VOLUME 11 NUMBER 4 JUL/AUG 2019

A SHEPHARD MEDIA PUBLICATION

DB

Flair for defence

Airborne self-protection measures

TACTICAL TIMES
Battle management systems

BETTER CONNECTED
Data links

FINAL FRONTIER
Space SATCOM

SHEPHARD

WWW.DIGITAL-BATTLESPACE.COM

Own the spectrum. Win the first battle.

Our adaptive Signals Intelligence (SIGINT) systems exploit the spectrum to provide a decisive edge in the battlespace. Founded on a software-defined open architecture, our technology hosts applications across the industry and addresses dynamic mission needs. We collaborate with our customers to provide reliable systems that keep pace with the rapidly evolving threat environment.

baesystems.com/SIGINT

BAE SYSTEMS

Photo courtesy of NASA.

DB

Editor-in-Chief and Sea Editor
Richard Thomas richard.t@shephardmedia.com
Tel: +44 (0)20 3179 2591

Air Editor
Helen Haxell helen.h@shephardmedia.com
Tel: +44 (0)20 3179 2597

Deputy Editor – Land
Beth Maundrill beth.m@shephardmedia.com

Asia-Pacific Editor
Gordon Arthur gordon.a@shephardmedia.com

Senior Staff Reporter
Tim Martin

Staff Reporters
Kate Martyr

Editorial Assistant
Lukasz Furmaniak

Contributors
Claire Apthorp, Angus Batey, Gerrard Cowan, Peter Donaldson, Tim Fish, Scott R Gourley, Krassimir Grozev, Damian Kemp, Koji Miyake, Alexander Mladenov, Tereza Pultarova, Doug Richardson, Sérgio Santana, Richard Scott, Jason Sherman, Beth Stevenson, Andrew White, Thomas Withington

Production Manager
Georgina Smith

Junior Production Editor
Sirli Manitski

Publishing Assistant
Malika Kingston

Digital Development Manager
Adam Wakeling

Graphic Designer
Georgina Kerridge

Advertising Sales
advertising@shephardmedia.com

VP Operations
David Hurst

VP Business Development
Mike Wild

VP Content
Tony Skinner

CEO
Darren Lake

Chairman
Nick Prest

Subscriptions
Annual rates start at £90
Tel: +44 (0)20 3179 2592
Email: subs@shephardmedia.com
Web: shop.shephardmedia.com

Digital Battlespace is published six times per year by The Shephard Press Ltd, Saville Mews, 30 Saville Road, London, W4 5HG, UK. Subscription rates start at £90. PCM CitySprint is acting as mailing agent. Articles and information contained in this publication are the copyright of the Shephard Press Ltd and may not be reproduced in any form without the written permission of the publishers.

Print by Buxton Press, Derbyshire, UK

ISSN 1759-345X

The Shephard Press Ltd
Saville Mews, 30 Saville Road,
London, W4 5HG, UK
Tel: +44 (0)20 3179 2570

ppa The Professional Publishers Association Member

SHEPHARD

WWW.DIGITAL-BATTLESPACE.COM

CONTENTS

Front cover: In recent years, Etienne Lacroix has designed several IR countermeasures optimised to equip specific aircraft such as the Airbus A400M strategic turboprop freighter. (Photo: Etienne Lacroix)

SHEPHARD

BUSINESS INSIGHT

FOR AEROSPACE, DEFENCE AND SECURITY

PREMIUM ONLINE **NEWS**

INDUSTRY LEADING **MAGAZINES**

CONCISE, COMPACT REFERENCE **HANDBOOKS**

VISIT SHEPHARDMEDIA.COM

Helen Haxell, Air Editor

The expendables

Cyber warfare is a very real threat that warfighters and industry leaders describe as the 'thing that keeps them up at night'. Combined with aggressive weaponry, the fourth domain of warfare poses significant challenges for combat jets in the battlespace as aggressors employ radar-guided weapons.

Silver linings

In an effort to evade such tactics employed by adversaries, militaries are demanding the evolution of effective countermeasures. For example, Leonardo was contracted by the UK MoD at the end of May 2019 to support trials of the BriteCloud 55 EAD (expendable active decoy) on the RAF's fleet of Typhoons.

Following extensive testing, the MoD approved the BriteCloud 55 for operations in Q4 2017. The first trial with the Typhoon took place in April this year, with 33 BriteCloud rounds dispensed from aircraft flown by the RAF's 41 Test and Evaluation Squadron against a range of representative threats.

The technology is a Digital Radio Frequency Memory-based active RF countermeasure missile decoy designed to protect combat jets from the latest radar-guided missiles. The BriteCloud 55 variant is named for its compatibility with 55mm flare dispensers, such as those on the Typhoon and Gripen E aircraft.

With the potential to apply the system to two major platforms in Europe, it seems natural that Leonardo would seek a quasi-footprint in North America, which holds a large share of the market.

This has been helped by the US DoD selecting the BriteCloud 218 EAD to be assessed under the Office of the Secretary of Defense's Foreign Comparative Testing (FCT) programme, for which Leonardo was selected as one of the providers at the end of last year. The BriteCloud, which is not yet available in the US, will be compared against existing DoD systems and evaluated for adoption onto US aircraft.

The 218 version was specifically developed with the US market in mind, as generally the dispensers used for decoys in this market are in a square format. The system decoys RF-seeking missiles and fire control radars, with the 218 model fitting into a 51x203x25mm form factor.

The US Air National Guard will lead the way on the FCT, as the 218 will be launched from countermeasure dispensers installed on the service's F-16s. The trials aim to show the heightened survivability that the EAD affords the aircraft. The FCT programme is likely to take two to three years.

Adding to Leonardo's BriteCloud portfolio, the 55-T model was revealed to market in Q2 2018. It is designed to protect wide-body aircraft from modern radar-guided missiles and includes a significant power increase on previous decoys to deliver the bigger radar return required to protect large transports.

Taking the bait

The evolution of the global battlespace and the wider aggressive threat posed by the proliferation of surface-to-air missiles emphasise the role that decoys can play in contentious airspace and hostile theatres.

In the next issue

- SATCOM part 2
- Naval radar
- Soldier situational awareness
- Air defence networks

In addition to their offboard jamming capability, decoys fall away from the aircraft at a rapid rate, causing the missile to be lured away from the target by its radar-homing seeker.

Such countermeasures can be applied to defeat current missile systems, as well as offering a reprogrammable capability to adapt to new and different threats, thus adding to the longevity of decoy solutions.

Also within this arena, BAE Systems has developed a new next-generation threat management technology, Smart D2, which is designed to defend military aircraft. The system can efficiently manage and deploy expendable countermeasures – including multi-shot flares, active RF decoys and kinetic interceptors – in order to protect airborne platforms from existing and emerging threats.

The Smart D2 enables two-way communication between the dispenser and aircraft using a NATO-standard interface, providing crews with critical inventory information and the ability to programme EADs in real time to improve aircraft survivability against advanced and evolving threats.

So, whilst cyber technology remains significant in the aerial battlespace, decoy technology is offering an effective method of combatting radar-guided threats. ■

Weakest link eliminated in international exercise

The wide availability of Link 16 is now removing interoperability issues between air power platforms during challenging international training exercises.

At an *Arctic Challenge Exercise 2019* (*ACE 19*) press briefing in May, a Swedish Air Force official commented that when multiple players are working together in combat training scenarios, nations need to adapt to less advanced platforms.

'Every time you bring a lot of countries together, you always have to adapt to the weakest link. The weakest link might be that one aircraft type might not have Link 16, one aircraft might only be air-to-air or air-to-ground,' the official said.

'Throughout this journey, we have found ourselves being less limited for every update on the aircraft, so nowadays we don't have to raise our hands and say: "Sorry, we cannot do that,"' they added.

ACE comprises different scenarios and covers areas such as high-density and high-threat crisis management operations under a NATO mandate to a realistic training environment – all under air power.

The large scale of this undertaking would present a natural challenge, but results will be achieved through ally interoperability.

Photo: author

Participating platforms include Sweden's Gripen – which has its own data link system along with a Link 16 or National Data Link that can enable a battlefield network – and the Lockheed Martin F-16 Fighting Falcon.

By Helen Haxell, Luleå

Photo: Lockheed Martin

Directional communications likely in future aerial battlespace

In the arena of battlespace communications, particularly for the air domain, there is a trend towards direct platform-to-platform transmission as the capabilities of near-peer and peer adversaries render current systems increasingly susceptible to intercept.

Fifth-generation stealth fighters could run the risk of exposure in connecting to legacy data link systems for battlespace communications when operating in contested environments.

Anjali Ramachandra, director of business development for international campaigns at Northrop Grumman, told *Shephard* that the OEM has expertise in low-probability-of-detection and low-probability-of-intercept waveforms – like the Intra-Flight Data Link on the F-22 and the Multifunction Advanced Data Link on the Lockheed Martin F-35 – that can deal with threats from near-peer adversaries and meet the mission needs of different aircraft operators.

Although F-22s and F-35s can communicate with each other stealthily, this is not easily achieved with the rest of the network. Even though these aircraft can already exchange data with older-generation platforms and ground assets via Link 16, this would negate the stealthy characteristics in a combat scenario.

'With the introduction of the F-35 across aircraft fleets around the world, it is creating the problem of how to communicate with fourth-generation platforms,' Ramachandra confirmed.

Although this is a common issue when introducing new platforms into any military service, the focus for integrating fifth-generation aircraft is on the network and its architectural design, so that when new technology becomes available it can be integrated seamlessly and make use of COTS equipment.

As future platforms develop, they 'will continue to have [their] own language, because we want to push the envelope in terms of exploiting the capability of each of these data links and what they might provide', Ramachandra said. 'Trying to communicate with platforms that are not in that same space, there will always be a gap, so it is important to look at other means to integrate and interoperate.'

There is now a trend of moving away from omnidirectional communications, where signals are transmitted in all directions, towards directional communications. This is so that the information is only broadcast between two specific platforms and cannot be intercepted by anyone else. An enemy would have to be in that line of sight to be able to capture that data.

'This is far more secure and stealthy, and that is why the F-35 communications platform network is set up to ensure that,' Ramachandra explained.

However, the power and processing requirements and use of apertures to focus transmission in one direction are vastly different to what is being currently used.

'We are still looking at exploring how that will work, with the expectation that we will move to a laser-type approach to get from point A to point B. Some of this is still sensitive, and we are trying to figure out what the answer is to that problem,' Ramachandra told *Shephard*, adding that this is a focus of future investment for Northrop Grumman.

By Tim Fish, Auckland

Bandwidth challenges existing data link order

Over the years, NATO's Link 16 tactical data link (TDL) has proved its worth as a vital communications conduit for air operations, but thoughts are now turning to its successor.

TDL is used throughout NATO and among allied nations to share and track tactical data between air platforms, and between aircraft, land and sea platforms or installations involved in the air battle.

When Link 16 commenced its roll-out in the 1970s/early 1980s, it was revolutionary, with the TDL transmitting across a UHF waveband of 960MHz-1.215GHz. The 'secret sauce' in Link 16's approach is its time-division, multiple access (TDMA) approach.

In sharing its data, a Link 16 network will connect in turn with each link in the system, presenting new information as necessary while also providing a hub to which returning data can be assessed and further distributed. This 'roll call' is performed several times per second, with some limitations.

There is a slight time lag between when participants can receive and exchange information. Essentially, they have to 'wait their turn' on the roll call. This can inhibit the TDL from acting in a true real-time fashion, which, given the speed of contemporary air operations and their expected increases in velocity in the future, can have shortcomings.


Image: IAI

The other restriction is bandwidth. A Link 16 network typically handles data at rates of between 2.4kb/s and 16 kb/s. As a means of comparison, an average household Wi-Fi network handles data at speeds of megabits per second. Until now, the TDL's data rates have been adequate for supporting air operations. Nonetheless, the quantity of data that will be needed to support air operations in the future will only increase.

The growing number of sensors hosted by aircraft, not to mention the so-called 'Internet of Battlefield Things' where platforms and weapons are networked as well as sensors, will trigger ever more demand for bandwidth.

One potential solution could be found in cloud computing. Israel's IAI is one company which has developed cloud-based air operations C2/situational awareness tools, as illustrated by its OPAL product (example imagery pictured). This can tie a host of air platforms together using only minor modifications to their conventional voice radios and TDLs, allowing them to share information on a cloud. Such a network can grow and shrink organically according to the number of participants, and work in a real-time manner, thanks to eschewing the TDMA approach.

Moreover, significant increases in bandwidth can comfortably accommodate the exponential growth in data associated not only with air operations, but their counterparts in the land and sea domains. Link 16 certainly has several more years of service ahead, yet advances in cloud computing do offer a potential means to augment the TDL's capabilities, possibly even replacing it one day.

By Thomas Withington, Toulouse

For more news, visit
www.digital-battlespace.com

Philippines orders UAS jammers from TRD

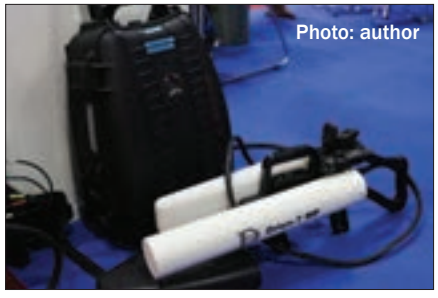


Photo: author

TRD, a Singapore-based company, has successfully won a public bid to supply nine man-portable directional counter-UAS (C-UAS) systems to the Armed Forces of the Philippines (AFP).

