Protecting Next-Generation Military Satellite Communications with an Innovative Disaggregation Approach: Delivering Major Gains through Business Change

By Dr Mark Chang

Biography: Dr Mark Chang is an aerospace, artificial intelligence and cybersecurity specialist at PA Consulting. He has been deeply involved in the space sector over the last 20 years. He has worked with major suppliers of deep space and Earth centred space missions for communications, navigation and observation in the UK, mainland Europe and the USA Mark led the engineering for three high capability satellite missions for the ESA, a satellite constellation for the private sector and the first 14 Galileo GNSS payloads. He is currently supporting the MOD's SKYNET 6 programme.

Abstract: The Military Satellite Communications (MILSATCOM) environment is more crowded and contested than ever, with 500,000 space debris items on one hand and over 40 space-faring nations on the other. Technological innovation has ushered in an era of offensive space assets, presenting a new type of Space Race. Yet UK military space budgets remain constrained with no foreseeable economic boost likely to relieve this. New architectures must respond more resiliently than before. To mitigate budget risks, we must examine defensive options: active (shoot back, escort), passive (e.g. hardening), rapid replacement or strategic disaggregation. Most choices are inflexible or limited in effect, except strategic disaggregation – where capabilities are made difficult to target by dispersing systems. A disaggregation dominated approach will improve system interoperability between allies, industry and the UK; strong interoperability disincentivises competitor threats.

Introduction

Satellites provide a strategic advantage for the UK defence establishment and it is of prime importance to continually re-examine the vulnerabilities and resilience of the nation's constellations. We propose that disaggregated systems, coupled with host satellite partnering at an allied nation or commercial company level, will yield greater survivability, robustness and resilient capabilities for defence force elements in the face of modern threats while retaining the key requirement of affordability. It can also provide a method to insert essential technology improvements in a controllable manner, which is an option not available currently.

The role of space capabilities

Sixty years ago, the Soviet Union launched the first man-made satellite[1] into orbit. In the following decades, space systems matured to provide critical capabilities to the military in the delivery of defence tasks. Nowadays they are a mandatory part of our modern national defence complex. Acquiring and deploying these systems in a timely and affordable manner is of crucial importance to UK national security.

In the early military space era, Western powers' space systems were focused on supporting strategic missions such as intelligence and nuclear command and control, with tactical missions very much an afterthought. The UK did experience an epiphany when it made effective use of Military Satellite Communications (MILSATCOM) in the 1982 Falklands Conflict.[2]

The global watershed moment for the use of space-based capabilities in tactical support of force elements undertaking conventional operations came during the 1991 Gulf War.[3] Use of the combination of Beyond-Line-of-Sight (BLOS) communications, precision navigation and timing in synergy with weapons systems formed a new set of abilities that demonstrated the unparalleled strength of the West's air and space power.[4]

The current MILSAT environment

The use of space during the Cold War era was dominated by the superpowers. The strategic détente that emerged between these two competitors created a no-conflict zone in the space domain which held throughout that period. The extension of destructive conflict into space was viewed as unlikely but, at worst, a certain prelude to a full-scale nuclear confrontation. Thus the UK's third and fourth generation military satellite capabilities (SKYNET 4 and 5) were developed and deployed into a relatively uncrowded and safe space domain.

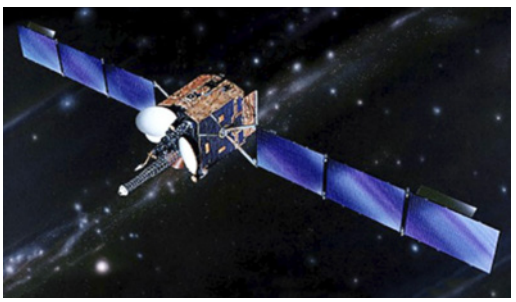

Figure 1: SKYNET 4A. Image by Dr Mark Chang

Today, space is no longer a sanctuary for the UK military capabilities.

