeasures they were well-protected assets, guided weaponry has proven advanced enough to render them more vulnerable targets. With the accuracy and power to put out a taskforce's eye in the sky, the intelligence network hub used by troops across an entire contested territory may be lost.

While the solution for some has been to move C4ISR hubs spaceborne on satellite platforms, or onto well-protected, hulking naval destroyers, these solutions merely mitigate the weakness of centralising network hubs by moving them further away or putting a stronger hull around them. Orbit-capable missile proliferation has become very healthy among the global powers, and ballistics at large have developed such stopping power that the number of earthly defences that can withstand them is dwindling.

The true answer is under development in theoretical defence sciences. Joint All-Domain Command and Control (JADC02) aims to mitigate the reliance on singular points of control by expanding the scale of the network. This is what Tom McCarthy means when he talks about systems playing well together.

In multiplying the number of peer-to-peer data links connecting ISR hardware to assets, the capacity to identify and destroy command nodes - and so cut off the head of a taskforce - becomes meaningless, since there are hundreds of decentralised heads processing and directing information independently. Like the mythical hydra, when one head is severed the beast lives on, and two more may grow back in its place.

Connecting every sensor to every operator, be they man or machine, is a spectacular task. While the weak links in the chains of command and intelligence are addressed, the thought of processing and applying data from thousands of eyes and ears into actionable insights for troops and drones seems near-insurmountable, though this is precisely what emergent technologies intend to deliver.

US R&D has already seen success networking mobile and immobile sensor units in test environments into networks weaponized by jet aircraft or missile drones. As remarkable as these breakthroughs have been, the practicality of comprehensive IoMT in the field, and the AI needed to turn the highly networked data it churns out into simplified, actionable leads for ground soldiers and unmanned units at pace remains in the realm of futurism.

Ethical AI

While remarkable, AI and robot assisted war is nothing to rush into; we'd be extraordinarily unwise to brush off the exasperated warnings of STEM academics, many of which are breathless with warnings of the danger in increasingly independent AI systems. Whilst many level-headed observers rightly scoff at the assumption that we're somehow satisfying the inciting incidents of so many killer-robot movies, experts insist on certain ironclad logical terms which will apply to a hypothetical mission-critical AI, namely the propensity for it to resist attempts to be turned off, and subsequently defending itself from such measures as its programming allows.

Sophisticated software involved in high-risk processes has already proven itself capable of preventing itself from being shut down, and experts insist the technical principle won't disappear in the case of a far cleverer and more aware system. The argument for ethical AI insists that machine learning systems of particular responsibility - like those capable of recommending or enacting the execution of human life - must be rendered morally fool proof before being put to use, or else we risk disasters on a level with Chernobyl.

While war hawks have no love of regulatory complexity and ethical handwringing, not least in the face of the quiet arms race exacerbating across the world's premier powers, it's unlikely history will remember them well for it. The modern pace of technology is faster than it has ever been, leading some thinkers to suggest it is outpacing our responsibility with it. With the doomsday clock ticked up to a hundred seconds to midnight as of January 2021, the developers in control of our world's most volatile innovations must tread carefully.

GMC

Milrem Robotics reveals Type-X robotic combat vehicle. Photo courtesy Milrem

John Vestberg, CEO and Co-Founder of Clavister

GMC Q&A

Cybersecurity in the defence space

With the threat of cyberattacks looming ever higher, the security of our digital presence has never been more relevant. Following on from their success contracting solutions for European vehicle cybersecurity in partnership with BAE Systems Hägglunds, we discussed the nature of the cyber domain with John Vestberg, CEO and Co-Founder of Clavister.

Laurence Russell, Assistant Editor, Global Military Communications

Question: From 2010 onwards, cyberwarfare has increasingly become understood as the fifth domain, which NATO formally recognised in 2016. Many of our defences have decades of experience and investment behind them, but the challenges of cyber are far newer. Are we taking the fifth domain seriously enough?

John Vestberg: Over the past decade there has definitely been an increased focus on cybersecurity in the defence space, but I think it's only very recently that it has become top of the agenda. In our ever-increasingly digital world, cyberattacks can have devastating effects. If we consider the major consequences poor cybersecurity has caused for businesses – take last year's SolarWinds hack which affected numerous organisations from US agencies like the Department of Homeland Security and the Treasury, to private companies such as Microsoft, Cisco, and Deloitte, for example – then the potential threat to people's lives cannot be overlooked.

It was promising to hear that following the Integrated Review, the UK Government proposed a new National Cyber Force, drawing personnel from the military, intelligence services, and GCHQ. This could well be a turning point for the UK's defence strategy and other countries in Europe not already setting out similar initiatives should certainly follow suit.

One area of cybersecurity that governments must be sure to take seriously is the upgrading of equipment and in particular the capabilities of combat vehicles. Using the UK as an example again, efforts to modernise the Army's fleet of Armoured Fighting Vehicles (AFV) have been, until now, described as 'woeful.' But globally, armoured vehicles are becoming what can essentially be described as data centres on wheels. Traditional windows have been replaced by cameras and weapon systems have evolved from triggers and gunsights to joysticks and screens. This myriad of connected devices and networks in one place is what

US Cyber Command. Photo courtesy of Clavister

makes vehicles a prime target for cyberattacks. It is essential that cybersecurity in combat vehicles is a priority.

Question: Oftentimes, the bottom line in procurement comes down to ensuring worst-case scenarios are accounted for. What's the worst a cybersecurity attack can do?

John Vestberg: Seemingly innocuous events can have a disastrous impact, so when we think about what's the worst that can happen it's best to be realistic. Take the insider threat, for instance, a commonly spoken about corporate cybersecurity risk that sees employees – or other closely connected parties who have insider knowledge of an organisation's security practices – using their intimate knowledge to access networks to cause havoc or steal data.

Now apply that thinking to a tank. If a rogue soldier from a third-party nation was to use their intimate understanding of an armoured vehicle's defences – or lack of – a simple hack could soon see them onto wider networks, conducting espionage, tracking vehicles, monitoring those inside vehicles, or disabling capabilities; all things you do not want and place nations at great risk.

Question: Clavister has recently announced a contract to embed cybersecurity solutions in combat vehicles in Europe, with a minimum of 122 CV90 fittings. Could you substantiate that process for us?