The deal under the Shoulder-Fired Directional Jammer Acquisition Project will see nine specialist teams field and operate the Orion jammer, according to the MaxDefense Philippines website.

A notice of award was issued on 10 May, with a contract presumably signed shortly thereafter. TRD is required to deliver its products within 120 days of receiving a notice to proceed.

Each of the Orion systems comprises two jammer modules (a rifle and manpack), four jammer module batteries, two basic repair sets and two operator manuals. The C-UAS teams will be mounted on 145cc sports motorcycles, giving them independent mobility both on and off road.

The contract is worth ₱32.45 million ($624,000) and is part of Horizon 2 of the AFP's modernisation programme, extending from 2019 to 2023. The Orion system can jam GPS, GLONASS, Galileo L1 and BeiDou navigation systems on which UAS rely.

Approval for the project was given on 1 August 2018, although the tender was issued four times before being successfully concluded.

TRD teamed with Southcoast Marketing to form a JV. The other bidder was a JV between Safer PH Innovations and NT Service UAB, although it is unclear what C-UAS model this team was offering.

The Philippines identified a need for such equipment during the brutal fighting in Marawi City in 2017, after Islamic insurgents used commercial UAS to monitor the battlefield and to identify the location of Philippine troops.

Ben Hang, business development director at TRD, told *Shephard* in April that there is a huge demand for C-UAS systems. He revealed that 'almost all ASEAN countries' are now using TRD products.

The Presidential Security Group in the Philippines has already been operating rifle-type C-UAS systems from at least early 2018 as well, these believed to be Hikvision UAV-D04JA types from China.

By Gordon Arthur, Hong Kong

Spanish Army's soldier modernisation efforts advance

The Spanish Foot-Soldier System (SISCAP) soldier modernisation effort will shortly enter its test readiness review (TRR) phase, *Shephard* has learned.

The programme passed its critical design review at the end of 2018, and the TRR is now necessary to begin factory tests. The project is the latest effort to improve soldier equipment following the collapse of the earlier COMFUT (Future Fighter) soldier modernisation programme. SISCAP is focused on developing fire control and targeting systems and communications systems for dismounted troops within the Spanish Army.

The first prototypes of SISCAP equipment – including a soldier computer, handheld control unit and a weapon control unit – will be delivered by the end of 2019, systems provider GMV confirmed.

GMV has produced a new soldier computer called LGB-11 that it describes as a smart device that integrates a soldier C2 computer with power distribution, power management and hardware acceleration for 'integration of optronics, cameras and helmet displays' in a low-SWaP configuration.

Launched at the FEINDEF exhibition in Madrid on 29 May 2019, the LGB-11 was developed using GMV's experience as the C2 lead on the COMFUT programme and its own internal R&D effort. Other selected equipment under SISCAP includes Ben-Tronics SMP batteries and Harris radios.

GMV is developing the soldier computer and electrical power system including batteries and power management, whilst Indra is responsible for providing the weapon sensors and weapon electronic and keypad unit.

This R&D phase is not addressing the procurement of the whole soldier system but is focused on developing soldier

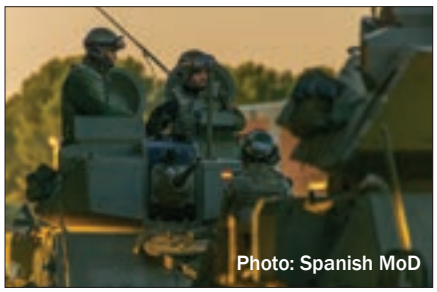


Photo: Spanish MoD

devices where a COTS solution is not available. Software for SISCAP is being developed jointly by the companies under the Spanish Army's new Dragon 8x8 Wheeled Combat Vehicle programme, based on the Piranha V.

SISCAP and Dragon will constitute the backbone of the Spanish Army's Force 2035 initiative, although the number of systems to be acquired is 'still under discussion'.

COMFUT provided some 'lessons learnt' for both GMV and Indra, which although did not field any equipment, enabled the companies to do extensive testing with different units in several environments, including desert areas in the south of Spain and high-altitude, cold environments in the Sierra Nevada.

'Without the experience gained in COMFUT, neither the Spanish MoD nor industry (GMV and Indra) could have faced SISCAP challenges with guarantees,' GMV said.

COMFUT was an ambitious early soldier modernisation programme that developed technology from 2006 to 2010, but nothing was able to reach maturity before the project was cancelled due to the economic crisis of 2008. 'The additional R&D activities that would have driven to an operational system were not launched,' GMV said. None of the components developed under COMFUT are being re-used for SISCAP as they have become obsolete in the intervening period.

GMV said that SISCAP will provide 'secure and high-bandwidth digital communications, enhanced situational awareness or integration with ISR assets' and is interoperable with NATO and EU standards, ensuring interoperability with allies in multinational operations.

By Tim Fish, Auckland

Viasat delivering LEO satellite to USAF

On 22 May, Viasat announced that it will develop a new low Earth orbit (LEO) satellite for the US Armed Forces as part of a new military programme.

Designed to provide secure global communications, the satellite is being developed for Link 16 – a tactical communications network intended for high-speed communications between military forces working in tandem. While Link 16 has so far been limited to line-of-sight communication, Viasat has stated that it is confident that the satellite will overcome this issue.

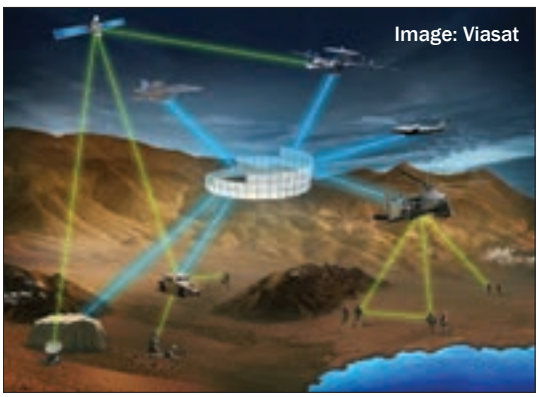


Image: Viasat

The satellite will fit Viasat's Hybrid Adaptive Network architecture, which means that services will work across both government and commercial satellite networks. This will make the beyond-line-of-sight Link 16 resilient against network congestion, cyber threats and other types of intentional and unintentional interference.

The company was contracted under the Air Force Research Laboratory Space Vehicle XVI programme. As a result, Viasat will be the first company to prototype and test space-based Link 16 capabilities compatible with the US Armed Forces, such as ground vehicles, aircraft, naval vessels and dismounted users.

'The XVI award highlights Viasat technology leadership in Link 16 and space-borne tactical communications,' said Ken Peterman, president of government systems at Viasat, adding that the company was in a 'unique position' to meet the US DoD's need for cost-effective, spaced-based Link 16 solutions.

By Claire Apthorp, London

WE'VE BEEN HERE SINCE DAY ONE,

YOU JUST DIDN'T KNOW IT.

Since 1997, WB Group has provided fire artillery control systems to militaries around the world. With a focus on innovation and development of world-class technology, we continue to empower end-users to visualize, analyze and engage threats through a collaborative operating picture.

We are proud to equip global forces with battlefield overwatch and strike capabilities from the individual ground soldier to the company level.

C4ISR **RECONNAISSANCE** **LOITERING MUNITIONS** **WEAPON SYSTEMS**

WB GROUP

OUR REALITY IS YOUR FUTURE.

WBGROUP.PL/EN

SCANNING... TARGET DETECTED

Today's ground surveillance radars (GSRs) can trace their ancestry back to the Camp Sentinel-II radar, which was developed by the US DARPA in a programme costing $2 million ($15 million at today's values). Work on this system commenced in 1967 and was completed in 18 months. It was then deployed to Southeast Asia to support US involvement in the Vietnam War. Six examples were deployed from 1968, the first of which was installed at the US Army camp at Lai Khê to the northwest of Saigon in what was then South Vietnam. The radars continued to protect US deployments until the withdrawal from Vietnam in the mid-1970s.

Roots and roles

The Camp Sentinel-II radar was an important technological step forward in the market. It transmitted on a waveband of 435MHz. A paper published in 2000 by the Lincoln Laboratory Journal entitled 'Tactical Radars for Ground Surveillance' noted that this frequency was a good compromise between the need to locate targets with reasonable accuracy and having a small enough antenna to make the radar's transportation practical.

The radar could discriminate and detect a moving person amid the natural movement of jungle foliage. In order to enable this, the system's transmissions propagated over the top of the foliage rather than through it, exploiting the diffraction technique – bending around objects. This allows the RF energy to travel through the tree canopy to the ground and then back to the radar. However, the returned signal is very weak, so the receiver must have a suitable sensitivity to detect this.

Moreover, the Camp Sentinel-II used a cylindrical array which would sequentially scan 32 sections of 12° each, encompassing a 360° azimuth. Another clever part of the radar's design was its processing, which allowed it to discriminate between foliage moving in the wind and a person moving comparatively slower beneath the canopy. An automated alarm that signalled detection removed the need for an operator to be permanently monitoring the radar.

Since then, GSRs have developed exponentially. Contemporary systems detect people, vehicles, boats and sometimes low-flying aircraft, whether targets are moving or stationary. Unsurprisingly, a major application for GSRs is base protection. One or more systems can be deployed and arranged to provide either complete coverage of the ground or just the most likely area of approach for a threat.

Beyond force protection, ground radars can support reconnaissance to provide specific information about targets in an area under surveillance. In low-intensity conflicts, GSRs can be used to guard borders and provide surveillance of possible guerrilla infiltration and exfiltration routes. Unlike optronics, radars are able to operate effectively in adverse weather and penetrate battlefield obscurants such as smoke. Furthermore, they can be used in an unattended capacity, only alerting human operators when a new target appears or when movement in the nearby locale is detected.

Like many radars, GSRs exploit the Doppler shift to determine the speed of a moving target. The change in frequency of a radar echo is witnessed when the transmission hits a moving object and is reflected, which is used to ascertain that a target has a velocity.

Designed for permanent, all-weather installations and mobile, stop-and-scan operations, R3D can detect pedestrians, crawlers and vehicles. (Photo: FLIR Systems)

The primary operational advantage provided by ground surveillance radars is enhanced situational awareness, as they offer the ability to detect and track moving targets both on land and in the air. These essential systems have been employed on the battlefield for over 50 years and are now being further advanced through the integration of evolving technologies.

By Thomas Withington

Design considerations

Mark Radford, founder and CEO of Blighter Surveillance Systems, said that a major advance in GSR technology was witnessed with the advent of electronic scanning.

Traditionally, GSRs, like other radars, had antennas that were physically moved to scan either a 360° azimuth or a specific area. This is still the case for air traffic control radars at airports, for example, which manually scan the locale with their rotating antennas. Radford noted that such systems could not necessarily perceive a target as moving unless it was large and travelling at a comparatively high speed. Electronic scanning, however, moves the radar's beam in a particular direction, allowing it to scan a particular area far more rapidly than was previously possible.

'The combination of electronic scanning with Doppler signal processing removes a traditional limitation on slow and small target detection which resulted from the physical movement of the antenna,' he remarked. 'Modern, non-rotating GSRs will typically detect a crawling person at ranges over 4km, a walking person at 10km and vehicles well beyond that.'

In tandem with detecting moving targets, 'military GSRs should be able to detect and classify personnel, vehicles and animals on varying terrain, in all weather conditions', according to SRC, a New York-based R&D company. 'They need to perform this mission while minimising nuisance alarms from windblown vegetation, waves on bodies of water and precipitation.'

Other design considerations for these systems include durability and ease of operation. 'They need to survive extremes of temperature and precipitation [when operating], as well as shock and vibration [from transportation over rough terrain],' SRC added. From the operator's perspective, 'military GSRs should be intuitive to operate, requiring minimal training'.

Finally, ease of transportation and low power consumption are equally important. 'They have to be lightweight, minimising the resources needed to transport them to their operational sites. The radars should operate with low power consumption, as remote placement requires battery power or other low power sources such as solar power,' SRC confirmed.

With regard to a GSR's transmissions, Amela Wilson, general manager of FLIR Systems' surveillance division, noted that choosing the radar's optimum frequency will depend on 'a number of factors such as size, weight and power consumption, desired detection range and clutter'. X-band (8.5GHz to 10.68GHz) and Ku-band (13.4-14GHz to 15.7-17.7GHz) frequencies tend to predominate for this type of system.

The radar section of the radio spectrum covers 3MHz to 110GHz – the lower end of this waveband can detect and track targets at comparatively long ranges (albeit with relatively large antennas and less target precision), while radars higher up the spectrum offer impressive precision using smaller antennas, but at the cost of range. Ku- and X-band frequencies therefore represent a useful way of detecting, discerning and tracking targets precisely.

As SRC noted: 'X band allows slightly better performance in heavy precipitation, [whereas] Ku band requires lower input power for equivalent detection range ▶

The SRC Hawk GSR provides continuous 360° surveillance of the ground, ports, harbours and airspace. (Photo: SRC)

The Blighter A400 Phased Electronic Scanned Array Ku-band Doppler radar sits atop a Supacat vehicle. (Photo: Blighter Surveillance Systems)

performance. Accordingly, Ku-band GSRs are typically lighter and more transportable.'

Target discrimination

Today's GSRs have a multitude of targets to detect and track. 'Some of the biggest factors we work to incorporate into our radars are a wide-area monitoring capability, the ability to detect low- and high-speed threats and sufficient warning time to assess and counter various threats. Detecting surface threats from drones is another important consideration,' Wilson observed.