Since the end of the Cold War, the Earth-centred space domain has seen a huge increase in activity. There are more than 1,950 active satellites[5] and a plethora of other trackable man-made objects in Earth orbit, where the majority of this is debris. Almost all nations depend on space capabilities for civilian applications like weather forecasting and navigation, and just over 40 nations have assets in Earth orbit. Some two-thirds of the active satellites are used for BLOS communications; most of these systems belong to commercial operators.[6]

The increase in the number of space-faring nations from a handful prior to 1980 to over 40 now has led to a congested and crowded domain.[7] An example of this problem is the first collision involving an active satellite occurring in 2009, when the inactive COSMOS 2251 and the operational Iridium-33 satellites impacted on orbit, creating thousands of pieces of debris in low-Earth orbit.[8] A second example highlights the potential threat at ground level: in 2016, the loss of control of the Chinese space station Tiangong-1 caused worldwide concerns over a two-year period, though it eventually burned up in the Earth's atmosphere, with the glass and titanium remnants falling into the oceans.[9]

This situation is set to worsen as a new Space Race has recently taken shape, this time driven by tech start-ups and private businesses spearheaded by billionaire entrepreneurs. All indications are that these private sector initiatives (SpaceX, Blue Origin, Bigelow Airspace, Virgin Galactic, Boeing, Lockheed-Martin, PlanetLabs, Rocket Lab for example) are not only growing rapidly but are also quickly 'besting' their government-sponsored competitors, irrespective of measure used; but, most importantly of all, in the time-to-service. The barriers-to-entry in the space sector have also decreased, the clearest measure being the number of satellite deploying launches.[10] In 2016 it was 169 while in 2017 it was almost double that number, at 310. In effect, a 'democratisation' of the costs for access to space is underway.[11]

Beyond congestion and crowding, other nations' defence establishments have taken note of the distinct advantages space capabilities provide and have developed counter-space challenge capabilities. In a highly visible demonstration, China successfully tested an anti-satellite (ASAT) weapon in 2007, destroying a malfunctioning weather satellite in low-earth orbit (LEO). The action was swiftly followed by the USA, which successfully destroyed a defunct, de-orbiting surveillance satellite by ASAT in 2008. Most recently, India[12] conducted a controversial ASAT test in March of 2019, dubbed 'Mission Shakti', destroying a 740 Kilograms (Kg) satellite which had been launched into LEO specifically as a target. In another notable milestone, China launched a quantum experiment on a satellite nicknamed Micius (or Mozi in Chinese), designed to transmit hack-proof keys from space in 2016, thus demonstrating further advances in possible competitor counter-space systems.[13]

Moreover electronic, cyber and physical attacks against the ground infrastructure used by space systems are increasingly concerning because the technological barrier-to-entry for these threats is falling, attacks are less attributable and the technology itself is more easily

proliferated. From the perspective of third nations, UK and allied military space capabilities are weapon systems, and space is a domain of warfare that can and will be contested.

Understanding the UK need for military space capabilities

The UK has eight military satellites for communications (MILSATCOM) in current operation.[14,15] The MOD has not yet directly acquired any other satellite capability class other than as demonstrators, be it intelligence, surveillance and reconnaissance (ISR), navigation, meteorology, signals intelligence, early warning or space situational awareness (SSA).

Figure 2: SKYNET 5. Image by Dr Mark Chang

While it appears that the UK lags in military satellite deployments (in the first tier the USA has 134, while in the second tier Russia has 81 and in the third tier China has 31 satellites), it is important to realise that these numbers are deceptive. Space systems are unlike many other weapons systems because they cannot be matched to comparable adversary systems to determine who has the upper hand. More or better tanks may create an advantage in a ground domain combat theatre. This logic does not necessarily hold true in the space domain as military space systems are part of a global infrastructure delivering core force element capabilities, such as precision attack or global power projection. Having a greater number of satellites or more capable satellites than an adversary does not mean there will be enough space-based capabilities to support forces. The value of military space systems is ultimately a function of how they contribute to winning the nation's wars.

A direct consideration of the numbers and types of satellites is therefore not a useful metric for the military competition in space. What matters are the BLOS capabilities these satellites enable for combat forces in other domains and the threats these systems face.

In short, the UK does not need numbers of space assets greater than its potential adversaries. Rather, the nation needs reliable, robust space capabilities that enable both freedom of action and operational advantage. In other words, we must have the right space capabilities at the right time to enable other weapon systems to be superior to those of an adversary in contests where the mission is important to the UK's interests. The use of the MOD's Skynet 5 capabilities by allied nations shows that this constellation achieved the right balance of priorities for its generation.