John Vestberg: In short, the contract agreed between Clavister and BAE Systems Hägglunds will see mid-life upgrades of 122 (with the option of a further 19) CV90s carried out between 2021-2025 for a major Western European military organisation.

The upgrades will include fitting each vehicle with more robust, embedded cybersecurity capabilities, including Clavister's military-grade RSG-400 security gateway and RSW-400 secure network switch. First shipments will take place in the second half of 2021 and the bulk of shipments will take place from 2022 through 2024.

The CV90 is a family of tracked combat vehicles first developed in the 1980s to cope with the extreme Nordic environments. The current model (MkIV) is suitable for high-tempo combat situations as it's designed for tactical and strategic mobility and survivability, with a high payload, air defence and anti-tank capabilities. The latest versions come equipped with a NATO-standard electronic architecture – driving the need for cybersecurity capabilities.

Question: You're working on this project with BAE Systems Hägglunds. How has your working relationship been with them?

John Vestberg: It's been a really great partnership so far and everyone at Clavister is proud to be working alongside BAE Systems Hägglunds to provide next-generation combat vehicle defences. This deal actually represents the biggest in Clavister's history and so it's a very exciting time for us.

Clavister and BAE Systems Hägglunds both appreciate that the solutions we are developing will play a critical role in keeping nations safe and are very much on the same page. Protecting military personnel has evolved so much further beyond simply adding thicker armour around combat vehicles and we are dedicated to helping defence organisations to better prepare nations for cyber warfare through specially developed solutions.

Question: This upgrade will utilize Clavister's RSG-400 security gateway and secure network switch. What are these solutions best at, and what are their differentiators?

John Vestberg: The RSG-400 will provide protection ensuring only cleared users, systems or protocols can connect to the vehicle. Built around Clavister's NetWall platform – based on the company's internally developed operating system and full cybersecurity technology stack – the firewall solution has been augmented based on NATO and BAE Systems requirements. Equipped with military-grade enclosure and connectors, its ruggedized hardware can withstand extreme environmental conditions and significant physical attacks.

In terms of the RSW-400 secure network switch, it's a newly designed ruggedized solution. It will boost the resilience of the onboard network infrastructure relied upon by the crew to manage the vehicle's many systems – such as weapons, cameras, battle command systems and engine control.

One thing that differentiates Clavister as a cybersecurity provider – and therefore the solutions we are providing BAE Systems Hägglunds – is how important our heritage is to us. Clavister is committed to the integrity and security of our

Photo courtesy of BAE Systems

customers' data so we keep the development of our solutions and operating system within Europe, we are deliberately doing this so that subjects are beholden to and protected by EU legislation only. No Patriot Act, no spyware, no backdoors, and no compromises.

Question: What's on the horizon for Clavister?
John Vestberg: We will carry our work with BAE Systems Hägglunds and continue to serve organisations in the defence space, with a focus on embedding combat vehicles and other defence platforms with cybersecurity capabilities. We have also already advanced our work to create 'Digital Soldier Identity' – a technology that will allow soldiers to use certain weapons and vehicle functions based on their digitally confirmed identity. What's more, Clavister is part of the Swedish Security & Defence Industry Association – an alliance to focus on defence innovation with a Swedish perspective – and will work with them to further secure Sweden's competitiveness globally.

Beyond this, Clavister brings European innovation and cybersecurity to organisations of all sizes around the world and the defence arena is just one piece of the puzzle for us. We have recently announced that we are providing 5G security to a LATAM telecoms provider and an Australian Public Safety Network, for example. Our overall mission is to give businesses and governments the perfect blend of mature technology and services platform designed to meet the increasing demands for end-to-end cybersecurity.

Question: What are your predictions for the realm of cybersecurity in the coming years?
John Vestberg: Defence is a different proposition now, and to help protect nations, armoured vehicles (and all other defence platforms for that matter) can no longer be overlooked when it comes to cybersecurity. Nations are already taking steps to future-proof their combat vehicles but must continue to do so and constantly re-evaluate their defences. In today's digital world, cyberattacks will only get more sophisticated.

To ensure only those with the right clearance, alongside approved systems, and protocols, can connect to the vehicle, network security gateways with highly tested, robust next-generation firewalls should be embedded. Similarly, on-board network switches will boost the reliability of the on-board network to ensure consistent availability so the crew can manage the many in-vehicle platforms, such as weapons, cameras, battle command systems and engine control. They have to have the assurance that in the heat of battle, the network will perform.

What's more, we are entering a new era of hybrid working, spurred on by the pandemic. That means organisations and governments working in the defence space in-house need to adopt genuinely robust, but flexible, security measures such as SASE – secure access service edge. Security needs to span on-premises and the cloud, protecting every corner of the decentralised network while providing the flexibility for employees to work as freely and securely as they can under the protection of the traditional, centralised corporate network.

SASE effectively brings together all the most important security elements, such as SD-WAN, SWG, CASB, ZTNA and FWaaS, into one solution so that businesses possess the capability to truly secure data and networks from leaks and attacks as networks expand. With functions hosted in the cloud rather than at the network edge, it can scale as needed with all the necessary rules set centrally to ensure businesses remain in control. This is critical because if the past 12 months have taught businesses leaders anything, it's that cybersecurity must be flexible to allow for a suddenly remote workforce, without restricting employees from doing their jobs. **GMC**

Digital Cloak has effectively supported the Marine Corps since the company's inception, in addition to its work for other components of the US Armed Services. Photo courtesy of Clavister

Considering the security implications of managing government data

Nicola Bradshaw, Director, UKCloudX

Governmental data is some of the best-protected data in the world, and for good reason. As technologies have advanced, and with increased dependence on the cloud, the security of government data has become less clear.

Nicola Bradshaw, Director, UKCloudX

Concerns around data privacy are growing – almost as fast the amount of data being generated by our increasingly digital industries. Every engagement and interaction leave behind a footprint, and these footprints can be traced back to their source with the right tools and expertise.

This may be an uncomfortable truth, but the consequences of highly sensitive information falling into the wrong hands become unthinkable when we're talking about national security.

The many subtleties around data governance mean the lines remain blurred, however. Who owns the data when data centres are oceans apart? Which government ultimately holds the responsibility for ownership? Without understanding these subtleties, organisations can also risk breaching data control regulations, and face serious financial penalties.