The threat to military deployments from UAVs cannot be understated. Moscow's military operations in Syria in support of the regime of President Bashar al-Assad have seen drone attacks being performed against Khmeimim Air Base in the northwest of the country, where Russia maintains a sizeable military presence. An attack on 5 January 2018 from so-called 'kamikaze' drones directed against the airbase was neutralised by EW and ground-based air defence systems.

FLIR Systems is cognisant of the drone threat. Wilson said that the company's R8SS-3D and R20SS X-band GSRs are capable of detecting nano drones.

Radford agreed that there is an emerging requirement for drone detection in the GSR domain. 'The ability to monitor both the ground and the skyline simultaneously is becoming essential,' he said. Blighter's A400-series Ku-band radars can detect UAVs, alongside other conventional targets. These systems were deployed to London's Gatwick Airport in the wake of a three-day closure of the facility in late December 2018 following reports of a drone flying in the vicinity of the airfield.

Thales also recognises the importance of UAV detection, and the company expects 'future GSR radars to include technologies' for this purpose.

Despite the technical sophistication of GSRs, a compromise must be made between 'detection capabilities versus the false alarm rate', Wilson said. Having a highly capable radar that can accurately detect every moving target may have limited use if it cannot differentiate between a wildebeest moving majestically across the plain and guerrillas moving into position for an attack. SRC thus emphasised nuisance target reduction and human/animal classification as aspects of GSR design that will need to be increasingly sharpened. 'Overcoming this challenge will provide more accurate information to users, enabling better decision-making when potential threats are detected,' the company told *Shephard*.

Likewise, the ability to share radar imagery is important. Thales believes that GSRs will take an important role in collaborative combat as the front-line sensor of choice, so technologies that enable easy and robust integration will be key. Many ground radars, including those produced by FLIR Systems and SRC, employ XML (Extensible Markup Language) to share radar data with other users. Other protocols such as ASTERIX (Eurocontrol Surveillance Information Exchange) perform similar functions, digitising the radar's data so it can be transmitted across landline or wireless communications to other users.

Another area of interest for GSR developers is enabling the ability to use such radars while mobile. Wilson stressed the need to 'detect threats faster, provide automatic target classification and perform detection on the move'. This requires a specific approach. 'The challenge here is adapting the signal-processing technology to accommodate moving ground clutter,' explained Radford. 'For the past 50 years, ground clutter has always been non-moving and therefore well-defined and relatively easy to process and extract, even though the bulk of the radar clutter reflection is often orders of magnitude greater than the radar's targets of interest.'

The challenge of developing a GSR that operates effectively while moving concerns clutter discrimination, because clutter will now appear to be moving along with the ground targets that need to be detected and tracked. Radford added: 'Vehicle shock and vibration also mix into the complex Doppler signal-processing space.' He stated that processing techniques help to alleviate these issues, and Blighter is now trialling GSRs with on-the-move capabilities.

Rise of the machine

Meanwhile, algorithms and software-based functions, as well as efficient and powerful hardware resources, hold the key to

meeting current and future GSR design challenges, according to Wilson. One promising technology in this arena is AI. The ability of a radar to observe its environment, learn from it and then incorporate this knowledge in future operations could assist in sharpening the system's performance.

Such advances will be helped by similar strides in computer processing power. Just by comparing one's smartphone with the 'brick'-style mobile phones of yesteryear, one can comprehend how computing power has dramatically improved and miniaturised over the past three decades. 'Machine learning will be enabled by more powerful processors,' SRC noted. Ultimately, 'GSR technology will continue to evolve along with advances in computing power'.

Returning to our wildebeest, if a radar has been deployed several times in a section of rural terrain where such creatures are commonplace, it will initially learn to discriminate the wildebeest from other moving targets and not sound an alarm. Over time, it could learn to filter out the movement of the animals altogether. This would allow the radar to devote more of its capabilities to detecting other targets that have not been encountered before and which could represent a tangible threat.

As machine learning 'is extremely powerful, scalable and adaptable to all kinds of problems, it can provide an efficient way to rapidly implement new features and [offer] continuous performance improvements,' said Wilson.

SRC similarly argued that advances in machine learning and processing power are the best technologies to improve target classification and reduce nuisance alarms. The company is thus examining the use of AI by its radars.

Automation is the watchword regarding how GSRs will evolve. AI could help these radars to function with progressively less human oversight or intervention. Wilson believes that tomorrow's GSRs will 'detect relevant threats more effectively and be fully automated'.

Ground radars are likely to be increasingly networked with other sensors such as optronics to provide an ever deeper level of situational awareness for the foxhole and HQ alike. The advent of AI in GSRs in the form of 'intelligent and adaptive algorithms will allow for full cooperation between all sensors to optimise their use and provide high-level information of unprecedented quality and richness', Wilson continued. Improvements are not confined to software and computer power. 'RF hardware design will allow increased detection range and accuracy,' he said.

In the 52 years since the Camp Sentinel-II radar was deployed in the unforgiving jungles of Vietnam, GSRs have had to contend with an increasing array of targets that they must detect and track, with the proliferation of drones being one of the most recent examples. At the same time, radar performance has increased and false-alarm rates have declined. GSRs are now indispensable in supporting many missions, from force protection to manoeuvre. ■

Systematic's chest-mounted SitaWare Edge BMS has been optimised to support dismounted close-combat personnel. (Photo: Systematic)

With increasing emphasis on the provision of battle management systems down to the lowest tactical level, ground force commanders are studying a series of next-generation capability injections to further enhance the operational effectiveness of small unit teams.

By Andrew White

KNOWLEDGE IS POWER

Battle management systems (BMS), which must be capable of a smooth transition between mounted and dismounted roles, are continuing to be explored by industry. Some of the most innovative developments include 3D mapping, AR and haptic displays, as well as software upgrades to extend the number of nodes capable of being accommodated across a network.

However, any BMS solution seeking to integrate itself into modern or future network-centric systems must be capable of operating in anti-access/area-denied environments, which in turn can include more specific C2 disrupted or degraded environments (C2D2Es).

Within constraints

As NATO defence sources explained to *Shephard*, some of the most prevalent threats to ground forces can currently be observed in Eastern Europe, where Russian-led information operations continue to hinder a coalition of partner nations' forces through the employment of disruptive TTPs to hinder C2 and tactical communications capabilities.

These operational constraints are now commonplace across the contemporary operating environment (COE), which is making it increasingly harder for ground force elements to not only establish but also maintain sufficient levels of C2 connectivity.

Speaking to *Shephard*, Lt Col Nick Serle, commanding officer of the Infantry Trials and Development Unit in the British Army, explained that any BMS capability selected by a modern force must be capable of operating in a cluttered environment where RF, electromagnetic spectrum and bandwidth requirements are more important than ever before and where any latency in connectivity is unacceptable.

'Small steps are good so a spiral approach to the development [of BMS] is what we are after,' he said, adding that collaboration with industrial partners is essential in overcoming issues associated with closed electronic architectures, which would prevent the plug-and-play operation of subsystems.

'New technology might require new solutions, but there are also new ways to employ old technologies,' Serle continued. 'The enemy has a vote too, although they cannot dominate all domains and environments. We just maximise technology where we can and develop countermeasures.'

Attempting to tackle these operational constraints, multiple armed forces remain in the early stages of implementing next-generation BMS software to support tactical mounted and dismounted units working in C2D2Es.

Examples include the Australian Army's Land 200 (Tranche 2) effort, which places

an emphasis on the dismounted close-combat space; the UK MoD's Battle Management Application for Morpheus (currently contracted to Elbit Systems) and Dismounted Situational Awareness (DSA) effort; and Norway's 'Mime' C4I programme, which will cover BMS measures to also incorporate air defence capabilities, EW, fire and manoeuvre and fire support.

Seeking to satisfy an urgent need across the COE, the UK MoD is continuing to explore CONOPS associated with its DSA programme. In April 2019, the British Army selected to restart the DSA effort after the programme had effectively been on hold for two years due to funding restrictions. DSA is aimed at providing a BMS capability for dismounted close-combat units operating at the lowest tactical level, equipping personnel with an end-user device (EUD), data bearer/software-defined radio (SDR) and battle management software.

The MoD is seeking to equip a total of 28 battle groups over the next ten to 13 years, across all three services of the British Armed Forces.

According to Lt Col Toby Lyle, SO1 Tactical Communications and Information Systems, DSA programme manager for the British Army, the ability to see where everybody is on the battlefield at any given time remains key to combat operations across the COE. Speaking to *Shephard*, he explained: 'The ability to focus on the mission at hand and what you want your soldiers to do is a game changer and increases our tempo to make better and clearer decisions.'

The British Army is seeking a BMS capability to support operations of a dismounted close-combat company-sized group, which can network together more than 120 nodes across a flat network. This means that 'everyone can see everyone' across the network and provides ground commanders with the flexibility to 'regroup and move across the battlefield' when necessary, Lyle added.

MoD sources disclosed to *Shephard* that BMS software for DSA is yet to be downselected, but they suggested that options could include Elbit Systems' TORC2H (which has already been selected as the Battle Management Application for Morpheus) as well as Systematic's SitaWare Edge software.

Under experiment

Another battle management solution currently in service with NATO SOF that according to Lyle could be easily integrated into DSA is the Tactical Assault Kit (TAK), which has been developed by the US Air Force Research Lab, Army Research Laboratory and DARPA. Reliant upon either an Android (ATAK) or Windows (WINTAK) operating system, TAK has been designed to feed 'precision targeting, intelligence on surrounding land formations, navigation and general situational awareness information' onto a single EUD, according to official documentation.

Featuring GPS and National Geospatial Agency mapping overlays, integrated with real-time situational awareness of ongoing events, TAK software relies upon MIL-STD-2525B symbology to support iconography, cursor-on-target data formats and communication. According to Lyle, some kind of TAK variant could be used as an early adopter for DSA, providing interoperability with US Army partner forces.

The British Army has specifically highlighted the latest TAK 3.6 software, which has additional capacity to support end-users by integrating AR, live weather reports, open-source intelligence data streams, air traffic information from around the world, elevation and heat map data, Rover full-motion video controls, laser rangefinders, georeferencing information and tactical common data links.

TAK 3.6 also provides users with a manipulative 3D image of a target area, with blue/green and red force tracking where applicable as well as ranges, bearings, elevation and other mission-critical information.

Further requirements, Lyle added, include establishing how end-users will operate DSA after they have dismounted from infantry fighting vehicles, including the Warrior and the future Mechanised Infantry Vehicle. The army is also interested in the design and development of a position location information solution that can autonomously generate data for both blue and green forces as well as being able to disseminate orders, overlays and other information.

'These issues are to be worked out and costed in the next phase of experimentation,' Lyle confirmed. 'So, we hope to understand the problem better.' He said that the British Army aspires for DSA to interoperate with Morpheus's Battle Management Application. 'We require a suite of applications, because everybody won't need the same services. Morpheus is working with other aspects of industry to look at the top-to-bottom solution,' he asserted. 'We are behind on this, and this needs to happen.'

In terms of an EUD to display DSA information, the MoD is considering a variety of form factors, including smartphone designs similar to those employed by the US Special Operations Command for ATAK. 'We could use Samsung smartphones like the US. Our opinion is ▶

Systematic continues to upgrade its SitaWare software to support land-based operations in C2D2Es, with solutions including the Guard Zone feature for force protection. (Image: Systematic)

US personnel operate ATAK to support force protection missions at Eglin AFB, Florida. (Photo: US DoD)

that smartphones are familiar [to users] and [are a] cheap, recyclable technology, which makes them very useful. A variety of smartphones are being used in experimentation, but Samsung is in the lead space at the moment – but they are not necessarily what we will use in the future,' Lyle explained.

Samsung smartphones can also be networked to the company's SmartThings Hub, which would allow for the additional integration of battery packs, encryption processes, heads-up displays, power management tools, UAVs and weapon sights into a single ensemble.

Concurrently, the UK MoD has secured funding to run experimentation phases over the remainder of 2019. 'We are back on the rails to explore what DSA can do. ATAK is ready and probably what we're going to work with in initial phase,' Lyle told *Shephard*.

Divided into three phases, DSA experimentation has already considered data bearer and waveform designs to support BMS applications. This has covered operation of Trellisware Technologies' TW-950/900 TSM Shadow mobile ad hoc network (MANET) SDR and could include Harris Corporation SDRs such as the AN/PRC-152 in the future.

Block 2 experimentation, which was conducted over the course of February 2019, saw a total of 110 close-combat personnel connected over a single network during patrolling, offensive and defensive action missions during day and night, as well as in adverse weather conditions.

A third and final phase, which remains in the planning stage and is due to run over the course of Q2 2019, will consider the deployment of multiple data bearers, waveforms and BMS software by the Armour Trials and Development Unit. This final phase will also consider both dismounted and mounted close-combat configurations as well as the integration of AR helmet-mounted displays into BMS software.

'We will be looking at the technology to refine requirements, including getting in and out of vehicles,' Lyle explained. However, he conceded that target hand-off using DSA had yet to be explored. 'This might be achieved through the integration of an intelligent sight in the future,' he said.

Cognitive capacity

Already providing more than 30 armed forces around the world with BMS software is Danish company Systematic.

Andrew Graham, group senior VP at the company told *Shephard*: 'We recognise that the COE presents a number of challenges for militaries, especially for those who have been focused on asymmetric warfare for close to 20 years and now have to be equipped and prepared to counter near-peer threats also.