Threats to MILSATCOM

We highlight how the changing threat environment affects the capabilities needed in the next-generation architecture for MILSATCOM as a focus, although the same principles apply to any other satellite capability class.

MILSATCOM provides core infrastructure services upon which other weapon systems depend. Force elements at all levels are dependent on MILSATCOM for reliable BLOS communications in the air, sea and land domains. The key type of protection for UK systems developed in the Cold War was nuclear survivability, an implicit assumption being that in conventional conflict deterrence would hold and space-based systems would not be attacked. Limited space domain threats combined with the high cost of launches in the Cold War also encouraged the creation of 'Battlestar Galacticas', which concentrate multiple MILSATCOM capabilities in a very small number of systems, to be able to address a variety of defence missions rather like a Swiss Army knife.

In the post-Cold War era, potential adversaries may not have symmetric vulnerabilities, in that they do not rely on MILSATCOM systems yet can reach the space domain, making deterrence in space difficult to enact. The legacy of Cold War decisions has left the UK's space systems vulnerable to counter-space operations in an anti-access or area denial (A2/AD) situation. In the next sections, we examine the vulnerabilities of MILSATCOM systems to inform the future space domain architecture argument.

Physical threats

MILSATCOM satellites are vulnerable to kinetic attacks, like ASATs, be they ground launched or initiated from co-orbit. These types of strikes tend to be catastrophic and will create space debris that affect the satellites belonging to owners not directly involved in the conflict. Such threats are widely accessible internationally and legacy deterrence strategies are the only mitigations for now.

Non-kinetic (directed energy) attacks, such as lasers, can temporarily or partially degrade a satellite or its payload with less risk of debris. The targeting is far faster than kinetic platforms, though the effects do not need to be immediately evident (so attribution may be problematic). Enacting this threat requires costly technologies that are not widely nor easily available currently.

All Earth-centric space system architectures are comprised of the space segment and a ground segment. The ground segment is also at risk of physical attack. While they can be disrupted, they can be repaired in days to months; as such, we choose to focus on the space segment in this article.

Electronic threats

The use of electromagnetic energy to interfere with communications, commonly known as jamming, is an attack vector that can be recovered from. For example, as soon as the jammer

has disengaged, communications can be restored. Jamming can be done on the uplink to the satellite or on the downlink. An uplink jammer should be about as powerful as the signal it is attempting to jam and must lie within the footprint of the satellite antenna it is targeting – signal power dominance then becomes the game. There are other methods for uplink jamming which are more sophisticated, but the impact is the same: uplink jamming effects are generally broad, across many satellite operators.

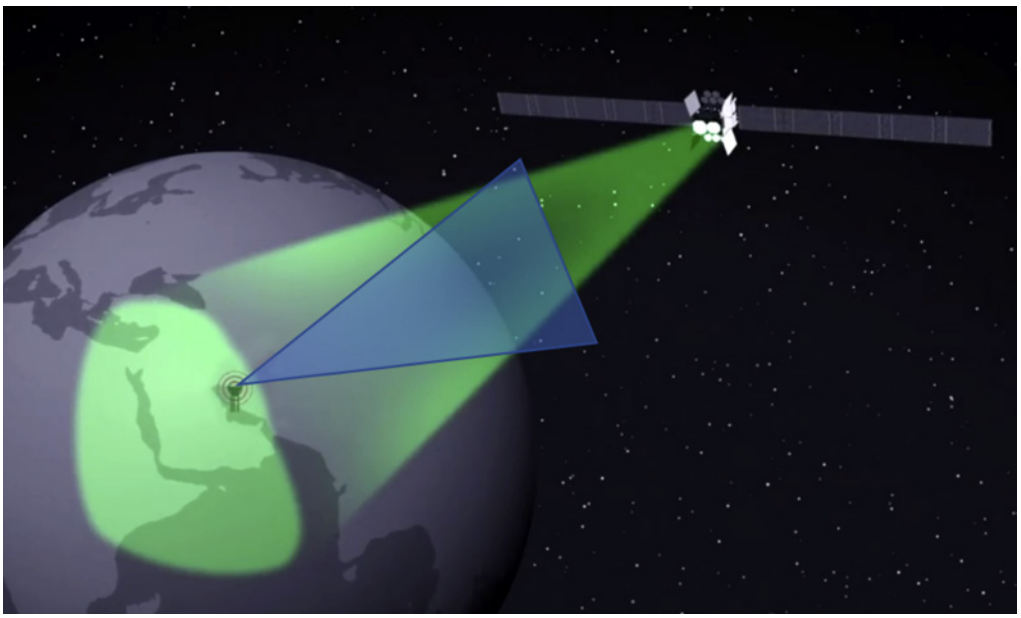

Figure 3: An illustration of uplink jamming. Image by Dr Mark Chang

In Figure 3, green areas represent the satellite footprint while blue areas represent the jamming signal.