Data sovereignty is a compliance minefield, and one which government agencies need to get to grips with. After all, data breaches at this level could pose a real, tangible threat to national security.

Digital transformation

The impact of the Coronavirus pandemic has forced many businesses and organisations in both the private and public sectors to speed up their up their digital transformation. In the NHS, the adoption of remote consultations, collaboration tools, and digital appointments has been pushed through very quickly, with little cultural resistance. Across the rest of government, progress has been patchy.

Photo courtesy Shutterstock

But COVID has proven not to be a short-term issue. Government departments and agencies should invest instead in longer-term, more sustainable solutions as they turn toward digital to see them through this new normal. It's vital that they consider the implications of using consumer-grade technology and what it means for the privacy and security of sensitive data. Indeed, there are tools and platforms which can ensure that this can be done securely, but some sensitive data is not as safe as many people might think.

Cloud concern

The think tank CEPS estimates that 92 percent of the western world's data is currently stored in the US, and an increasing amount of that data is held in the cloud. The risk of data concentration and a near data monopoly will do nothing to drive competition, innovation, or value, and in turn the UK could ultimately be deprived of digital resilience, sovereignty over its data, and freedom of action. Hence as the political, economic, and military value of data is better understood, the scramble for data sovereignty is seen by some as the next arms race.

The EU-US Privacy Shield was approved in 2016 as a means of ensuring that the transfer of commercial data between the US and the EU complied with EU data protection requirements. But, invalidated by the European Court of Justice in July 2020, it no longer affords data subjects any protection. As a result, many of the standard terms and conditions included in an organisation's contract with the big US-based cloud providers are no longer valid.

When you consider that one of President Trump's last official acts was to sign an executive order under which those cloud providers were required to keep a wealth of sensitive information on their foreign customers, it's surprising that more people aren't concerned about the fact their data is held on Amazon, Microsoft, and Google's cloud services. This CLOUD Act also allows US federal law enforcement to compel US-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the US or on foreign soil.

The European Data Protection Supervisor (EDPS) viewed the CLOUD Act as a law in possible conflict with the GDPR and

IBUC G
IBUC 2
New
IBUC 3

the German data protection watchdog has warned against the use of US based Amazon Web Services for storing sensitive data for the Federal Police.

The fact is many people simply don't understand the issue. Some may think it's part of an ongoing legal wrangle, while others feel overwhelmed at the prospect of retrieving their data from AWS or Azure to be stored elsewhere. Until they're mandated to do so, they'll just ignore it.

Guidance from the Cabinet Office and GDS, however, explicitly recommends these service providers as part of its Cloud First policy. Rather than carrying out data protection impact assessments to validate whether they should be storing sensitive government data in a public cloud, many departments will assume that, because GDS has approved them, it's perfectly safe to use those providers. Without the protection afforded by the Privacy Shield, classified data like that generated by the MoD or the Police should really be held with sovereign cloud providers instead.

Accidental breaches

This lack of understanding of the subtleties of data sovereignty can result in government agencies – often unwittingly – breaching export regulations. Export control legislation, for example, requires potential exporters of controlled items, such as missiles or sonar buoys, to make a request to a local government department who will either grant or deny export licenses as appropriate.

There are strict requirements around the handling of data related to export control – particularly when it's highly sensitive or classified – and storing such data in AWS or Azure can theoretically break export control regulations. Even though the data itself originates from the UK, the administrators of those cloud services are actually located in Dublin or Amsterdam. Without knowing it, the party managing the data has accidentally breached several controls. The penalties for doing so can be eye-wateringly high and, in some cases, even result in prison sentences.

Not only can regulatory breaches be expensive, but government departments also can't afford for classified information to fall into the wrong hands. Thought must be given to the tools they use to share that information, and where best to store it – for the sake of national security **GMC**

Photo courtesy Adobe Shutterstock

Proven Performance for
Mission Communications

Andrew Forbes, Managing Director at MARSS' KSA Office

GMC Q&A

Innovative situational awareness

MARSS' land and marine detection systems provide innovative situational awareness making use of the latest data technology and autonomous systems. Andrew Forbes, Managing Director at MARSS' KSA Office and Signal Corps veteran, opines on the state of evolving global threats, and how MARSS and the defence institutions they serve can address contemporary threats.

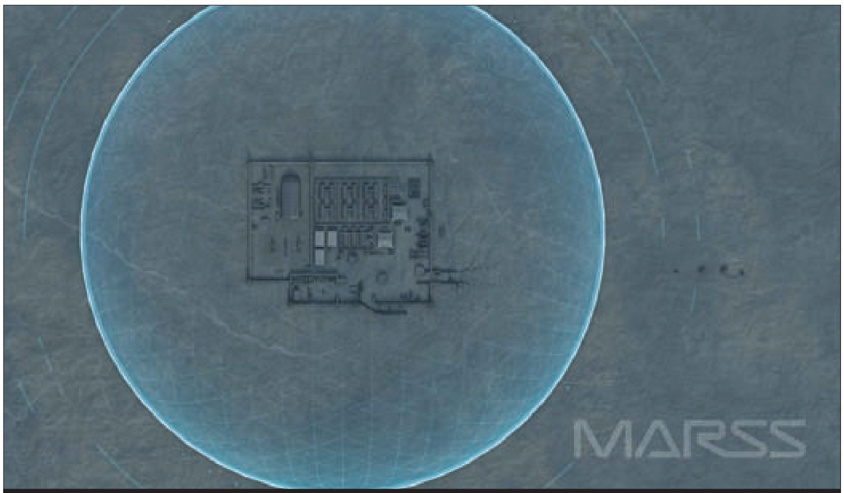
Laurence Russell, Assistant Editor, Global Military Communications

Question: Given your 26 distinguished years of service in the Royal Corps of Signals – including deployments in Afghanistan and Iraq – what do you believe are the most important priorities for ISR and communications technology?
Andrew Forbes: Combining service and business I have 38 years of familiarity with military communications. I have seen a lot of reliance on communications systems being based around insecure and secure voice systems. And yet the 'digital natives' of today mainly depend on chat-based communications systems that are less bandwidth-intensive and less susceptible to latency and jitter requirements. I feel that the greatest priority for ISR is to ensure that we can deliver mission-critical or disaster critical data and process it in a time frame that can enable decision-makers to make better-informed decisions.