'These potential adversaries possess advanced technologies that can be disruptive to C2 capabilities across the battlespace. As such, C2 systems need to be resilient and capable of working with a variety of communications means that may not always be available, and we have designed our systems to operate effectively in this environment – for both situational awareness and C2,' he continued, highlighting the potential to network with cellular networks, MANET and SATCOM, for example. 'RF is key for forces deployed at the tactical edge, and we have developed our systems to be able to deliver C2 capabilities via all of these.'

However, Graham emphasised that it remains crucial to avoid overloading end-users with technology, thereby enabling them to access and view only the information which is required for them to complete their mission objectives successfully and efficiently. 'Ease of use and preventing cognitive overload are of paramount importance, and C2 systems can only be effective if they do not detract from the warfighting capabilities of the user. When investigating technologies that promise a step-change on the modern battlefield – such as augmented reality – we have to consider the human factors element as much as the delivery and presentation of information,' he said.

'Our core technology is more than capable of presenting the situational awareness information required by the dismount, for example, however this is only useful if it is done in a manner that does not introduce cognitive burden. We are constantly evaluating emerging technologies – such as cyber capabilities and artificial intelligence,' Graham added.

He pointed to open and modular architectures, as well as increasing levels of interoperability, as critical elements for any BMS software operating in C2D2Es and the wider COE, in order to ensure seamless integration with partner nation forces.

'Providing an open, modular architecture is a central tenet of our system design as we believe that C2 capabilities should be customer-driven and not stovepiped. Our software development kit is available to customers and third parties, enabling apps to be developed for the SitaWare suite, and we are seeing users do this. Likewise, we have developed bespoke apps for users. It's all about meeting the customer's needs and not dictating what they can and can't do.

'Similarly, interoperability is also of paramount importance. Few militaries conduct missions independently, therefore we understand that it is crucial for information from our systems to be made available to others, even those that do not operate with SitaWare. While it might not be as extensive or delivered as seamlessly as between SitaWare users, mission-critical information from our systems can be shared across the battlespace,' he stated.

Systematic's SitaWare Tactical Communications technology comprises a suite of solutions that can automatically optimise the use of bandwidths across C2D2Es. 'For example, it recognises when it is not possible to transmit the requisite information and will wait for windows of opportunity to do so. In the tactical environment, this can frequently be the case, such as when dismounts take cover behind obstacles that restrict communications or enter buildings,' Graham said.

'That is why we have designed our Frontline and Edge systems – for the mounted and dismounted commanders respectively – to have intuitive interfaces and the ability to create information overlays that can be quickly added and removed.'

On 24 April, the Finnish Defence Forces (FDF) announced plans to upgrade its full suite of Systematic SitaWare Edge, Frontline and Headquarters software products. According to a company statement, SitaWare software has been in service with the FDF for five years, although the military is now planning to provide ground forces with a series of capability enhancements in line with emerging operational requirements.

Merja Annala, president of Systematic Finland, said: 'The FDF employs SitaWare for a variety of roles and often in innovative ways. Learning from their experience has certainly been beneficial in the development of the product. As operators of all elements of the SitaWare suite, the FDF are able to benefit from the advanced C2 and situational awareness capabilities that the software brings. Dismounted personnel, mounted units and command post elements can share the same operational picture, whether that be on an Android device for the SitaWare Edge solution, a vehicle-borne laptop or on more established infrastructure in a command post.'

SitaWare software is disseminated across the battlespace using SATCOM as well as MANETs, facilitated through Bittium's inventory of next-generation SDRs, providing end-users with a common operating picture accessible to all command levels. This includes HQ elements in Finland through to forward-deployed task forces in expeditionary theatres.

Upgrades to the FDF's SitaWare software will include a mapping mode with 3D functionality that will be integrated into SitaWare Headquarters to allow users to switch from the standard plan view into a 3D format whilst maintaining the same information and planning overlays. ▶

The US Special Operations Command Tactical Assault Kit, illustrated in a chest-mounted configuration on the second soldier, continues to be considered for the British Army's DSA programme. (Photo: US DoD)

The British Army has tested BMS software with Trellisware's TSM Shadow SDR to support up to 110 connected nodes across a MANET. (Photo: Trellisware Technologies)

Additional enhancements include a declutter tool, enhanced search functionality via tagging feature and enhanced record and replay capability for after-action reviews and hot debriefs.

Sitaware Frontline upgrades include a Guard Zone function to assist force protection with the designation of out-of-bounds areas, a declutter tool, cursor-on-target capability and the ability to simultaneously display two video feeds that are generated from external sensors and subsystems.

Tactical logic

Elsewhere, industry partners continue to stretch the boundaries of the capabilities of BMS software to support dismounted and mounted personnel operating at the tactical edge of the battlefield.

Seeking to integrate its own AI-based weaponry readiness enhancement solution on board TAK is Israel-based Secubit. Speaking to *Shephard*, company CEO Itay Weiss said that the WeaponLogic Ecosystem technology is scheduled to be integrated on board ATAK software by the end of 2019 in response to emerging operational requirements from both the US armed forces as well as the wider international community.

According to Weiss, ground forces in particular are expecting 'more' in terms of information gathering in the future operating environment. 'Everyone is focused on situational awareness – connected weapons across a battlefield can influence decision-makers and provide more insight to command posts and small unit teams,' he said.

The WeaponLogic Ecosystem comprises a smart counter device, which can be integrated into the pistol grip of a small arm, a data retrieval tool and a dashboard to exploit information. The 20g Smart Counter relies upon AI algorithms, networked through SDR technology, to report information between small unit teams as well as back to a tactical operations centre, regarding the operational state of a weapon system. Providing more than 1MB in memory, the technology is based on passive and secure RF identification technology.

The WeaponLogic data reader, which weighs 249g, measures 155x75.5x18.6mm and comprises a 5in high-definition screen powered by a rechargeable 4,300mAh lithium-ion battery. The device features USB 3.0 connectivity with a PC.

As Weiss explained, the integration of a smart counter device can be used to add layers of intelligence on board a BMS solution. This can be augmented further with the integration of weapon-mounted sensors capable of measuring the position of fire selection switches, barrel temperature and muzzle velocity, as well as direction of fire, allowing a tactical operations centre to be alerted when troops are in contact, for example.

Additional utility for such a solution includes automatic alerts for medical support elements to perform casualty evacuation serials as well as the automatic launch of ammunition resupply missions by autonomous vehicles when small unit team ammunition states run critically low.

Secubit's suite of modular and scalable sensors (which are enabled by Wi-Fi or Bluetooth connectivity) could also alert small unit teams to dangers of fratricide as well as triggering of ISTAR assets when safety catches on small arms are disengaged ahead of a potential contact.

'This is critical information when connected to BMS software,' Weiss confirmed. He added that the solution had already been successfully integrated into a variety of small arms, including 5.56mm M4, M16 and SAR21 assault rifles as well as Glock handguns.

Armed forces in Sweden, New Zealand and the US already operate WeaponLogic Ecosystem technology to support logistical requirements in small arms. However, industry sources informed *Shephard* that undisclosed special operations customers around the world are already considering integrating sensors into wider BMS applications to enhance information gathering and situational awareness.

Smart tech

Finally, Thales is seeking to futureproof its BMS capabilities with the launch of its Smart and Seamless Command and Control (SC2C) software, which was launched on 2 April at SOFINS (Special Operations Forces Innovation Network Seminar).

Developed in tandem with French SOF, a S2C2 minimum viable product has already been designed for evaluation, which would allow small unit teams to optimise levels of information exchange and situational awareness at the tactical edge. Specific BMS capabilities include georeferenced iconography with mapping overlays, chatrooms for real-time voice and text exchanges and a virtual assistance to help forward-deployed personnel troubleshoot.

Thales officials were unable to provide *Shephard* with any further information, but it is understood that a technology demonstrator is due to be unveiled later in the year as the company continues to develop the product in a 'collaborative and agile' manner.

There remains little doubt as to the mission-critical nature of ground-based BMS in the future operating environment. However, as technologies and capabilities evolve through the introduction of AI and AR, commanders must remain alert to avoiding any additional cognitive burden on small unit teams already operating in complex environments. ■

PLUS

The most cost-effective solution for aerospace, defence and security market intelligence.

IDENTIFY	OPTIMISE	ANALYSE
NEW OPPORTUNITIES	YOUR MARKET POSITION	YOUR COMPETITORS

Request a free trial

Email plus@shephardmedia.com

Call +44(0)20 3179 2598

USA Toll free 855-3416-602

Visit www.shephardplus.com

SHEPHARD

IN THE RIGHT DIRECTION

A JTAC checks his radio before the start of the operational assessment of a handheld Link 16 radio. (Photo: US DoD)

Data links are the backbone of any modern defence force, supporting communication between individual soldiers and units at the bottom end, up to an entire deployed force or during allied joint operations at the highest level of complexity. The ability of military elements to cooperate is only as effective as the data links that can facilitate the required transfer of information.

By Tim Fish

Since the 1980s, the ability of units to communicate with each other has centred around the US-developed Link 16 data link. The line-of-sight system transmits data at a rate of 26-107.5kB/s over the UHF range (960-1,215Hz). It uses a J-message format and TDMA (time division multiple access) to send data packages in time slots that can be accessed by air, ground and maritime forces.

Multifunctional Information Distribution System radio terminals that host Link 16 are fitted on fighter aircraft such as the Dassault Rafale, Eurofighter Typhoon, General Dynamics F-16, McDonnell Douglas F-15 and F/A-18 and Saab Gripen, as well as support aircraft such as the Lockheed C-130 and Northrop Grumman B-2 and E-2D.

First choice

Link 16 can provide an integrated air picture that contains the location details of friendly and hostile aircraft, situational awareness information and additional data on air and ground targets, particularly air defence threats. This combat information can be distributed in near-real time to any platform that is in line of sight.

The benefit of Link 16 is that it is secure and robust enough to operate in a jamming environment and allows users to join on an ad hoc basis. However, because it is being broadcast in all directions, information transmitted across the data link is very detectable, its capacity for higher data rates is limited and it operates on a line-of-sight principle only.

SWaP requirements have previously prevented tactical data links from being installed on ground vehicles, smaller aircraft like helicopters and UAVs and smaller maritime vessels. However, Andy Kessler, business director of tactical data links at US-based Viasat, told *Shephard* that since

the mid-2000s technology has now advanced to allow the development of smaller radio terminals that can be installed on such platforms, giving users access to the direct RF network and the same level of situational awareness as C2 aircraft.

To show how far the terminals have come, Viasat launched its new AN/PRC-161 BATS-D (Battlefield Awareness Targeting System-Dismounted) radio in 2018, which is used by JTACs to coordinate close air support with supporting fighters. It is described by the company as 'the world's first handheld Link 16 radio'. 'These things used to be the size of 1,000 cubic inches,' Kessler said.

The Link 16 waveform has proven useful over the past three decades and is still expanding, but new challenges are emerging as military forces develop platforms and capabilities that require a more enhanced form of communications and networking. There are additional requirements for more stealth and increased throughput, capacity and security.

There is a finite amount of network capacity in Link 16, and with miniaturisation allowing an increasing number of platforms to use the data link, there is less network capacity available for each user. 'That is why we invested in the ability to do concurrent multiple receptions [CMR] coupled with Link 16 Enhanced Throughput,' said Kessler, adding that this increases the capacity of the network without changing its fundamental structure.

CMR means that the radio can listen to, and process information from, two or three frequencies at the same time, therefore increasing the capacity of the network. Enhanced Throughput is where the network is enabled to squeeze more capacity into each time slot given for each participant. These two techniques are facilitated by the growing capabilities of digital processors.

These modifications, among others, mean that Link 16 is here to stay, and its proliferation among numerous US allies makes it the data link of choice for any military wanting increased situational awareness and interoperability. However, new requirements are developing, for which Link 16 just does not meet the task.

Facing challenges

'Asymmetrical adversaries are acquiring force multiplier technologies and are modernising at an alarming rate. We need to work to optimise, prioritise and diversify military data link systems,' said Jim Schryver, director of ISR Systems at Lockheed Martin. 'There are requirements to counter both jamming and passive detection/geolocation capabilities while sustaining adequate and reliable communications throughput. Existing waveforms need to be adapted to better perform in highly contested environments.'

Evan Deneris, data links subject matter expert at L3, reiterated that the nature of the battlefield is changing. 'What has changed now is that the adversary is looking for our communications and trying to find us and so the need to use more stealthy communications and to hide is more important,' he explained. 'Link 16 is very poor at that, so it is not a good choice. In peace time it is fine, and I don't see it going anywhere... The challenges are now in overcoming the structure of Link 16, which is everywhere and has a loyal following.'

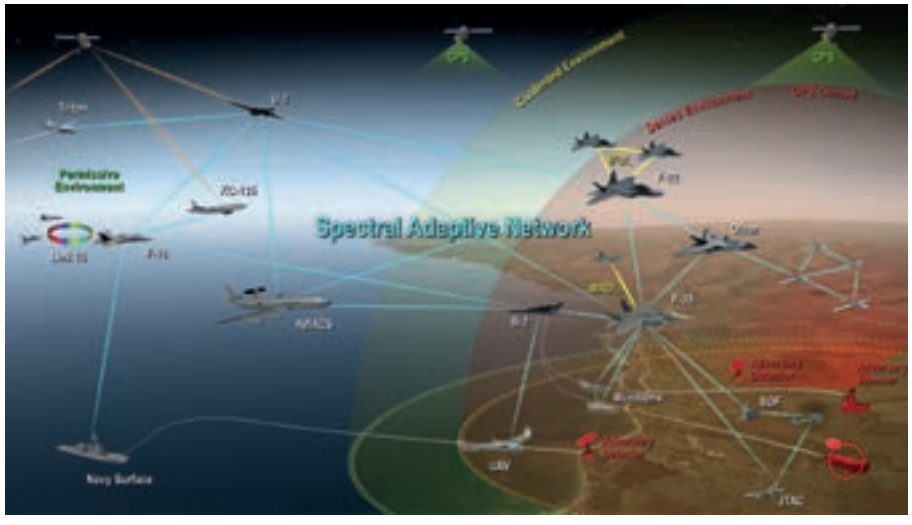
Western militaries and alliances like NATO cannot expect to control the electromagnetic domain when facing new threats from near-peer rivals. They must look to leverage technology to enhance every part of the development, transmission and maintenance of the network, from antennas, modems and power supplies to processors, network management and security.