Conversely, a downlink jammer needs to be only as powerful as the signal being received, but it must also be within the field of view of the receiving terminal's antenna. Thus, there is a limit to the number of terminals that can be affected by a single downlink jammer. Such jammers are more localised in impact.

It can be difficult to detect and distinguish jamming activity from accidental interference. It is also difficult to attribute a jamming instance to an identified source. Even where attribution is possible, neutralising the source of the jamming can present challenges.[16]

Cyber attack threats

MILSATCOM systems are also vulnerable to cyber attacks, which can intercept data, corrupt data or take control of systems for malicious purposes. Unlike electronic attacks, which interfere with the physical transmission of data by the electromagnetic spectrum, cyber

attacks target the data itself and the systems that use this data. Any data interface in the system is a potential intrusion point, including the antennas on both the satellites and terminals and the landlines connecting ground stations to terrestrial networks. Cyber attacks can target satellites, ground control stations, and terminals – successfully attacking any one of these segments gives the adversary the chance to launch additional attacks on the other segments through the vulnerability. The effects of a cyber attack on MILSATCOM systems could range from local disruption to whole network disruption and potentially the permanent loss of a satellite. Attribution for a cyber attack can be difficult, if not impossible, because attackers can use a variety of methods to conceal their identity. Cyber attacks range over eavesdropping, denial-of-service, deploying a botnet, spear-phishing, ransomware, man-in-the-middle and spoofing activities, all of which are tactics that are used more generally in our society.

Like physical and electronic attacks, cyber attacks in the space domain are already occurring. In 2009, it was discovered that insurgents in Iraq and Afghanistan had been intercepting video feeds from US Predator unmanned surveillance aircraft after copies of the videos were found on insurgents' laptops. Because the video feeds were transmitted without any protection or encryption, insurgents were able to use commercially available software to intercept the data.[17]

Budget Environment

A maxim in defence planning is 'the enemy gets a vote', meaning an adversary's decisions will affect your plans. This can be extended to include the acquisition process itself because MILSATCOM systems are just as vulnerable to cost overruns, funding instability and programmatic problems as they are to physical, electronic, and cyber attacks. Any of these can prevent a satellite from getting off the ground.

Budgets have risen and fallen in irregular cycles in response to changes in the political, economic and security environment. As plans for the next generation MILSATCOM architecture get underway, affordability becomes a major concern.

Key cost drivers
Space Segment

The main cost components of the space segment are the satellite bus (the platform, ie. the structural frame, propulsion, power, control plus any intersatellite link equipment) and its payload, and the launch vehicles used to orbit them. The cost of the satellites varies significantly depending on the type of system. For communications, in general, the bigger the satellite is the lower is the cost per data bit carried. There is a reduced satellite size needed for assets in low-Earth orbit (around 800 km altitude) compared to geostationary orbit (around 36,000 km altitude) because less power is needed to close the communications link as the satellites are closer. However, large constellations of satellites are needed to enable global coverage from low-Earth orbit.

Launch costs are also an important consideration for MILSATCOM systems. One reason MILSATCOM satellites have typically been large and highly aggregated is that the launch cost per unit mass tends to decline as the mass of the satellite increases.

Protected satellites are more expensive because the satellite bus and payload are more complex and have many unique military requirements. Naturally, the more complex and multifunctional the satellite is, the fewer there are likely to be, so more needs to be done to provide military protection per asset.

Ground Segment

The MILSATCOM control segment includes ground systems that control the satellite bus and payload.

The total cost of the control and terminal segments is difficult to quantify because the systems are funded through many different sources, some of which overlap with other programme costs. The control segment is typically funded in part through the satellite development program and is often not reported separately. The cost of the terminal segment is more complicated to calculate because the costs are spread across multiple terminal acquisition programs in all branches of the military.

