UK Strategic Commander DSEI 2021 Speech

Good morning. It’s great to be back doing events live and in person and I want to join you all in expressing my thanks to Clarion, the organisers and Fujitsu, our sponsors here, for putting on such an outstanding conference, so far. It is very good to see so many faces in the audience.

When I last spoke here, in 2019, it was shortly before we launched Strategic Command. It’s been quite a journey, standing up the Command to drive the Integration and S&T agenda for Defence, but I think the fact that Multi-Domain Integration is the theme of DSEI this year shows that the imperative is well-recognised and our advocacy has been gaining some traction. Why should we care about Multi-domain integration?

One word: Threat.

The threat isn’t diminishing. In fact, the security outlook is more perilous than it was 2 years ago: we are now facing the twin spectre of emboldened Jihadi terrorists and something not seen since the 1930s – a growing authoritarian zeitgeist that celebrates the suppression of political and individual freedom as a better way to govern. This ideology is intersecting with geopolitics and driving great power competition as these autocratic regimes subvert and challenge the international order and adopt bold risk-taking strategies.

The risks are clear: it is a recurring pattern of great power behaviour that interests expand with power, that the appetite grows with the eating, and that risk-taking accelerates the potential for escalation and miscalculation unless this behaviour is challenged and contained. Without that we will find ourselves in a world where the strong do what they can and the weak suffer what they must. Or put another way to use my favourite cautionary tale from Hilaire Belloc: Pale Ebeneezer thought it wrong to fight. Roaring Bill, who killed him, thought it right.

What links these authoritarian regimes (let’s name them, Russia and China) is two things.

First an approach that seeks to win without fighting. What George Kennan described memorably as political warfare. General Gerasimov put it like this “The very rules of warfare have changed. The role of Non-military means of achieving political and strategic goals has grown and in many cases they have exceeded the power of force of weapons in their effectiveness”. Welcome to the so-called Grey Zone.

And secondly the expansion of warfare into the novel domains of space and cyber, coupled with an approach to modernisation that pursues the exploitation of disruptive information age technologies and allies these to winning operational concepts that seek to have the same impact as Blitzkrieg did. It is nothing less than a race for advantage in the defining technologies of the future.

Under its ‘Made in China 2025’ strategy, China has explicitly declared the ambition to dominate these technology frontiers. It includes artificial intelligence, advanced computing, quantum technologies, robotics, autonomous systems, commercial space technologies, additive manufacturing and the Internet of Things, along with new generations (5G and beyond) of the mobile telecommunications that will connect it.

And so the PLA has concluded that the Centre of Gravity in military operations has shifted from the concentration of forces to information systems. They look to dominate a system of systems confrontation, creating new operating concepts: cross domain, autonomous swarms and precision attack to achieve persistent paralysis.

So how can we respond to these threats?

Well we shouldn’t take counsel of all our fears. Great power conflict is not inevitable. Coercion doesn’t have to lead to a binary outcome between capitulation or conflict. Competitive coexistence is possible. But we can’t be passive: the preservation of peace requires active effort, planning, the expenditure of resources and sacrifices to underscore our credibility and will to secure our national interests, just as war does.

And we should recognise the advantages we have. Most notably for Defence, in the last 12 months we have been given the means to modernise with a historic funding settlement, the mandate to radically adapt our acquisition model in DSIS and in the Integrated Operating Concept the source code for how we will operate and fight as an integrated whole across domains.

We can respond to these threats at a national level by being more strategic, more assertive, by modernising and by being more integrated across domains, nationally, with partners across government, industry, academia and civil society, and of course internationally, with allies and partners.

But I want to be more specific. Because the reason we are all here at DSEI is to solve operational problems together and create national strategic advantage by harnessing the latent talent and ingenuity that exists in industry, and allying it to those who will have to adapt and overcome these threats in future – for those in uniform. So I want to spend the rest of my time here bringing MDI to life in a way you can relate to so you can help us solve some of these challenges, then describing the technological advances I need us to work on together, pose some questions about how we can grow the skills in our workforce to tackle these problems and then suggest how we might develop an integrated relationship with you as our industrial partners.

So what does MDI look like when it’s operationalised? And it’s important that we develop specific operational concepts to solve problems either against a particular adversary, a bit of geography or a particular problem

We need to become much more adept at operating with agility across this grey zone. Fundamentally, we have to make sense of, exploit and manipulate data. Our challenge is twofold – the data landscape is so complex and handling the sheer volume of information (and intelligence) that could be available to us. Using software to exploit freely available information is important – which is where many of our conversations are with industry – but it is much more challenging than that. Let me try to explain why.

If you work left to right, if you will, across this spectrum between competition, confrontation and conflict. We want to be more proactive on social media, exploiting it to deliver consistent, pervasive and also targeted messages. We also need to 'operate' through social media platforms with much greater agility, countering adversarial campaigns through a range of fora, including using third parties if necessary.

Taken a step further, we may wish to generate social reaction 'on the ground'. To do all of this, we need a deeper understanding of our audiences. This will take time to build, we need well trained people, including locals, and the right tools. In short, we must become more adept, and comfortable, with acting across and dominating the cognitive domain.

Let's step up the pressure. We need to be prepared to conduct 'precision soft strike'. Sometimes this will be avowed, to deter, sometimes not. We may wish to target adversarial media campaigns, as we have in the past, or disrupt, even neutralise, military systems, such as a supply chain. These activities take potentially years to plan, so we need to think ahead, ensuring that they are nested within enduring campaigns, its to taking a strategic view

Let's go one further. We will be prepared to prosecute hard strike, at extreme range, to destroy carefully selected targets. Designing, maintaining and constantly developing a pervasive ISR architecture, across all five domains, at multiple classification levels, has to be central to this. Communicating across it, protecting it, understanding and exploiting the bulk data inherent within it, measuring the impact of strikes and then going again – all of this requires us to move well beyond a fragmented, stove-piped and poorly governed environment to a single, interactive and responsive one.