Deneris highlighted ISR in the tactical environment as an opportunity, particularly UAV swarms and UAS that have requirements to provide video reconnaissance imagery in near-real time, guided munitions and direct downlinks of video from the ISR pods on aircraft into handheld devices on the ground. Data links for these have to work in a denied environment and provide assured communications. 'The trick is to hide in plain sight,' Deneris said. 'There are ways to obfuscate the communications signal so that people cannot pick them up – whether that is [varying] power levels, moving frequencies or changing signatures, there are lots of techniques you can employ and you can combine some of them to hide.'

L3 has invested in its Chameleon waveform product, which can provide direct communication between the Lockheed Martin F-22 and F-35 without a gateway, offering data link operators a stealthy communication method when needed. The self-programmable system can be upgraded with new software as it is developed.

'If the adversary does not even know you are there, then they won't necessarily turn on jamming or other things to use against you. The first layer [of protection] is not to have your communications be detected. Then after that, if they start employing tactics, there are other things you can do with communications to work around or avoid any of the active threats to your communications,' Deneris told *Shephard*. 'More recently, the tricks for better hiding ▶

L3 Technologies is developing interoperable communications architectures, providing resilient C2 and continuous networking connectivity regardless of environmental conditions and adversary activity. (Image: L3)



The F-35 fighter is a multifunctional stealthy platform that has capabilities that are a direct result of it being a network-enabled asset. (Photo: Lockheed Martin)

is highly controlled power. You want just enough power to reach the intended receiver with the data and not go any further, in case someone else doesn't have the opportunity to pick you up.

'The other is modelling the bandwidth and the data rate depending on the mission or the threat. There have been advancements in coding and antenna efficiencies and power efficiencies taking advantage of those, but the real clincher is the ability to control all of those things on any particular mission,' he continued.

Integration situation

Using these types of techniques requires additional power and signal processing, which have been the focus for recent advances. For example, the modern field-programmable gate array allows a much larger amount of horsepower into radio waveform signal processing whilst still being able to link back and retain compatibility with existing hardware.

However, integration is a challenge. The existing hardware on most platforms is suited to Link 16, and militaries cannot afford to replace every antenna on an F/A-18 or F-22 or other platform with its communications architecture. 'What we have to do in some cases is replace an existing radio slice with one of ours and work within the frequency and interface constraints within the platform, but still there are things you can do with the waveform to operate in the modes we are talking about,' Deneris confirmed. When some equipment is replaced, opportunities to enhance the communications capability must be taken.

Advances in antenna developments with planer or conformal arrays and electronically assured arrays mean that bigger bandwidths are available when conventional antennas are replaced. However, higher transmitted power with more efficient power amps and larger antenna aperture size are required to cover the wave.

'That is a double-edged sword too. It allows us to do better with the techniques I am talking about – more bandwidth is better – but the other problem is that antennas are electronic vacuum cleaners and bring in all kinds of noise and interference, and you need mitigation techniques to work with them, because now you have a huge amount of processing at the front end of the antenna with additional full beams or even beam nulling to get away from the threats, but the communications signal processing and waveforms have to work hand in hand with that,' Deneris said.

There is only so much space on an aircraft for radios, and there are systems that are mandatory such as for refuelling, air control or IFF. Therefore, due to SWaP limitations, it becomes impossible to continually install more radio hardware and antennas. One solution is to make the processing multifunctional and radio-

The AN/PRC-161 BATS-D radio is used by JTACs to coordinate air support. (Photo: Viasat)

agnostic, which means it can process any kind of signal that comes in – whether that is EW, communications or ISR.

'With the same processing, you could put up five or six UAVs – one might be doing jamming, another might be doing a BLOS communications link, one might be doing spectrum-sensing signals analysis and then queueing the other UAVs. We are seeing finally this convergence of tactical EW, SIGINT and strategic communications all being done in one box, with the other enabler being the state-of-the-art multifunction antenna arrays that are digitising the RF at very high speed and are

literally pushing the digital boundary right up through the antenna,' Deneris explained. 'The arrays can do multi-mission [operation] too – one part of the antenna is actively listening for signals whilst the other part is running the communications link to the same aperture. That is how we are going to stay ahead of the SWaP limitations on the platforms and also prevent overwhelming the operators and pilots.'

Equipping future platforms

The new fifth-generation F-35 fighter is at the forefront of the market, as it is a multifunctional stealthy platform that has capabilities that are a direct result of it being a network-enabled asset.

Anjali Ramachandra, director of business development for international campaigns at Northrop Grumman, told *Shephard* that the OEM has expertise in low-probability-of-detection and low-probability-of-intercept waveforms – like the Intra-Flight Data Link on the F-22 and the Multifunction Advanced Data Link on the F-35 – that can deal with threats from near-peer adversaries and meet the mission needs of different aircraft operators.

Although F-22s and F-35s can communicate with each other stealthily, this is not easily achieved with the rest of the network. Even though these aircraft can already exchange data with the older-generation aircraft and ground assets via Link 16, this will not be an option in a combat scenario as it would negate the stealthy characteristics.

'With the introduction of the F-35 across aircraft fleets around the world, it is creating the problem of how to communicate with fourth-generation platforms,' Ramachandra said. Although this is a common issue when introducing new platforms into any military service, the focus for integrating fifth-generation aircraft is to focus on the network and its architectural design, so that when new technology becomes available it can be integrated seamlessly and make use of COTS equipment.

As future platforms develop, they 'will continue to have [their] own language, because we want to push the envelope in terms of exploiting the capability of each of these data links and what they might provide', Ramachandra said. 'Trying to communicate with platforms that are not in that same space, there will always be a gap, so it is important to look at other means to integrate and interoperate,' she added.

There is now a trend of moving away from omnidirectional communications, where signals are transmitted in all directions, towards directional communications. This is so that the information is only broadcast between two specific platforms and cannot be intercepted by anyone else. An enemy would have to be in that line of sight to be able to capture that data. 'This is far more secure and stealthy, and that is why the F-35 communications platform network is set up to ensure that,' Ramachandra confirmed.

However, the power and processing requirements and use of apertures to focus transmission in one direction are vastly ▶

While the F-22 and F-35 can communicate together, it is communication with older-generation aircraft that will be more complex. (Photo: US DoD)

different to what is being currently used. 'We are still looking at exploring how that will work, with the expectation that we will move to a laser-type approach to get from point A to point B. Some of this is still sensitive, and we are trying to figure out what the answer is to that problem,' Ramachandra said, adding that this is a focus of future investment for Northrop Grumman.

Unmanned connection

Another major trend in the tactical environment is the rapid increase in the number of smaller UAVs that are entering service. With these platforms therefore having to operate in more urban areas, this presents a challenge for data links.

Ariel Kandel, CEO of Israeli manufacturer Commtact, told *Shephard* that 'the RF environment is becoming very dense, with a lot of sensors being used at the same time in the same space. Frequency has become very expensive real estate, so you need to lose the last bit and byte; squeeze the most out of it.'

He said UAV operators want to transmit the real live imagery from their sensors all the time and in high-definition video. It used to be analogue, but now it is digital and consumes a large portion of bandwidth. In the past, it was enough to use 2MB/s, but now it is 10MB/s line of sight and 100MB/s for a mesh network. 'In defence you are talking 150m/s mores in the latency that you are sampling the HD video to the time you see it on the see regardless of the range or the number of sensors on the ground. This is something that is very hard to get,' he said.

Kandel believes that the commercial sector – in which R&D investment is many times what can be spent by defence – can offer the solution. 'New data link systems are going to have technologies that support multiple waveforms... The operator can decide depending on the mission and CONOPS which modulation to use; all this is combined in the same form factor.'

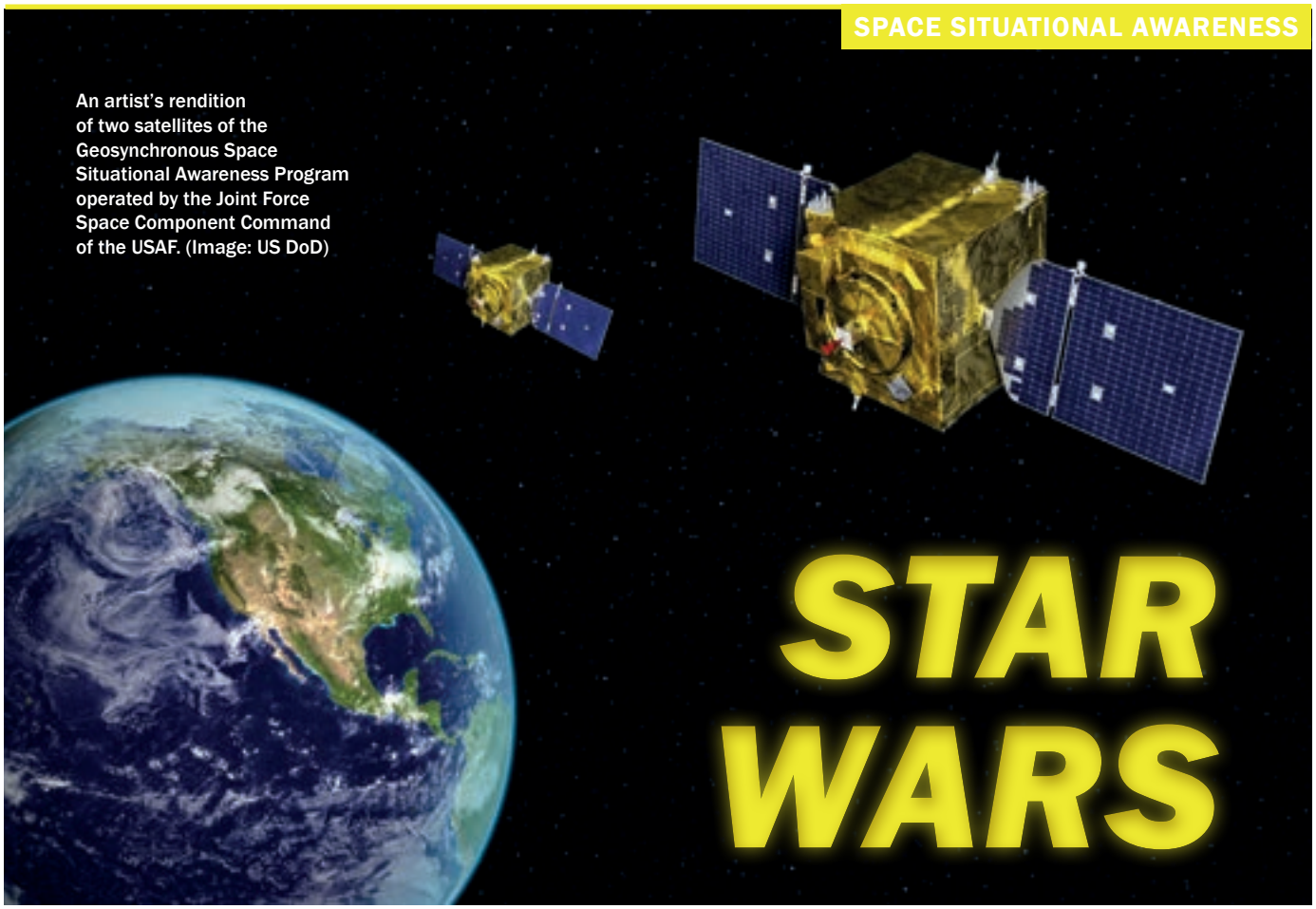
A new system to be launched by Commtact this year will employ civilian technology that is hardened to bring the latest developments to the defence market. It promises to support two channels of HD video encoding in real time, thereby reducing latency to 150m/s, and will offer a range of up to 200km in the same onboard SWaP of the existing system in the UAV. This can be achieved by putting additional hardware on the ground station rather than the platform itself, such as a larger antenna.

'It can work point to point or have multiple receiving options, using advanced collection codes to work in the dense areas, with built-in AN 256 encryption. In addition, we have immunity frequency hopping and spread spectrum to help to be immune in those dense areas to RF attacks or interception by the air and have a cyber mechanism built into the fieldware of the data link system,' Kandel explained.

'[We will keep the system] as light and efficient as we can, with all the extra changes done on the ground because it is more adaptable to the client, easier for them and flexible to switch between. A 400g kit can give UAV support up to 15km, but with a directional antenna and tracking system that can be GPS-independent, this can be extended to 50-100km with a 5kg pack,' he added.

Preparing platforms to meet the tests of the new threat environment is presenting a serious challenge. New waveforms have to be developed that can transmit larger flows of data than ever before and satisfy requirements for stealth and assured connectivity. This also needs the right architecture and software to support it.