Moreover, the costs of terminal antennas and integration are sometimes funded in whole or in part by the platforms in which these terminals are used.

Programmatic challenges
The Vicious Cycle

MILSATCOM acquisitions are complex with long development and production schedules and relatively small procurement quantities. These factors reinforce one another in a 'vicious cycle of space acquisition'. That is, higher costs lead to smaller constellations and longer production times; smaller constellations require more capabilities to be packed into each satellite; and packing more capabilities into each satellite drives up complexity, leading to even higher costs and longer production times.

The key risks for MILSATCOM satellites appear to be programme instability, leading to breaks in production, and unique military requirements on the satellite bus and payload. These risks are detrimentally reinforced by the UK's intermittent approach to MILSATCOM acquisitions – from both a production point of view (which impedes the existence of economies of scale) and from a perishable specialist skill set within buyer and supplier organisations (which affects the ability to specify, buy, design, build and launch into service a military satellite).

Synchronisation between ground and space programmes

Another programmatic vulnerability for MILSATCOM is synchronisation across the space, control and terminal segments. Synchronisation is the alignment of schedules among

interdependent programmes to deliver capabilities efficiently and effectively. This is important in MILSATCOM because all three segments (space, terminal and control) are needed for the system to be operational. Satellites have a finite life on-orbit: fuel is consumed for station-keeping, parts degrade from the harsh environment of space, and technology becomes obsolete with time. When one segment of the overall system is behind schedule due to funding shortfalls or development issues, other segments might be forced to delay their schedules as well.

A further complication is the spread of programmes and associated budgets that fund the three segments of MILSATCOM across the Services. Delays in a satellite programme can cause a ripple effect of delays across the terminal programmes managed separately by different Defence organisations. Likewise, delays in separate terminal programmes could lead to decisions to delay the launch of a satellite, so as not to risk placing an under-utilised asset on orbit.

Satellite programmes are also keenly dependent on other elements of the space enterprise, such as launch vehicles. A delay in the launch segment, whether due to funding, political or technical issues, can have far reaching effects across MILSATCOM acquisition programmes. Because current MILSATCOM architectures rely on a relatively small number of satellites acquired over long periods, a loss of even one satellite on launch could have severe consequences.

Defensive options for the future MILSATCOM architecture

Improving the defences of MILSATCOM systems makes it harder for an adversary to attack these systems and disrupt or degrade the ability to communicate.

Defences must cover the space, control and terminal segments. Depending on future architecture, a level of launch segment defence may also be necessary. Ultimately, the protection of an overall system is only as strong as its weakest link.

The current MILSATCOM architecture divides systems into protected and not protected, with many of the requirements for protected MILSATCOM focused on the strategic mission. Separating the architecture distinctly along these lines is somewhat arbitrary because protection is not 'all or nothing'. There are varying degrees of protection and different types of protection depending on the threat risks to a system.

To determine how best to improve MILSATCOM defences, four fundamental questions need to be answered:

1) What current and evolving threats does the system need to be defended against;
2) What is the weakest part of the system relative to these threats;
3) What level of protection is enough; and

4) What level of protection is affordable?

There are several approaches that can be adopted in response to protecting space capabilities within the environmental spectrum ranging from benign to contested or even nuclear. We emphasise that no single response will suffice to cover all conditions. Nevertheless, there is an approach that will do much to mitigate the risks present in current programmes.

For our favoured response, we identified a series of primary causes arising from the 'vicious cycle of space acquisition' problem and found five impacts that need to be disrupted.

Programmatic Vicious Cycle Primary Causes	**Impacts & thus Challenges**
Aggregated Requirements	1. Aggregated, concentrated architectures
Complex & inexecutable baselines	
Funding & Requirements instability	2. Systems vulnerable and not technologically advanced with little ability to deal with changing threat environment.
Large, complex, expensive systems with no spares	
Long schedules with no risk tolerance	
Low risk launch requiring huge, slow review process	3. High costs of launch.
Expensive launches lower launch rates, which drives up costs	
Lengthy acquisition approach leads to instability in the industrial supply base	4. Controls limiting competition & partnering. 5. Space capability acquisition mindset shaped by legacy approaches: Top down redesign and re-optimisation for new requirements & hesitancy to use leading edge technologies.