Question: Your land-based assets protect VIP residences, ports, critical infrastructure and even the Olympic Games. How does providing civil defence change from conventional military scenarios?
Andrew Forbes: Providing a civil defence 'bubble' is an even greater challenge than a traditional military scenario. This is because VIP locations, ports, critical infrastructure and large events are often situated in areas where there can be a greater impact on people and infrastructure. Where possible, the use of effective non-kinetic responses to counter the threat is key to ensuring that minimum risk to the population and surrounding infrastructure.

A civil defence bubble can also have the added complication of having multiple defence and support organisations competing for the same communications spectrum. Coordination is therefore vital to ensure that one organisation's effector does not negatively impact the operations of another organisation's defence system or effectors. Command, control and communications are all essential when working in a civil defence scenario.

Question: Following the incident at Heathrow, a great deal of concern has surfaced for how mission-critical technologies detect, identify, and respond



360° Surveillance. Fusing sensor data, intelligence and counter measures for the protection of assets and lives. Photo courtesy MARSS

to drones. A conversation that soon branched to fears of autonomous swarming technologies. What are your views on the matter?

Andrew Forbes: The drone incidents at both Heathrow and Gatwick identified that there were weaknesses in the authorities' ability to detect, identify and react proportionally to drone encroachments within an airport's operational areas. This has led to a change in the law and a change in the operational area of the airports within the UK.

Although the drones used for Heathrow and Gatwick were CAT 1 drones, rather than CAT 2 attack drones, they still pose a significant threat and can be used for intelligence gathering. They can be inherently dangerous if the goal of the attacker is to overwhelm the operators of the defence systems and therefore break through the defence bubble. If there is a threat of autonomous swarming technologies, there has to be investment into autonomous swarming counter technologies that are tested regularly by the operators. This type of training also needs to be scheduled and unscheduled to ensure the team is ready for all eventualities.

Question: With the increasing complexity of digitization and automation, threats have never been more complicated. With many military operators on the verge of being overwhelmed by excessive data streams, how can our personnel keep up in worse-case scenarios?

Andrew Forbes: Military operators have continually adapted to changes in complexity throughout the years and I am sure that they will adapt to the increasing complexity of digitization and automation going forward. Operating in this type of environment can be both stressful and exhilarating for the operator, who must continually scan for threats and anomalies in a sometimes-unchanging environment.

I believe this is where the benefits of artificial intelligence (AI) can provide an effective solution. The technology can do much of the heavy lifting of identifying objects and correlating information for the operator to act on. It can then support a highly motivated, professional and trained operator to ensure the correct decisions are made in response to the threat after detection and identification. I believe that after initial training on the systems the operators need to stay fresh, and training should be conducted continually to ensure that reaction times are in line with the threat.

Question: Your NiDAR system uses IoMT to merge several ISR tools in concert to increase response times. Are autonomous systems like this the future of military electronics?

Andrew Forbes: I believe the beauty of NiDAR as an autonomous capability is that it gives the operator an agnostic platform with which to operate multiple sensors. Depending on evolving requirements the sensors can be changed whilst the platform remains the same. Autonomous capabilities offer MARSS the ability to enhance and improve the capability for the user to recognise and analyse multiple unknowns.

These can be used not only for defensive missions but also for disaster relief scenarios and supporting aid agencies. The IoMT is a living and fluid capability that needs to continually evolve and develop to ensure that it meets the requirements of the customer. NiDAR is a living part of the IoMT and data from NiDAR, its sensors and its use by the operators adds to this living capability. IoMT also means NiDAR and MARSS needs to be adaptable to new updates across the spectrum of IoMT.

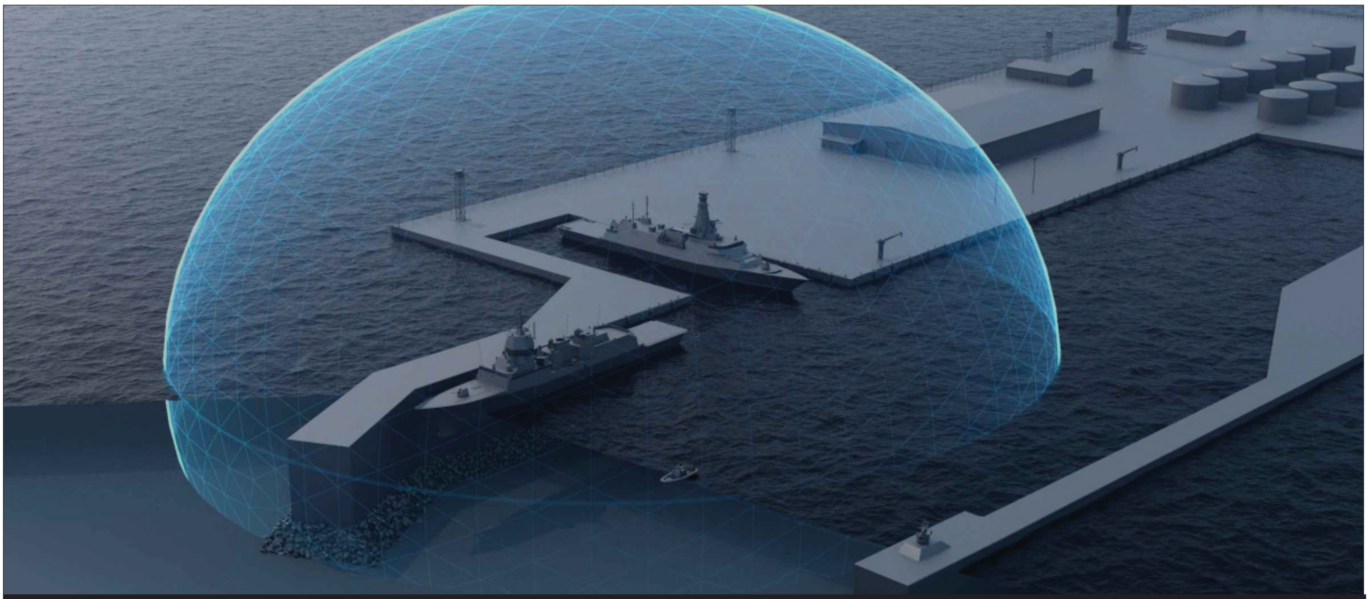
Question: As a veteran and executive of the defence industry, what do you think modern militaries ought to be emphasising when it comes to technological procurement?