Whilst technology advances are resulting in new systems being brought to the market, integrating them onto platforms and ensuring backwards compatibility with existing networks and systems – while still meeting SWaP limitations – remains very much a work in progress. ■



An artist's rendition of two satellites of the Geosynchronous Space Situational Awareness Program operated by the Joint Force Space Component Command of the USAF. (Image: US DoD)

STAR WARS

Although the UN has worked tirelessly since the launch of the USSR's first satellite Sputnik in 1957 to ensure that human use of outer space would be solely for peaceful purposes, a growing number of countries are working to demonstrate capabilities in space that not everyone considers peaceful, and the level of commercial involvement appears to be increasing.

By Tereza Pultarova

On 23 May 2019, the US Senate Armed Services Committee approved plans by President Trump's administration to establish the US Space Force, the sixth branch of the nation's military forces. The initiative, which aims for military space operations to become independent from USAF, is testimony to the growing importance of space in the military arena.

The race for space domination is no longer only between the former Cold War rivals – Russia, the heir of former USSR space assets, and the US. Other nations – mainly China – are now making major strides to prove that they too can control what is going on in the orbit around the Earth.

While the traditional use of space assets for combat support, such as for communication and espionage, has historically been accepted as peaceful, the establishment of the Space Force is seen by many analysts as a move towards the possible militarisation of space.

Wake-up call

SATCOM is becoming more significant in the era of connected warfare, and the protection of space-borne capabilities is thus gaining importance. The problem is that the risks to orbital assets have increased substantially over the past decade.

In March 2019, India flexed its muscles by performing a successful anti-satellite (ASAT) test, shooting down one of its own operational satellites located in a low Earth orbit with an interceptor derived from a ballistic missile. The event, hailed by India's Prime Minister Narendra Modi as a moment of 'utmost pride', was seen by many analysts as a wake-up call to the international space community to start taking seriously the issue of long-term sustainability of space operations.

'With the US talking about the Space Force and India launching its ASAT mission, we are now absolutely talking about the militarisation of space,' said Shagun Sachdeva, senior analyst at satellite and space market consultancy Northern Sky Research. 'The problem is that right now there are not enough regulations to be able to have a peaceful way of having a space force, if there needs to be one. Right now, there is a pretty big risk of these things going wrong and causing a big disaster in space.'

Mission Shakti, the name of the ASAT demonstration, not only proved that India (like China, Russia and the US) can now shoot down adversary satellites, it also generated a huge amount of space debris, which is hurtling through space ▶

on out-of-control trajectories, jeopardising spacecraft in the heavily used and already dangerously cluttered low Earth orbit.

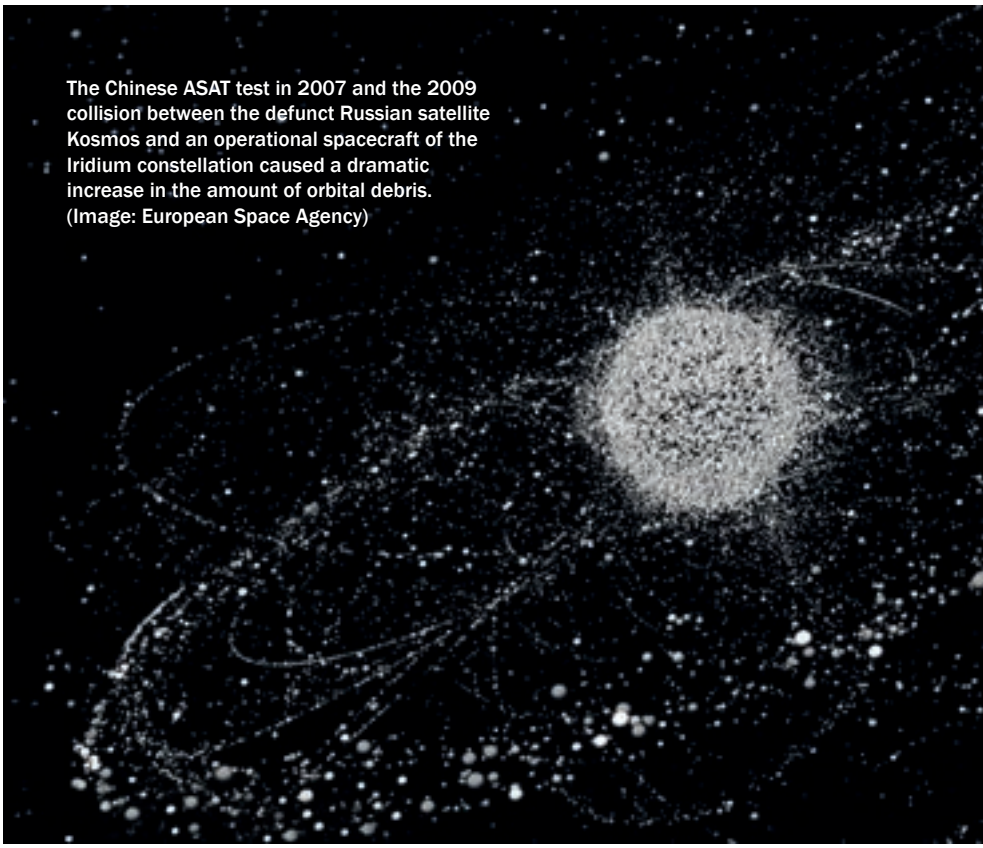
The Indian ASAT generated at least 270 pieces of space debris, according to the US Joint Force Space Component Command, which monitors and tracks objects orbiting the Earth, including debris fragments larger than 10cm. Although India claimed that the target of the test was so low that the generated debris would burn in the atmosphere within a few days, many analysts questioned this assessment, saying that many pieces were actually boosted into higher orbits by the missile and will take years to clear up.

'The debris is freely floating now and can cause collisions with other countries' satellites,' Sachdeva told *Shephard*. 'The Indian ASAT test was a pretty catastrophic event and could have even more catastrophic consequences. One of the problems it created is that other countries might want to follow suit to have a strategic advantage, and that creates a big problem.'

A similar test conducted by China in 2007 targeted a larger satellite in a much higher orbit. That event immediately generated more than 2,000 pieces of trackable space debris, making it the largest debris-creating event in history, followed closely by the 2009 collision between the defunct Russian satellite Kosmos-2251 and the operational Iridium 33, one of the communications satellites of the Iridium constellation.

The number of detected fragments generated by the Chinese ASAT demonstration has since increased to nearly 3,500 as a result of further collisions. Only 570 of those are known to have since decayed. In addition to that, the event produced an estimated 150,000 smaller particles that cannot be tracked with existing technology.

The 2007 and 2009 events brought the problem of space debris and the sustainability of orbital operations to the fore for leading global space agencies. Concerns have been raised that the negative trend could easily tip over into the so-called Kessler syndrome – a scenario predicted in the late 1970s by NASA astronomer Donald Kessler that foresees that at some point the density of orbital fragments will result in an out-of-control cascade of collisions.



The Chinese ASAT test in 2007 and the 2009 collision between the defunct Russian satellite Kosmos and an operational spacecraft of the Iridium constellation caused a dramatic increase in the amount of orbital debris. (Image: European Space Agency)

'Prior to the 2007 Chinese ASAT and the 2009 Iridium-Kosmos collision, space situational awareness [SSA] was a fairly static and not very dynamic area,' said Travis Langster, VP of DoD and intel space business development at AGI, a Philadelphia-based software company that is developing solutions for aerospace and defence organisations. In 2014, AGI launched its Commercial Space Operations Center, the world's first commercial SSA centre, which currently tracks over 9,000 public objects in space.

'After these two events, momentum really started to shift to space becoming a contested and congested environment. There were suddenly many more objects to track. The problem is that the traditional systems were built to detect incoming missiles and provide warnings for these types of things,' Langster added.

Warning signs

In addition to emerging countries flexing their space muscles in the form of debris-creating ASAT tests, the problem is further exacerbated by fast-paced developments in the commercial space sector.

Since 1957, nearly 8,500 satellites have been launched. Nearly 5,000 of those are still in orbit, but only about 2,000 are currently operational. However, in the past decade, commercial companies started launching large quantities of small satellites for various purposes, including Earth observation and telecommunications. The largest of these schemes, such as the constellations of SpaceX and OneWeb, involve possibly thousands of satellites.

'Over the next few years, it's been proposed that more than 14,000 satellites could be launched,' confirmed Langster. 'Even if only 25% of these plans are successful, it's still more than double or triple the number of active satellites today.'

The task of monitoring what is happening in space is therefore becoming bigger and more complex. Furthermore, there are concerns that some nations may be using satellites to spy on other countries' satellites or even disrupt their operations. In 2015, a Russian satellite known as Luch caused a lot of concern with its suspicious manoeuvres in geostationary orbit.

A satellite in geostationary orbit, located at an altitude of 36,000km, travels around

the Earth at a speed that matches the rotation of the planet. As a result, a geostationary satellite (unless deliberately moved) appears to stay fixed above a certain spot on the Earth, offering a stable view of a section of the world. This is a unique position that is frequently sought after by communication satellite operators. The Luch satellite, however, kept changing its location every few months, manoeuvring dangerously close to some strategic international assets.

Traditionally, the US Joint Force Space Component Command, through its 18th Space Control Squadron, has been responsible for tracking objects orbiting the Earth, including operational satellites, defunct spacecraft and fragments generated in collisions. The command also provides warnings to commercial operators whose spacecraft is at risk of being hit by another object.

Earlier in 2019, it was revealed that after ten years of planning, the USAF cancelled its Joint Space Operations Center Mission System (JMS) programme, which was intended to modernise the tracking and cataloguing of space objects. 'At the time of its inception, JMS represented the best approach to space operations,' said Capt David Liapis, spokesperson of the USAF Space Command. 'Today, JMS is simply not agile enough to meet the challenges of the rapidly expanding and evolving threats of the space domain.'

> ***"Since 1957, nearly 8,500 satellites have been launched. Nearly 5,000 of those are still in orbit, but only about 2,000 are currently operational."***

He added that the command is now pivoting to an open-architecture approach that would utilise existing funds to host cutting-edge DoD-certified SSA and C2 applications developed by commercial industry, as well as the US government, on government-provided infrastructure. The new system will, according to Liapis, incorporate the best parts of JMS, but at the same time open the door for faster innovation.

'Because a more agile acquisition approach is needed for software, we are employing a developmental operations approach for rapid fielding of capabilities,' he told *Shephard*. 'These capabilities are customer-derived, executive level-endorsed and executed via a series of production sprints designed to put certified tools on the floor in a matter of only weeks. We must shift to an SSA paradigm based on advanced threats to US dominance in space, increasing our ability to predict activity, interpret new data and react with speed and certainty.'

At the core of the new development is what Liapis calls 'agile software', which will allow users to define – and government and commercial developers to provide – responsive, relevant software in a matter of weeks or months instead of trying to plan for what is needed five years from now. 'Space is an increasingly dynamic and contested environment, and our space operators must have rapid access to any new applications they need,' explained Liapis.

The agile software will function in the framework of the enterprise battle management C2 concept that will provide software and hardware architectures to enable the US to share critical data with partners, develop new applications and identify and mitigate threats more efficiently.

Seeking improvement

Over the past few years, the USAF has signed agreements with several commercial entities to purchase innovative SSA technology and services. For example, in October 2016 Applied Defense Solutions won a contract from the air force to provide SSA services to augment the military's own capabilities. The company then said it would work with partners including Lockheed Martin, Pacific Defense Solutions and Kratos RT to provide commercially sourced SSA data.

In April this year, the USAF Space and Missile Systems Center awarded a $6 million contract to Austin, Texas-based Slingshot Aerospace to deliver AI solutions for next-generation SSA technology. According to a press release, the intelligent algorithms will enable the air force to move from traditional catalogue-based approaches to a more predictive solution.

AGI also has a stake in serving the military. The company signed an agreement with the USAF in April to exchange information and services. As part of the deal, AGI will be able to request specific information from the 18th Space Control Squadron, which it will receive within one day instead of the previously required three to four months.

Langster stated that the development of faster and more capable algorithms for data processing is the biggest challenge facing the SSA field. AGI operates its own network of optical telescopes, but also utilises data provided by third parties, and is actively looking at developing new sensors. The amount of data that these telescopes and sensors generate needs to be processed in near-real time and with better accuracy, in order to help satellite operators to understand the risks from approaching space debris.

AGI has been developing its SSA data-processing analytical engine since 2009, ▶

and the company hopes to offer its products to the defence forces. 'There is a critical gap in being able to process the number of data sources that exist today, in being able to fuse it and turn it into actionable information in a timely manner,' said Langster. 'The military are also interested in fusing commercial and government sources and bringing in additional data sources.'

He added that the need for a better data-processing capability will only get more pronounced once the USAF's Space Fence surveillance system goes fully online, which is expected to happen later in 2019. Space Fence is a second-generation space surveillance system that was built by Lockheed Martin and is currently operated in the test regime. The powerful S-band radar located at Kwajalein Atoll in the Marshall Islands successfully detected the breakup field from the Indian ASAT test earlier this year. Once fully operational, the radar will be able to detect ten times more objects than existing US SSA telescopes.