The challenges can all be addressed by adopting the approach of buying more, and smaller platforms to provide space-based capabilities. The key word is platforms, and not simply satellites. Moreover, each of the primary causes listed will be successfully addressed by the adoption of a 'disaggregation-of-monoliths' approach.

Resilience and Disaggregation

Our innovative approach in response to a rapidly changing security and fiscal environment is to make MILSATCOM system elements more difficult to threaten or be interfered with by

1) disaggregating capabilities: so multiple missions do not depend on the same satellite constellation; and
2) disaggregating systems: payloads are distributed across a larger number of satellites in different orbital planes.

In a disaggregated architecture, each satellite is smaller and less capable than current

'Battlestar Galacticas', thus individually less expensive. The overall cost of the constellation will still depend on many factors, so would need to be carefully implemented.

This 'disaggregation of monoliths' approach enables threats to be avoided and ensure the survival of critical capabilities despite hostile action. It also creates the capacity to rapidly reconstitute, recover or operate through adverse events should robustness fail.

Attributes of Disaggregation

Disaggregation is a strategy to affect multiple elements of our overall space architecture. Its purpose is to provide options to drive down cost, increase resilience and distribute capability. It brings other benefits too – allowing systems to be less complex, more maintainable with lower per-unit production costs. An emergent outcome should also be the ability to improve the stability of the industrial base, which is not something that occurred when the current generation of monolithic space systems were fielded.

It is important to observe that, while this paper is focused on the space segment, disaggregation is an enterprise level approach. All connecting nodes, ground systems, command and control and launch vehicle architecture will benefit similarly.

Disaggregation offers an enduring ability to keep pace with advancing technologies, sustainment of the space sector's industrial base, achieving affordability and deterring adversarial action.

The Payload-Centric Model

One approach to facilitate disaggregation within the space segment is to adopt a payload-centric acquisition model. Rather than designing and building satellites from the top down with a defined set of capabilities, a payload-centric approach would focus on specifying the capabilities of the payload first and then finding a satellite bus to host the payload. Using this approach, the payloads could be designed from the outset to be hosted by a wide range of satellite buses.

It would also separate the procurement of satellite buses from satellite payloads and create greater options for MOD payloads to be hosted on non-MOD satellites.

Hosting MILSATCOM payloads on the satellites of other nations, a dispersal method allowed by disaggregation, could be used to complicate an adversary's calculus. While such an arrangement would require overcoming various political and operational challenges, the potential benefits are high and worth exploring. From the UK allies' perspective, this approach would improve interoperability with the UK military and give them access to a global constellation at a much lower cost than fielding an equivalent capability on their own. From an adversary's perspective, this would greatly complicate planning because an attack on the hosted payload (whether physical, electronic, or cyber) would be an attack on both the

UK and the host nation, creating the risk of horizontal escalation in a crisis. Thus, the approach provides an incentive for good behaviour in space.

Make Systems Easier to Replace

Another aspect to address the vulnerabilities of MILSATCOM systems is to make the systems easier to replace after an attack. The current space segment architecture is difficult to reconstitute because existing military satellites are large, complex, expensive, and procured over long periods at low production rates. A more easily reconstituted architecture using the approach outlined will result in UK MOD assets that are smaller, less expensive, and procured in larger numbers at a steady production rate.

Obviously, the most basic option is to have spare satellites in storage and ready for launch, but that brings with it the risk of a large logistical infrastructure cost. Two key limitations in this simplistic spare satellite approach are cost and schedule. The spare satellites would have to be sufficiently inexpensive to allow for the procurement of reserves and they would need to be ready for launch within a short timeframe. Even with satellites sitting ready in storage, it would take weeks to months to integrate them with launch vehicles, launch them, and move them to the desired orbit. Right now, the time-to-service for a MILSATCOM space asset from early development is about 14 years.