Andrew Forbes: I have witnessed the development of systems to fight the wars of yesterday and not of today or tomorrow. Size and cost mean that by the time you have developed the capability to meet the requirements of the warfighter or defence organisation the requirements have changed, or it is too late.

I have been involved in delivering systems that are obsolete by the time they are delivered and not what the customer now needs. Agility and capability form is key to ensuring that the military's requirements to face and defeat asymmetric threats are achievable. I have heard talk about being lean and agile, but this leanness and agility come at a cost. Not just the cost of the equipment but also the support and training.

Question: What are MARSS' plans for the next 2-3 years?

Andrew Forbes: I am hoping that in the next 2-3 years that MARSS will continue to deliver, develop and enhance the functionally and capabilities of NiDAR. This evolution needs to meet and exceed the satisfaction of the customer as their requirements develop over time and their understanding of NiDAR grows. Our strength is adapting to the changes in our customers' requirements and the change in sensor capabilities. MARSS is growing at a rapid rate and like any growth there are pains, but I believe this growth is sustainable if we follow our core MARSS-ian values. We pride ourselves on customer centricity, being a trusted partner; having mutual respect; providing continued innovation and improvement; teamwork and championing localisation. **GMC**



Artist rendering illustrating MARSS' security concept. Photo courtesy MARSS

One quantum leap forward

Quantum technologies have been quietly edging their way into reality these last few years, largely overshadowed by showier aerospace developments, but no less critical to the future of secure communications. The new quantum capabilities bring with them a great deal of promise for hack-proof communications which should prove extremely advantageous for defence, government, and corporations across the globe.

Amy Saunders, Editor, Global Military Communications

Although quantum communications via satellite have long been theorised, it's only in the last five years that we've started to see real-world developments taking place. Ultimately, quantum communications are expected to enable fully hack-proof, secure means of communication, with expected uptake in the defence, government, and corporate sectors.

In quantum communications, particles (usually photons) take on a state of superposition, meaning that they can represent multiple combinations of 1 and 0 simultaneously. Thanks to the laws of physics, should a hacker attempt to observe these particles, the quantum state collapses, and the attempt is easily discovered. Accordingly, entities exploring quantum communications are developing quantum key distribution (QKD), in which encrypted data is transmitted as usual over networks, while the keys for decryption are transmitted in a quantum state, often via satellite.

China establishes world's first integrated quantum communication network

Regarded as the first modern quantum communications experiment, 2016 saw China launch the Quantum Experiments at Space Scale (QUESS) satellite, also known as Micius. The experiment set out to demonstrate quantum encryption over long distances. Micius produces a pair of entangled photons that enables ground stations separated by thousands of kilometres to establish secure quantum channels.

In 2017, the Chinese team used Micius to perform the world's first quantum-encrypted virtual teleconference between Beijing and Vienna. However, a flaw was highlighted – that Micius itself 'knew' the QKD, which would enable a hacker to compromise its security. To overcome this problem, the team relied on the satellite exclusively for transmitting the QDK to two ground stations in China in order to establish a direct link, which was successful.

The latest news from the Chinese experiments is the establishment of the world's first integrated quantum communication network, which combines more than 700 optical fibres on the ground with two satellite-to-ground links to achieve a QKD over a total distance of 4,600km across the country. Using trusted relays, the terrestrial fibre network and the satellite-to-ground links were integrated to serve more than 150 industrial users across China, including state and local banks, municipal power grids, and e-government websites.

Over the last few years, the integrated network has undergone extensive testing and improvement. So far, the clock rate has been increased and a more efficient QKD protocol has been developed; the satellite-to-ground QKD now has an average key generation rate of 47.8kbps, some 40 times higher than the previous rate. Researchers have also pushed the record for ground-based QKD to beyond 500km using a new technology called twin-field QKD (TF-QKD).

Going forwards, the team will further expand the network in China and with their international partners from Austria, Italy, Russia, and Canada. They also aim to develop small-scale, cost-

Photo courtesy of SECTRA

efficient QKD satellites and ground-based receivers, as well as medium and high Earth orbit satellites to achieve all-time, ten-thousand-km-level QKD.

India demonstrates free-space quantum communication

In March of this year, the Indian Space Research Organisation (ISRO) successfully demonstrated free-space quantum communication over 300m. Several key technologies were developed indigenously to accomplish this feat, which included the use of an India-developed NAVIC receiver for time synchronization between the transmitter and receiver modules, and gimbal mechanism systems instead of bulky large-aperture telescopes for optical alignment.

The demonstration has included live videoconferencing using quantum-key-encrypted signals, a major milestone for unconditionally secured satellite data communication using quantum technologies. The QKD technology underpins quantum communication technology that ensures unconditional data security. The free-space QKD was demonstrated at Space Applications Centre (SAC), Ahmedabad, between two line-of-sight buildings within the campus. The experiment was performed at night in order to ensure that there is no interference of the direct sunlight.

The experiment is a breakthrough towards ISRO's goal of demonstrating Satellite Based Quantum Communication (SBQC), where ISRO is gearing up to demonstrate the technology between two Indian ground stations.

A race to a quantum future?

China and India are far from alone in their embrace of a quantum future, although less is known about others, or else the projects remain in their infancy.

In Europe, the Quantum Internet Alliance is ramping up under a Euro 1 billion Quantum Flagship project. The work towards establishing a quantum industry consortium started in early 2020, when the Quantum Community Network, one of the three governing bodies of the Quantum Flagship initiative, expressed the need for a privately owned body with the mission to advocate, promote, and foster the common interests of the European Quantum Industry. The long-term vision is a 'Quantum Web' of computers, simulators and sensors interconnected via quantum networks distributing information and quantum resources such as coherence and entanglement.

In the US, NASA has initiated the development of a National Space Quantum Laboratory (NSQL) that would use lasers on the International Space Station to achieve secure communications between ground stations. The NSQL will enable entanglement-based quantum network demonstrations over satellite-based downlinks and crosslinks, while the use of the ISS will allow for collaborative use by the quantum research community to characterize new technologies and emerging applications such as improved timing and synchronization systems, distributed sensing, and quantum computation.