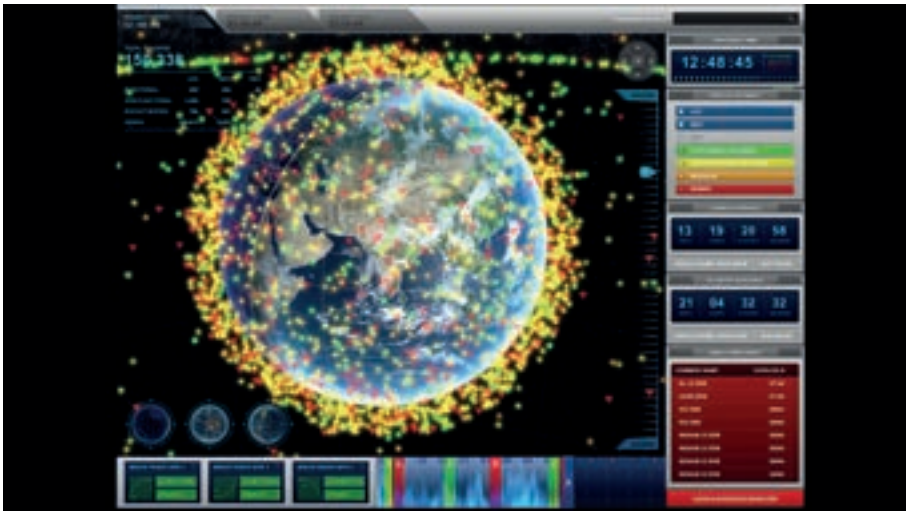
'Space Fence will bring major improvements to the way the US detects, tracks, catalogues and characterises space debris and adversary space systems,' asserted Liapis. 'It will provide near-real-time small-object detection, high-accuracy observations and the needed Southern Hemisphere coverage for timely detection of events and threats and improved object characterisation.'

The Air Force Space Surveillance Network currently tracks more than 25,000 objects. When Space Fence comes online, it is anticipated that this number will increase significantly due to the greater sensitivity to see smaller objects which can threaten critical assets. 'Space Fence could add another 200,000 or more objects to the catalogue,' commented Langster. 'There is a glut of data that is out there now and that will be out there in the future, and if you think about the upcoming low Earth orbit constellations, they will be generating data too. SSA is not only about physical space flight safety but there is also radio frequency interference.'

According to Sachdeva, currently available technology generates a large number of false positives – alerts that prompt operators to perform avoidance manoeuvres with their spacecraft to avoid a presumed risk when the piece of space debris is actually passing within a relatively safe distance. Avoidance manoeuvres cost fuel and therefore reduce the life span of missions. Reducing the number of false alerts and providing alerts with better accuracy is therefore one of the goals of the new technologies.

'We need more accuracy, more precision and more timely solutions,' Sachdeva said. 'Right now, most SSA systems are ground-based telescopes and radar, but we might need to add some space-based systems that could provide the latencies, accuracy and precision that we need. We need to be able to merge data from space- and Earth-based sensors.'

The Space Fence system, once fully operational, will be able to see ten times more orbital debris objects than what is possible with existing technology. (Image: Lockheed Martin)



Ready to launch

The USAF runs the Space Based Space Surveillance programme, which currently has five satellites in orbit designed to gather data about other man-made objects in space.

The Block 10 Pathfinder satellite was launched in 2010 and is expected to last until at least 2020. Orbiting at an altitude of about 630km, the satellite looks up towards the geostationary belt at 36,000km, where most important military space assets are located. It can detect and monitor objects that are no smaller than $1m^3$ and provide data to enable predictions about their trajectories.

As part of its Geosynchronous Space Situational Awareness Program (GSSAP), the air force also operates four satellites in a near-geostationary orbit that monitor the geostationary ring in greater detail. The first two of the GSSAP quartet of satellites were launched in 2014 and became operational in 2015 after a period of testing. The second pair was added in mid-2016 and became operational about one year later.

Commercial operators also have their stake in space-based SSA. In April this year, California-headquartered ExoAnalytic Solutions, which operates 'the largest ground-based SSA telescope network in the world', partnered with Canadian start-up Northstar, which is developing a constellation of 40 satellites that will track orbital objects from space.

With space-borne sensors, SSA providers can overcome weather challenges and any disturbances caused by the atmosphere that limit ground-based telescopes. In November 2018, Northstar won funding from the Space Alliance, a strategic partnership between European aerospace manufacturers Telespazio and Thales Alenia Space, to build its constellation of 700kg satellites fitted with optical cameras for monitoring the orbital environment.

Langster said that AGI is looking at the development of innovative sensors such as the commercial deep-space radar. The technology – located at the Algonquin Radio Observatory in Ontario and developed jointly with Canadian company Thoth Technology – can detect objects

The powerful S-band Space Fence radar located at Kwajalein Atoll in the Marshall Islands is set to become fully operational this year. (Image: Lockheed Martin)

about 2m in diameter located in the geostationary orbit and higher.

Langster added that AGI is also looking into other sectors for inspiration on how to achieve further improvements. For example, some systems used in the maritime domain, which allow ships to constantly transmit information about their position, could be used in satellites in the future. 'We have lots of concepts and ideas that we would like to bring to the marketplace... that would also give us the resources to help other international customers,' he explained.

Scope of responsibility

In addition to integrating more commercial services into the military SSA toolkit, there is a trend emerging for increased international cooperation.

To date, the US Strategic Command has signed one hundred SSA cooperation agreements with other countries, international organisations and commercial satellite operators. Partners include the European Space Agency, the European Organisation for the Exploitation of Meteorological Satellites and multiple nations: Australia, Belgium, Brazil, Canada, Denmark, France, Germany, Israel, Italy, Japan, the Netherlands, New Zealand, Norway, Poland, Romania, Spain, South Korea, Thailand, the UAE and the UK.

'The way we defend and protect our way of life is to build alliances and partnerships with countries who also embrace the shared goal of continued peaceful use of space,' said Liapis. 'Our international partners have contributed to SSA and have aided our ability to communicate across the globe for years.'

However, since an ever-increasing proportion of what is happening in space is a result of commercial endeavours, there is an impetus to delegate some of the SSA responsibilities to another body and allow the military to focus purely on defence-related SSA activities.

'The US Air Force is inherently a military organisation, and currently its resources are being utilised for non-military purposes when it comes to space traffic management or space flight safety for commercial, civil and international operators,' said Langster. 'In the last five years, there has been a growing momentum to hand this responsibility over to a civil agency, such as the Department of Commerce.'

Langster believes such a move would significantly boost the opportunities of commercial SSA providers internationally. 'We believe that there is a tremendous amount of opportunity for commercial players like AGI to provide SSA capabilities from the processing side, the collecting side, and the distribution of SAA information,' he said. 'That includes the DoD developing concepts of operations that employ and leverage the continuous innovation offered by commercial providers.'

Both Langster and Sachdeva agree that there is a growing urgency for all players globally to start taking the issue of SSA more seriously both in terms of regulations and the deployment of technological innovations. 'The problem is that right now nobody is really thinking about these things, because they think that it is a future problem,' Sachdeva said. 'They think that the biggest thing that could happen is having a collision and some money being wasted, but they don't realise that if nothing is done, in the future the space around the Earth could become inoperable.'

Langster added: 'Some people think that we have time to take on this challenge, but we really don't. SpaceX has launched the first 60 of their satellites. OneWeb started launching their constellation back in early March, and there are lots of other players launching small satellites. There is a real urgency to address this problem.' ■

The BriteCloud-218 decoy entered service on board the RAF's Tornado-GR4 fleet. It has now been deployed on board the Typhoon F/GR4. (Image: Leonardo)

TRIPLE COUNTERTHREAT

Although threats to aircraft keep evolving, so do expendable countermeasures, helping aircrews to complete their missions and get home safely. *Shephard* investigates the roles of three complementary advancing technologies in the airborne self-protection domain: chaff, flare and active RF decoys.

By Thomas Withington

The sky can be a dangerous place. 'The use of more refined targeting systems both in the RF and IR domains, coupled with evolving counter-countermeasures techniques, all contribute to the increasing lethality of the modern surface-to-air missile [SAM] and air-to-air missile [AAM]', noted Andy Hogben, managing director of UK-based expendables manufacturer Chemring Countermeasures. Never before have AAMs, radar and SAMs possessed more capabilities to recognise and reject countermeasures. At the same time, legacy threats are still able to land a punch, as recent conflicts in Afghanistan and Iraq and ongoing operations in Syria have illustrated.

These realities are keeping the airborne countermeasures industry on its toes. Manufacturers are working hard to continue the momentum of innovation in chaff, flare and active RF decoy technology.

Fantastic four

Flares, which are vital for outfoxing IR-guided weapons, form one part of the expendables triumvirate, alongside chaff and active RF decoys. Each element has its own unique attributes which work to keep an aircraft safe. Flares exploit a fiendishly simple principle – they ignite to produce a heat source that the IR-guided AAM or SAM will find more tempting than the targeted aircraft's engines to which the missile had locked on.

Flares employ four approaches: traditional, pyrotechnic, spectral and kinematic. Traditional systems tend to be produced from materials such as MTV (magnesium Teflon Viton), which will burn at a higher temperature than the aircraft's engine to present a seemingly more lucrative target. They must be deployed in a particular sequence and, like most

expendables, are used in conjunction with certain aircraft manoeuvres intended to help break the missile's lock. 'An MTV flare is there to defeat the simpler heat-seeking missiles,' commented Hogben.

Pyrotechnic flares will ignite in contact with oxygen upon release from the aircraft. These countermeasures have the advantage of being largely covert in that they cannot be seen during the day and will produce only a faint glow at night. This makes it very difficult for the launcher to determine if the missile has locked onto the aircraft or the countermeasure. Such expendables tend to be used pre-emptively.

Spectral flares aim to produce a varied heat signature. A plane does not have the same temperature across its airframe – areas closer to the engine will be hotter than those further away. A spectral flare replicates this differential and presents it to the missile to lure the weapon away from its target.

It has been more than 60 years since the USAF deployed the Hughes AIM-4B Falcon, which was the first IR-guided AAM. During that time, missile engineers have devised methods to outflank IR countermeasures. This has in turn triggered new approaches to the design of countermeasures. For example, when a missile's IR seeker can compare the temperature increases caused by a flare suddenly igniting in the atmosphere and the more gradual changes in an aircraft's engine temperature as the pilot increases or decreases the throttle, the missile's seeker programming can cause it to reject this new heat source and continue to focus on the original target of the engine.

Similarly, IR seekers can identify and reject heat sources moving rearward and downward from an aircraft, as the flares are ejected. This has given rise to the development of forward-firing kinematic countermeasures, which are projected ahead of an aircraft's direction of travel to outflank the seeker's discrimination technique.

A cousin of the kinematic flare is the rate bias countermeasure. Normally, when a flare is ejected from the aircraft, its relative angle and position will change as the flare typically moves at a slower speed than the platform. A rate bias flare contains a weight that causes the countermeasure to fall rapidly from the aircraft, thus defeating the missile's ability to discriminate the different velocities of the vehicle and flare. Likewise, thrusted flares follow the trajectory of the aircraft for some distance before falling away.

Another challenge is that a two-colour IR seeker is capable of comparing the extremely high temperature of the flare with the engine's lower temperature, and consequently conclude that the former is a decoy, so reject it. The trick for the pilot is therefore knowing exactly which countermeasure to deploy in response to each particular threat, but the chances of them being able to identify the danger in the speed and chaos of battle is remote.

Forward-firing flares are intended to outfox the ECCM capabilities of IR-guided missiles, which may be designed to discount flares travelling in an aircraft's wake. (Photo: Etienne Lacroix)

To combat this, 'you never fire one sort of flare', said Hogben. 'You fire a cocktail of flares (MTV, spectral and/or kinematic).'

Chemring is currently developing a single flare that can carry multiple payloads. 'This should be available within the next five years and will be configured to fire from standard countermeasure dispensers,' Hogben continued.

Snow storm

Chaff is arguably the most famous airborne countermeasure. Perfected by the Welsh scientist Joan Curran during World War II and codenamed 'Window', it was first used during Operation *Gomorrah*, which was the combined UK RAF and US Army Air Forces raid on the city of Hamburg in Northern Germany between 24 July and 31 July 1943. Window was intended to jam German Air Force FuMG-62D Würzburg 560MHz fire control/ground-controlled interception radars. These were used for directing fighters towards the attacking main force.

Window comprised strips of aluminium cut to precisely half the wavelength of the radar they were intended to jam, in this case, the FuMG-62D. When transmitting at 520MHz, this radar's waves would have a length of 536mm, so the aluminium strips would be 268mm long. The bomber crews would be outfitted with several bundles of the chaff, which they would physically throw out of the aircraft during their mission.

The effect would be that the aircraft was surrounded by large clouds of hundreds of thousands of aluminium strips, which was a nightmare for the radar operator. This is because transmissions would hit the bomber and the individual metal strips, which each produced their own radar echo. The effect on the radar operator's screen has been likened to a snow globe shaken to agitate the enclosed white particles – the screens would be deluged with a multitude of radar echoes, thus hiding the aircraft within the electromagnetic pandemonium.

Chaff was the US nickname for Window and is in popular usage today as a general term for that type of countermeasure. It has remained relevant thanks to the continued use of radar as the preferred means to detect aircraft and flying objects at range.

'In the past four to five years, I've seen a resurgence of interest in the RF countermeasures domain,' said Hogben. ▶

'The threats in Afghanistan and Iraq were more focused on IR-guided missiles, such as those launched by MANPADS [man-portable air defence systems].'

For instance, in Iraq between 2003 and 2010, open sources state that 46 aircraft were lost to hostile fire; at least six of these were due entirely, or in part, to MANPADS. However, the threat from semi-active and active radar homing (ARH) AAMs and SAMs – like the Almaz-Antey S-400 (NATO reporting name 'SA-21 Growler') high-altitude SAM system, which has been deployed to support Russia's intervention in Syria and to protect Russia's Kaliningrad enclave in the Baltic – is concentrating minds in NATO and beyond.