The options for making systems easier to replace overlap in many ways with the options for disaggregating the architecture. A payload-centric approach makes the system easier to replace. The military could have extra payloads ready to launch on hosts to replace degraded or lost space assets. While the limitations mentioned above still apply, the magnitude of costs and schedule impacts can be mitigated by aligning with the most competitive part of the space enterprise: the commercial satellite bus market. This market has consistently produced satellites in 24 to 36 months at much lower price points than the dedicated MILSATCOM sector. The technology to package militarily useful capabilities small enough to be hosted (or to make use of smaller launch vehicles) has been demonstrated and is publicly documented by the Hosted Payload Alliance.[18] Robust commercial encryption standards and components can be effectively leveraged to define protected communications waveforms, payloads and terminals that are small, less complex and more manageable than current UK MOD systems. In the unprotected realm, commercial wideband communications supporting Remote Piloted Aircraft (RPAs) and Airborne Intelligence, Surveillance and Reconnaissance (AISR) have been in use for over a decade. These capabilities can be secured and packaged as a payload or a dedicated platform, in turn enabling options for both hosted payloads and smaller, less complex satellites. Reducing the complexity of the capabilities provides options to recover terminal programmes that are suffering from slippages.

Security and Commercial SATCOM

Rather than designing, building, and launching its own unique satellites for unprotected communications, the military can and does lease SATCOM services from commercial providers.

Commercial SATCOM (COMSATCOM) provides several advantages, including no development costs and the flexibility to expand or reduce capacity as needed. COMSATCOM has proven invaluable over the past decade of operations in Iraq and Afghanistan, where front line demand for high-bandwidth applications has grown.

In general, COMSATCOM systems are not designed for a contested communications environment. In the main, they offer no protection from physical attack and will not have any nuclear hardened designs. On the other hand, they do have degrees of protection against electronic and cyber attack as these affect business critical capabilities.

Moreover, security is a highly significant concern for commercial satellites because they can be owned or operated by a foreign entity, may connect to ground stations in foreign countries, and may be used simultaneously by a foreign government or foreign-controlled entities.

We suggest that the security risks can be managed through an 'assured capability' process aligned with explicit recognition of the MILSATCOM mission. 'Assured capability' can be broken down into five steps:

1. Develop the MILSATCOM mission ecosystem taxonomy.
2. Risk assess each element of the ecosystem.
3. Determine the acceptable level of risk for each element.
4. Identify the level of assurance below which the MOD is not prepared to tolerate compromise of the mission capability, even in the face of mitigation activities.
5. Specify and audit assurance requirements, informed by a framework of assurance categories.

Changing our acquisition approach

To effectively and efficiently implement a distributed architectural strategy, the UK's military space acquisition strategies will have to change. Designing and procuring satellite capabilities to optimised top-down requirements will not be compatible with the highly interchangeable and interoperable view that we recommend. Uniquely designed and manufactured components must be dispensed with as much as possible; a more flexible model of commoditised capabilities and making use of economies of scale should be the concept for the next generation architecture.

We should consider a wholesale focus shift of current UK MOD space system development efforts towards mission payloads. By designing a payload to provide the core capability needed by force elements, supported by commercial buses, the ability to make use of both the commercial bus market and hosted payload, opportunities blossom. Acquiring the mission payloads as the core element of a mission-domain architecture allows a product to be created with the ability to fly on either a dedicated bus or as a hosted payload with minimal changes to the production baseline.

This focus shift allows for a mirroring of commercial practices such as competition for satellite bus procurement. Hosting payloads need not be, and should not be, a bespoke exercise requiring heroic efforts to gain approvals, modify products and meet schedules. It should be an inherent part of the national defence strategy to deploy capabilities in orbit. Adjustments to make use of hosting opportunities can be made by matching the timing of payload production with the host satellite assembly, integration and verification (AIV) schedule.

By tailoring the amount of capability that goes into a single payload, additional opportunities are created to synchronise the space and ground segment strategies. More payloads mean that terminals can be uplifted at a more regular drumbeat than the present once-every-15 years, giving opportunities to insert new technologies in a predictable fashion. A direct comparison between this proposed approach and that of commercial mobile telephony can be made to further understand and quantify the benefits.

Conclusion

Disaggregation, coupled with host satellite partnering at an allied nation or commercial company level, will allow the UK MOD to realise a more affordable and resilient set of capabilities for defence force elements. The involvement of commercial companies can be managed by providing a strong assurance wrapper to ensure the security of capabilities. By disaggregating battlespace awareness and other tactical MILSATCOM missions from core nuclear-hardened, strategic capabilities through a payload-focused acquisition strategy:

- Complexity and cost are reduced, allowing more predictable, controllable and executable programme baselines;
- Requirements are stabilised by creating a process for capability insertion;
- Operational and economic consequences of vehicle loss are reduced;
- A regular and shorter replenishment cycle is established;
- More launch and deployment opportunities are generated; and
- Any adversary's calculus with A2/AD actions are complicated, if not undermined, in any conflict.