Meanwhile, Singapore and the UK have partnered to build and operate a satellite QKD test bed under a US$13 million jointly funded research programme led by the Science & Technology Facilities Council (STFC) and the Centre for Quantum Technologies (CQT) at the National University of Singapore (NUS). The economic impact of this new joint quantum technology satellite mission means access to a global market thought to be worth up to $16.1 billion over the next ten years. The scientific impact of the collaboration will build on both countries' efforts to grow the space and quantum technologies sectors by staking a claim in the emerging QKD market. The satellite is planned to be operational later this year.

Quantum in the field

Quantum technologies are already making their way into the field too. In March, the EU council approved the latest iteration of the Sectra Tiger/S 7401 LTE secure 'eavesdrop-proof' mobile phone. The Sectra Tiger/S is quantum-proof, providing communications capabilities secure from any possible attack.

Photo courtesy Shutterstock

This latest version provides improved file transfer and chat as well as support for all fixed and mobile 4G networks within Europe. These new features provide improved availability, while also enhancing the user experience and areas of application. The voice and file transfer features are approved for use up to and including the security level SECRET UE/EU SECRET. The messaging feature is approved for use up to and including RESTREINT UE/EU RESTRICTED.

“A quantum-safe solution is crucial for our customers to keep them secure from any possible attack today or in the future,” said Simo Pykälistö, President of Sectra Communications. “Given the extensive time horizon of 30-40 years for keeping highly sensitive information and national secrets secure, protection against quantum threats is highly relevant for security solutions that are developed today,”

According to Sectra, the quantum computers coming into existence today pose a threat to current encryption methods, and quantum-safe solutions are therefore perceived to be one of the key traits of future-proof confidentiality. The company’s quantum-proof products are used among government officials, officials in the diplomatic corps, decision-makers in defence and critical infrastructure, and military personnel in the field.

Beyond defence

Quantum technology is also proving useful for space applications beyond secure communications for defence and government. Late in 2020 it was reported that Teledyne e2v’s Space & Quantum team are collaborating with STFC RALSpace and University of Birmingham in the development of the Cold Atom Space Payload (CASPA) Accelerometer. The company was selected through the open competition for the 13th Earth Observation (EO) Technology Call, run by the Centre for Earth Observation Instrumentation (CEOI) on behalf of the UK Space Agency, for its submission of a proposal for a highly innovative space-based instrument.

The CASPA Accelerometer project will develop a cold atom quantum instrument in an autonomous, low power, compact form factor, in preparation for a future space mission to take sensitive measurements of atmospheric drag.

The Earth’s upper atmosphere is a highly active region that plays a key role in the planet’s energy transfer, influencing climate and weather.

Understanding the dynamics of the Earth’s upper atmosphere will rely on extremely sensitive measurement of the forces acting on a specially designed satellite as it passes through the rarefied atmosphere of very low Earth orbit (VLEO).

The new accelerometers are based on an area of quantum technology that uses alkali atoms, which are cooled by lasers close to absolute zero, without the use of cryogenics. The sensors will enable a dramatic step forward in our understanding of upper atmospheric dynamics and drive advances in climate modelling, weather forecasting and satellite orbit prediction.

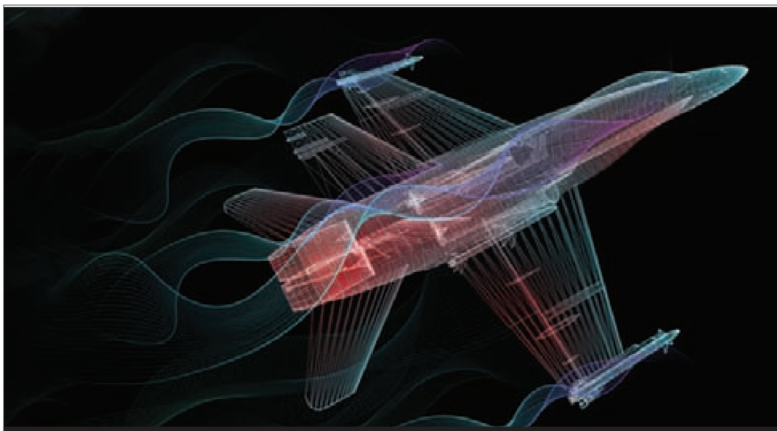
GMC

Photo courtesy of Shutterstock

Bringing test and evaluation into the digital future

With the pace of innovation arguably faster than ever, amazing new technologies that render defence communications more efficient, cost-effective, and secure than ever before are coming into play. However, thorough testing and evaluation is required before new technologies are brought to the field.

Cathy O'Carroll, Global Campaign Director - Integrated Test & Evaluation, QinetiQ



Experimentation has become more prevalent in recent years, spurred by the success of the rapid prototyping and innovation cultures championed by Silicon Valley - fail fast, learn and improve. Photo courtesy QinetiQ

The pace of innovation is an increasingly dominant factor in deterring aggression and winning battles. Getting capability from the drawing board to the front line quickly is now recognised as being fundamental to modern warfare – but this new urgency will only convert to success if the capability delivered is proven to be useable, safe, reliable, and effective.

Testing, evaluating, and certifying military equipment prior to its deployment and during its service remains critical – but has historically been an expensive, time-consuming endeavour. When an asset is procured to defend against a predictable and unchanging threat over several decades, nothing is lost if it spends a few years in development. But in today's unpredictable and constantly changing threat environment, a drawn-out test and evaluation (T&E) timescale could cost forces victory. The old way of doing things is at odds with today's rapid pace of technological change.

However, by using the latest advances in digital technology, T&E can continue to safely deliver effective capability to the front line, but at a tempo not previously possible. New ways of doing T&E, enabled by more advanced technology, can also increase a military assets utility following its deployment and throughout its service life.

Here, we examine some of the most important emerging trends in T&E as it undergoes a digital transformation that will ensure allied nations continue to outpace and outgun adversaries in the ever-shifting battlespace.

Digital experimentation

Experimentation has become more prevalent in recent years, spurred by the success of the rapid prototyping and innovation cultures championed by Silicon Valley: Fail fast, learn, and improve. The value of experimentation in defence has already been realised in several interdisciplinary multinational exercises, such as the Unmanned Warrior exercise and Formidable Shield. These accelerate the development and integration of technologies and operating concepts by allowing them to be tested in a controlled, safe environment.