Hogben stated that customers are keen to ensure that they can deploy 'cocktails' of chaff to jam a wide array of RF threats. 'There is a need to defeat broadband RF threats, including target acquisition and fire control radars and ARH seekers used by the missile itself,' he explained.

This can result in an aircraft needing to carry an array of chaff potentially spanning a wide segment of the radar spectrum, from L band (1.215-1.4GHz) up to Ka band (33.4-36GHz) and beyond into millimetric wavebands. Hogben added that 'the beauty of chaff is that it is relatively inexpensive and easy to manufacture'.

French manufacturer Etienne Lacroix told *Shephard* that 'chaff still remains a practical means for spoofing RF threats, mostly for aircraft which are equipped with airborne jammers, to decoy missiles which are out of the normal band or to degrade the tactical electromagnetic situation'.

Nonetheless, as radars have proliferated across the radio portion of the electromagnetic spectrum (30Hz to 300GHz), the design of chaff has followed suit. X-band (8.5-10.68GHz) radars use very narrow wavelengths of circa 3cm. This allows them to see targets with a high degree of accuracy, making such radars particularly favoured for fire control and missile guidance. Therefore, chaff needs to be cut to lengths of 1.5cm in order for them to be effective.

This creates its own challenge. Radar technology is moving into what is termed the 'millimetric wave' realm, encompassing frequencies of between 30GHz and 300GHz with 10mm to 0.9mm wavelengths. These radars provide even sharper precision than current X-band systems, making them attractive for missile guidance where airframe space is limited and the need for accuracy paramount.

> ***"A rate bias flare defeats the missile's ability to discriminate the different velocities of the vehicle and flare."***

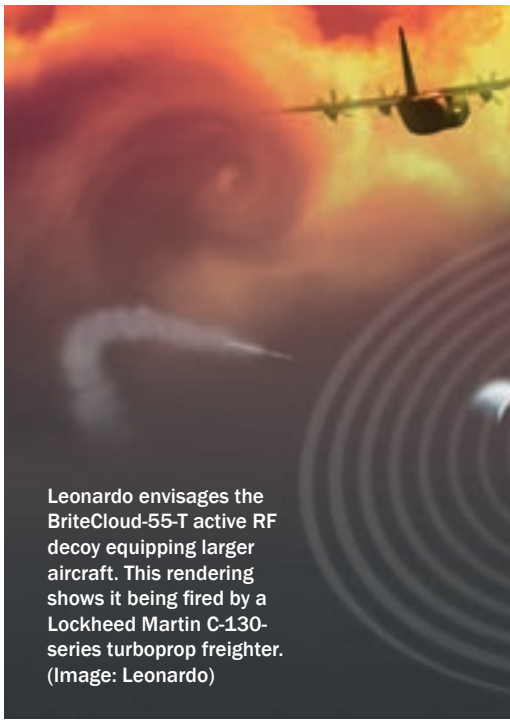
The problem for expendable countermeasures designers is that the chaff needed to spoof weapons thus equipped has to be cut to progressively shorter and precise lengths of between 5mm down to 0.45mm, which is difficult. 'Millimetre-wave threats are here and now,' noted Hogben. 'They are proliferating more and more.'

Con air

One riposte to the millimetre-wave challenge is the active RF decoy, which could also help to protect aircraft from contemporary radars with sophisticated electronic counter-countermeasures (ECCMs) that can detect and recognise chaff and discriminate it from the target.

'This is why active decoys are becoming so important against highly sophisticated threats,' confirmed Geoff Tithecott, Leonardo's EW capability manager. The company has developed the BriteCloud expendable decoy, which is available in two variants: the BriteCloud-55 equips combat aircraft with 55mm countermeasures dispensers; and the BriteCloud-218 covers 218mm systems.

In March 2018, the latter system was cleared for use with the RAF's now retired Panavia Tornado-GR4 combat aircraft. It has since transitioned onto the service's Eurofighter Typhoon F/GR4. One clever aspect of the countermeasure's design is its ability to be deployed from the platform's standard chaff and flare dispenser. This removes the need for new subsystems to be installed on the aircraft in order to use the decoy.



Leonardo envisages the BriteCloud-55-T active RF decoy equipping larger aircraft. This rendering shows it being fired by a Lockheed Martin C-130-series turboprop freighter. (Image: Leonardo)

Once launched, BriteCloud emits RF with the intention of jamming or spoofing radar-guided AAMs and SAMs. The countermeasure is capable of transmitting frequencies in the upper part of C band (5.25-5.925GHz) through to Ku band (13.4-14GHz/15.7-17.7GHz). As such, the decoy could be effective as a last-ditch countermeasure for use against ARH missiles using millimetric-wave transmissions, with lower frequency threats continuing to be engaged by chaff.

Another interesting aspect of BriteCloud is its use of DRFM (digital radio frequency memory) technology, which allows an incoming radar transmission to be captured, subtly manipulated and then retransmitted. This is done to achieve a far more 'surgical' method of electronic attack compared to blasting electronic noise across a selection, or a comparatively wide band, of frequencies.

Many contemporary radars employ ECCM techniques, which can detect jamming noise and filter it out. DRFMs record and digitise the incoming signal that can then be modulated to have a specific effect when it is retransmitted back to the radar. For example, a radar transmitting pulses that hit an aircraft flying directly away from it will take an increasingly longer time to return to the radar as echoes. They will also become progressively lower in frequency

as a result of this – a phenomenon known as Doppler shift.

By measuring the time it takes for the radar transmissions to travel to the aircraft, be reflected and return to the radar as an echo, and dividing that figure in two, it is possible for the radar to ascertain the aircraft's range. At the simplest level, a DRFM can take the characteristics of the radar pulses and transmit them within the gap it takes the real radar pulses to perform a round trip. This could have the effect of fooling the radar into thinking that the target is closer than it is, due to the comparatively large number of pulses it is now receiving.

Similarly, the change in frequency caused by the Doppler shift means that an object flying towards the radar returns echoes of increasing frequency as they take less time to return to the transmitter. Radars can therefore use Doppler shift to determine the speed of a moving target, but by manipulating the frequency of the echoes, a DRFM can obfuscate this.

These are just two of the simplest deception techniques that can be performed by DRFMs, but such systems possess a myriad of highly sophisticated similar tactics that can be brought to bear.

Presently, BriteCloud can only be programmed with the countermeasure schemes required during the mission on the ground. That said, Tithecott stated that work is ongoing to ensure that the decoy can be reprogrammed in flight. This could allow the pilot to request it to perform new jamming schemes if, for example, a threat suddenly appears during the mission. BriteCloud is currently able to 'listen for a lot of disparate threats and then counter them as and when they come on stream', remarked Tithecott.

Leonardo is now looking ahead to the development of new BriteCloud variants. The BriteCloud-55-T – which is the same size as the BriteCloud-55 but can transmit more power – is being designed to outfit military aircraft with larger radar cross-sections than fighter planes, such as freighters, tankers, large helicopters and airborne early warning aircraft, according to Jon McCullagh, head of combat air sales at Leonardo's EW division. 'We hope to complete testing next year and then move into production in early 2021,' he said.

Evolutionary triangle

Despite the advent of the active RF decoy, Leonardo does not see chaff disappearing. While BriteCloud is optimised for narrowband radars transmitting in frequencies that are typically employed by ARH seekers in missiles and fire control radars, ground-based air surveillance radars (which typically perform the initial detection of aircraft) tend to operate at comparatively lower wavelengths such as L, S (2.3-2.5GHz/2.7-3.7GHz) and C bands.

Notwithstanding the advent of ECCMs when teamed with specific aircraft manoeuvres executed by a pilot to break lock, chaff still has a role to play in protecting aircraft from these threats. 'There will still be a need for chaff,' noted Tithecott. 'There are circumstances where chaff is complementary, or the alternative, to BriteCloud. You can use chaff to stop the target acquisition, and then BriteCloud to break the missile's lock.'

Hogben agrees that the countermeasures market must remain diverse in order to combat the existing and future variety of threats. 'We see legacy threats in places like Syria, where you are still getting old-style SAM threats. It's about having a golf bag of capabilities.' It is noteworthy that when the Israeli Air Force lost a Lockheed Martin F-16I jet on 10 February 2018, the Israeli MoD blamed the incident on a Syrian Air Defence Force NPO Almaz S-200 (NATO reporting name 'SA-5 Gammon') battery. The plane was shot down over northern Israel, having completed a mission to strike targets at Tiyas Military Airbase in southern central Syria. It was believed the Iranian military had commanded a UAV flight into Israeli airspace earlier that day. The design of the S-200 dates back to the early 1950s.

In terms of the future development path for airborne countermeasures, Hogben believes that the need to do more without encumbering the aircraft with a greater number of expendables, and hence increased weight, will remain paramount.

R&D for expendables is consequently focused on them being able to cover a wide waveband of frequencies or to offer an ever-broader range of options to counter IR-guided weapons. 'This will drive the use of multi-shot flares and new compositions that give more capability and performance from smaller payloads,' said Hogben.

Etienne Lacroix prizes an evolutionary, as opposed to revolutionary, approach to developing new technologies. 'From the company's perspective, developing a new generation of flare remains time- and cost-effective, and risk-limited. Evolutions can follow the threats with the risk of a strategic, technological break,' the company told *Shephard*.

Crucial to this evolution for all manufacturers involved in the design of countermeasures will be continuing conversations with the user to understand how threats are developing, how existing countermeasures are coping with these threats and how emerging technologies can be co-opted to make countermeasures more responsive to contemporary and emerging dangers.

Etienne Lacroix stresses that its contact with the European community of Lockheed Martin's F-16-series combat aircraft operators 'gives us the opportunity to have smart feedback about operational situations and future needs. Such discussions help us to pursue improvements in our future chemical and effects compositions'.

Expendable countermeasures are here to stay, and continued evolution in missile technology will mean that alongside chaff and RF decoys, flares – unlike their 1970s fashion namesake – are unlikely to go out of fashion. ■

With EW at the forefront for many militaries, demand is rising for solutions that combat the effects of electromagnetic pulse events. UK-based MPE specialises in the manufacture of high-performance electromagnetic compatibility filters. **Paul Currie**, director at the company, spoke to *Shephard* about the changing threat environment.

Rising pulse rate

MPE has a long history of providing electromagnetic compatibility (EMC) filters to militaries to protect capabilities such as communications against interference from other signals within close proximity.

There is now another focus for the company, Currie explained. 'More recently, in the last ten or 15 years, there has become this electromagnetic pulse (EMP) phenomenon. This is where either due to natural causes or solar storm or intentional action – somebody firing a missile high into the atmosphere – an EMP would be radiated that couples onto any exposed cable and delivers too much power very, very fast in a high power surge. We're talking nanoseconds, and [it can] destroy any electronic equipment that was unprotected,' he said.

Currie noted that there had been talk of a large-scale attack of this type in the past. Since the first Gulf War, a number of national strategies have been developed that outline methods to achieve a 'blackout', which would completely switch off an adversary's power, via cyber, kinetic or EMP.

MPE manufactures power line filters that have a wide application in the EMC field where high performance is required. (Photo: MPE)

Focused attack

However, the probability of state-level attacks is considered to be relatively low. Instead, the consensus within the EMC community is that concentrated and directed attacks are likely, whereby tactical EMP events specifically target certain infrastructure in the military domain as well as commercial enterprises.

'The effects might not be as widespread or as totally crippling, but the likelihood of that happening is probably far [greater],' Currie confirmed. 'We have seen various terrorist organisations stating that they are now looking at EMP as a method of delivering their threat.'

Such targeted EMP events – known as intentional electromagnetic interference – are becoming increasingly prevalent.

For a small cost and not a huge amount of knowledge or experience, it is possible for hostile entities to create something that could deliver an EMP attack. Currie explained that although these devices might not take down an entire military base, they can disrupt communications, which is critical when missions are being carried out.

This type of threat is also affecting the commercial sphere, in which data regarding the effects are easier to come by than in defence. According to Currie, from publicly available information on US power and utilities providers, it is estimated that the cost of power outages has grown to $60 billion per year. While 25% of these outages are because of 'undefined reasons', it is believed that another 25% are the result of EMC- and EMP-type activities.

> ***"Targeted EMP events – known as intentional electromagnetic interference – are becoming increasingly prevalent."***

Necessary protection

One nation that has led the way in EMP protection is the US. South Korea also has a good understanding of its needs in this arena, said Currie. However, some nations are still playing catch-up, including the UK.

'It would be true to state that everybody is aware of the threat. Everybody knows how to protect [against it], but – probably because of budget constraints – so far they have not really invested in the protection of critical assets,' he told *Shephard*.

The UK may have been held back in this regard, because until very recently, the nation did not have an authority with the ability to test EMP protection filters.

'We can see already that over the next three or four years, the UK and Europe are going to play catch-up... They are going to go through a programme of upgrading their sites to this protection, because they can now test it and now realise it is a credible threat,' Currie noted.

Furthermore, he predicts that the development of EMC filters and associated technologies going forward will see some customisation. Whether that entails 'slightly different electrical specifications or whether it's a different mechanical look and feel, there'll be something different', Currie concluded.

Currie spoke to Beth Maundrill

SEE THE BATTLESPACE FROM A BETTER ANGLE.

ALL OF THEM.

Whether you are a dismounted warfighter on the ground or a pilot supporting from the sky, Viasat's BATS-D AN/PRC-161 radio brings 360-degree situational awareness — even in highly contested environments.

BATS-D — the world's only handheld Link 16 radio.
Learn more at viasat.com/batsd-3

Viasat™