We end with a comparison note: the precedent has already been set with both Galileo and GPS II (and III) GNSS systems. These are distributed, disaggregated assemblies of individual payloads. Taken together, the components form a robust, affordable and resilient architecture which has an established production line permitting routine insertions of new technology.

The UK has a need and an opportunity to seek affordable, resilient, survivable space capabilities in ways which keep up with the incredible pace of technological change and adapt in the face of evolving threats. Equally, a strong supply base which offers buyer choice and vendor competition is essential to control costs while protecting perishable skills and specialised logistics.

The mission-led, payload-centric disaggregation strategy that we are proposing can achieve all these aims – the time is ripe to harness this vision.

Acknowledgements

With sincere thanks and acknowledgements to colleagues for their valued inputs:
Harpal Singh*, James Bates*, Andrew Creber*, Nick Newman*, Peter Dingley#
Andrew Parsons## [*PA Consulting (https://www.paconsulting.com/); #PDRF Ltd, ##SVGC Ltd].

Notes

[1] Garber, S., "Sputnik and the Dawn of the Space Age". Retrieved 10.05.2019, NASA History Website: https://history.nasa.gov/sputnik/.
[2] UK Military Space Programmes, Whitehall Papers Volume 35, Issue 1, 1996, The Royal United Services Institute for Defence and Security Studies.
[3] Admiral Sir Jock Slater, "A fleet for the 90s", The RUSI Journal, 138:1, 8-20, 1993. DOI:10.1080/03071849308445672. Retrieved 13.05.2019, The RUSI Journal Website: https://tandfonline.com/toc/rusi20/138/1.
[4] Covault, C., "UAVs Drive SATCOM Modernization", 26 October 2010. Retrieved 13.05.2019, DefenseMediaNetwork Website: https://www.defensemedianetwork.com/stories/uavs-drive-satcom-modernization/.
[5] "The Satcom market", ESA. Retrieved 13.05.2019: https://www.esa.int/Our_activities/Telecommunicaitons_Integrated_Applications/The_satcom_market.
[6] Union of Concerned Scientists Satellite Database, https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database, accessed 05.03.2019.
[7] Hobe, S, "The Impact of New Developments on International Space Law". Retreived 13.05.2019 United Nations Office for Outer Space Affairs Website: http://www.unoosa.org/pdf/pres/2010/SLW2010/02-12.pdf.
[8] Retrieved 10.05.2019: https://celestrak.com/events/collision/.
[9] "Tiangong-1: Defunct China space lab comes down over South Pacific", BBC News 2.4.2018. Retrieved 13.05.2019 BBC News Website: https://www.bbc.co.uk/news/science-environment-43614408.
[10] Aaron Clark and Dan Murtaugh, "Satellites are Reshaping How Traders Track Earthly Commodities.", Bloomberg, December 16, 2017.
[11] "Total Launches by Country". Retrieved 13.05.2019: https://aerospace.csis.org/data/space-environment-total-launches-country.
[12] Retrieved 13.05.2019 BBC News Website: https://www.bbc.co.uk/news/world-asia-india-47729568.
[13] "China launches quantum enabled-satellite Micius", BBC News 16.08.2016. Retrieved 13.05.2019: https://www.bbc.com/news/world-asia-china-37091833.
[14] "What is Skynet?". Retrieved 13.05.2019: https://ukdefencejournal.org.uk/what-is-skynet-a-look-at-britains-military-communications-satellites/.
[15] "Skynet 5". Retrieved 13.05.2019: https://www.defenseindustrydaily.com/Skynet-5-uk-mods-innovative-satcom-solution-06244/.

[16] Peter B. De Selding, "Eutelsat Blames Ethiopia as Jamming Incidents Triple." Space News, June 6, 2014.
[17] Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones," The Wall Street Journal, December 17, 2009.
[18] Hosted Payload Alliance, http://www.hostedpayloadalliance.org/, accessed 05.03.2019.