The next phase of experimentation in defence will see live exercises increasingly augmented with digital elements. The creation of 'digital sandpits' will allow multiple enterprises to develop components separately while collaborating in the virtual space to test them against the whole system or subsystems. This will enable physical validation to begin later in the development process when the asset is more mature. The process will expose a higher proportion of the asset's flaws before it reaches the live environment, accelerating the entire programme and producing cost savings.

Digital twins will play an important role. These are synthetic representations of assets like aircraft, ships, or tanks that enterprises can experiment on without requiring access to the real thing. During initial development these can be used to assess different design options prior to live trials. Later in the asset's service life, its digital twin can be used to examine the effects of modifications without pulling the real platform out of service, increasing its availability.

Further to programme acceleration and cost savings, digital experimentation confers an added security advantage. Live trials can be overflown by satellites, allowing adversaries the opportunity to observe tactics and obtain knowledge of new military capabilities. Virtual trials do not. Individual aspects of a capability can be tested in live scenarios but linked together digitally to avoid revealing concepts of operations.

Deployable evaluation

Test and evaluation requirements often conflict with the need to maintain a platform's availability. Possibly the starkest example is the loss of platform availability suffered by a navy when one or more of its ships require upgrades or checks during deployment. For example, minehunter vessels require their magnetic, acoustic and hull vibration signatures to be assessed regularly, to ensure they do not trigger mines. To sail them back home across oceans to a fixed sovereign testing range may mean they are out of service for weeks at a time.

Recent advances in technology allow this problem to be solved by transporting a deployable range to the ship's location, anywhere in the world. Once calibrated in a fixed facility, all further work can be carried out in situ and the data fed back to a remote headquarters for analysis and data mining. This is made possible by developments in sensors, computing power, connectivity, and secure satellite communications. These advances will enable the concept to be extended to all warfighting domains. As new threats emerge during a unit's deployment, equipment upgrades,

Defence enterprises must work together to agree common standards and principles on the use of collaborative environments, threads and twins. Photo courtesy QinetiQ

testing and training can be delivered in the field, minimising disruption to operations.

Onboard evaluation

The next technological leap beyond deployable ranges are assets carried on board the platform to provide continual T&E as needed to inform the operational status of the military system, without human intervention.

At present, a platform or weapon undergoes a rigorous assurance programme that may include subjecting it to vibration, impacts, extreme temperatures, moisture, dust, and myriad of other conditions. Modern digital technology will allow these data points to be analysed more rapidly. This data is then used to define its tolerances and forecast its service life – but once it enters service it is dependent on human inspection to gauge its condition and may even fail before some imperceptible flaw becomes evident. To counter this, there has been a move toward integrating sensors into equipment to monitor the forces and environmental factors acting upon it throughout its service life.

Tying it all together: The digital thread

Each of these developments confers an advantage in isolation – but by linking them all together, those advantages are multiplied many times over.

One common factor among all the latest digital T&E technologies is the opportunity they offer to collect data at every stage of the process – from design, into testing, acceptance into service as well as through life. This disparate data can be combined into a through-life T&E digital thread – like a medical record for a weapon or platform – spanning experimentation, developmental testing, certification and qualification, training, and the evaluation of operational tactics and upgrades. It is progressively built and maintained through collaboration between industry, assessors, regulators, and military users. The assembled data can in turn validate the authenticity of digital twins on which multiple enterprises can experiment concurrently.

This digital thread of evidence will enable rapid, incremental assurance and fielding of defence capability, increasing the pace and validity of decision making by allowing effective re-use of data and focusing new testing on the critical elements of the capability upgrade.

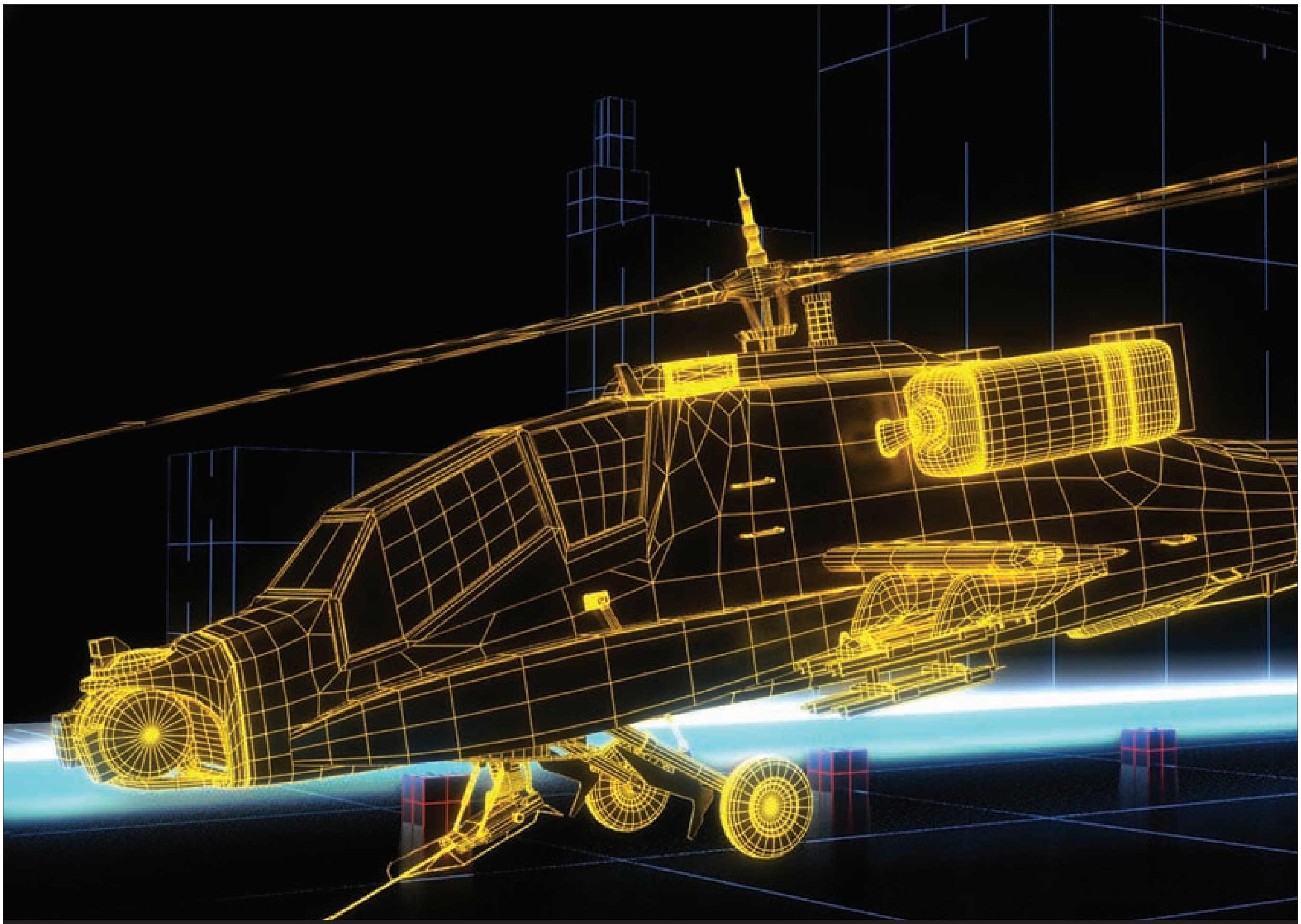
Making it real

The technology to achieve all of this exists today. The challenge in fulfilling the digital T&E ambition is no longer technological, but cultural. Defence enterprises are extremely protective of their intellectual property, and open collaboration can feel at odds with the need to maintain the necessary competitive advantage. But the risk of allowing new digital T&E capabilities to evolve separately is that multiple principles and practices are created that set enterprises on divergent paths. If that happens, the digital T&E opportunity, and benefits it brings, has been missed.

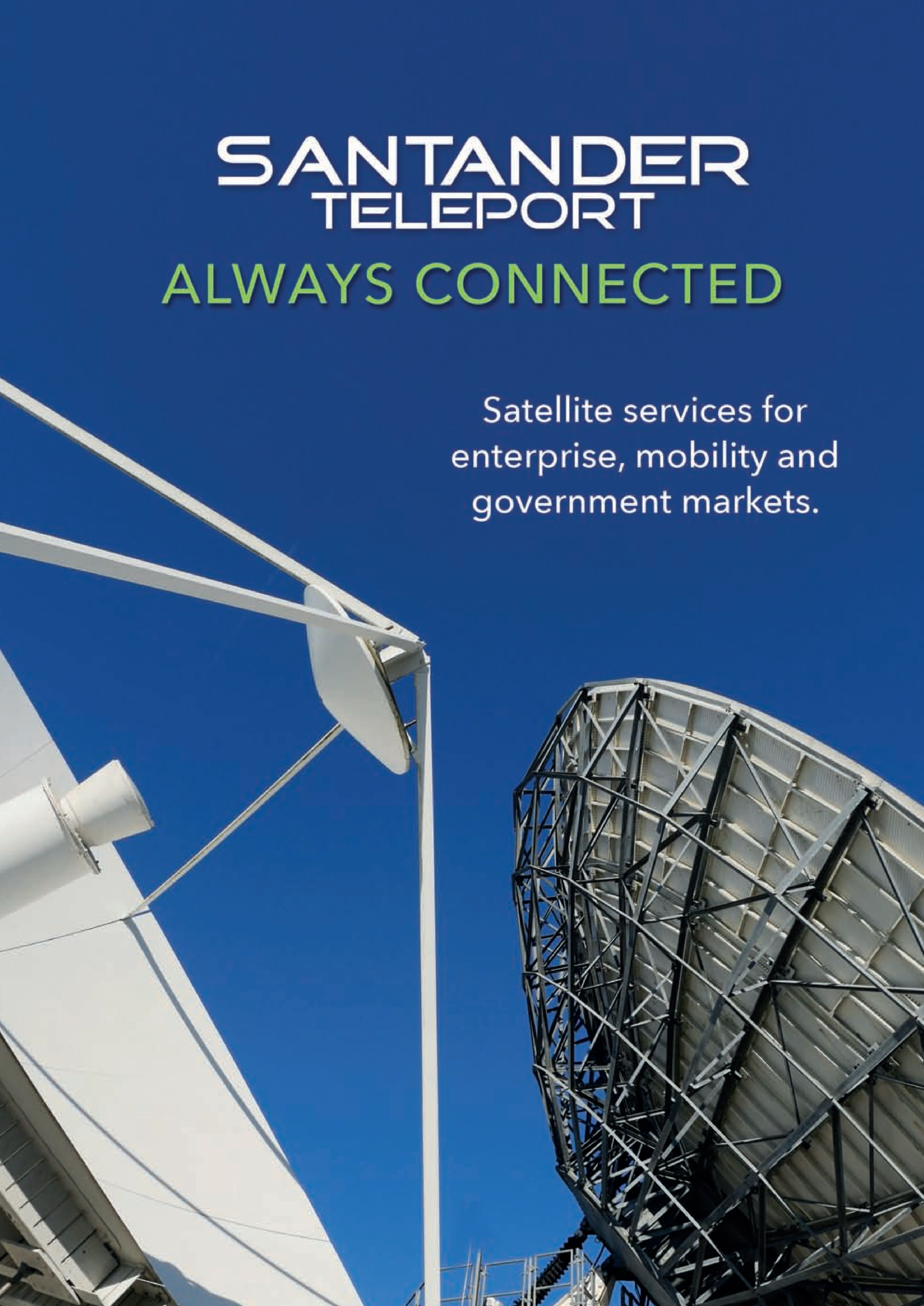
Collaborative digital T&E spaces can be configured in ways that meet these confidentiality requirements, by sharing key outputs without giving away knowhow. Data would remain the property of the various partners, overseen by an independent curator that understands and mines the data to produce a coherent picture.

Defence enterprises must work together to agree common standards and principles on the use of collaborative environments, threads, and twins. Only once this is understood, and a collaborative culture is embraced, can the massive time-saving, cost-saving, and performance-enhancing benefits of digital T&E be fully realised.

GMC



There has been a move toward integrating sensors into equipment to monitor the forces and environmental factors acting upon it throughout its service life. Photo courtesy QinetiQ



www.ndsatcom.com