We need to create synthetic environments where we can practice. To wargame, experiment, to plug and play. We need to work out what a flatter, more dispersed, more resilient command and control architecture looks like. Fundamentally, we must develop MDI operational art. We must exploit current operations in order to do so, and ensure lessons are fed into an interactive learning domain. We must integrate this with our longer-term conceptual development through the creation of digital twins and synthetic environments.

Bringing all this together, deliberately, and keeping it up to date, and operational, lies at the heart of our approach to MDI. It's much more than buying a software service.

What technological edge are we seeking?

Fundamentally, the source of battlefield advantage will not come from platforms. If we focus, as some commentary invariably does, on the number of grey hulls the Navy has, the number of Fighter Squadrons in the RAF and the strength of the regular Army, we will simply perpetuate a traditional, industrial age force that is costly, exquisite and vulnerable to being defeated in detail.

The true source of battlefield advantage will come from our ability to sense, understand and orchestrate across domains at a tempo faster than the enemy. To create and close kill chains, as Christian Brose put it, and this means a digital force – software defined, hardware enabled. A force that harnesses pervasive sensors, resilient networks, cloud and edge computing. One that applies Machine Learning and AI to exploit data, support decision-making and enable expendable autonomous systems and swarming. It will be more about drones and missiles, than manned platforms.

The IR investments lay the foundations of this force, specifically the Digital Backbone, which Defence Digital are building with its focus on people, process and technology to build ubiquitous and resilient networks, curate, harness and exploit our data, expedite cloud computing at multiple layers of classification and pursue agile software development though the Digital Foundry. We need your help with this. In all humility. But we urgently need to go further and faster together. In three areas in particular.

First in the development of synthetic environments for the reasons I covered earlier.

Secondly in pursuing the combination of pervasive sensors and edge computing that will enable us to create a Military internet of things and realise the potential offered by autonomous systems and intelligent machines. And that in turn will allow us to field a larger, more capable and more affordable force. Here we aren’t harnessing the pace of development in the commercial sector.

The text-book sized processor on an autonomous car has 800 times more processing power than the most advanced processor on any military platform – and that is the one on the F35, nicknamed the flying super computer. The same car has more sensors than any military platform, just as many of your homes have more sensors than any military base. We can change this paradigm.

And third, in the development of Artificial Intelligence and Machine Learning. We don’t have the time here to do justice to the potential of this technology – you could devote the entirety of DSEI to it, we probably will one day, and still only scratch the surface. Sundar Pichai, the CEO of Alphabet, said recently of AI: “We are in the early stages, but I view AI as the most profound technology that mankind will ever develop and work on…even more important than fire, electricity or the internet”.

The military use cases for AI – narrow AI at this stage – are pervasive: autonomous systems, swarming, cyber defence, decision support, intelligence processing to name only 5. But two things are clear. First, threat: Our adversaries will gain a decisive advantage if we do not compete in a more concerted and urgent way in this technology. And secondly, opportunity: Investment in military AI – will be symbiotic with the growth of AI in other sectors and will be at the heart of fuelling the UK as a S&T superpower.

I want to turn to the issue of skills, because we need to be clear-eyed about what is needed. Our current workforce is brave, talented, inventive, resourceful and resilient. But it isn't yet imbued with the culture to pursue Multi-Domain Integration, nor does it have the diversity and skills needed to be competitive in the digital age. Culturally we are still largely and recognisably a tri-service organisation, and that's where many of our strengths lay. We don't provide joint education until around the 15-20-year point in someone's career, yet MDI expertise will be needed at every level including the most junior. We value Royal Marines for being amphibians: comfortable in two environments. Some of us become tri-phibians – truly joint across all three physical environments.

But we need to evolve penta-phibians, with the ability to operate seamlessly across all 5 domains. We're going to need to think radically about the career model, training and education that accelerates the pace of this evolution because if we don't adapt, we will become at best become exquisite but irrelevant, and at worst we will die. In a similar vein, to achieve the vision of S&T advantage painted in the IR we are going to need access to fundamentally different skills and talent and to place equal value and afford equal status to computer scientists, data engineers and cyber operators as we do on the traditional warrior elite. I have more need of Q, than I do 007 or M.

So we will have to address the skills gap through attracting far more diverse talent, by inward investment, because we've not got enough STEM graduates so that coding and data literacy are seen as being as much a core skill as weapon handling, by much greater use of a larger and more diverse reserve, and by enabling a much more porous and flexible flow of talent between Defence, Industry and Academia.

Relationship with Industry

Bringing this to a close, I want to offer some thoughts about our relationship with you, our industrial partners here at DSEI, but I hope my voice may also reach the start-ups and small and medium sized enterprises for whom this is not a natural stamping ground.

The predominant image of the defence sector's impact on the economy is of aircraft carriers and jet fighters. As important as these industries are, in a world in which capabilities are moving to the cloud and software and data can be as 'real' as any physical assets for a modern military, this image is dated.

And it's worth reminding ourselves that the Digital sector is growing 2.6 times faster than the wider economy and that the market for military AI is projected to grow from £3.8Bn in 2016 to £6.6Bn next year. The benefits of this are much wider than Defence – it will drive a wave of upskilling across the economy.

Rob Magowan, my deputy, is part of a panel that follows this presentation. He will explain in more detail how we need to exploit DSIS in our development of MDI. He will set out those areas where we need to be most closely integrated with industry and suggest some collaborative models that will enable us to work on problems together.

No doubt, UK Defence needs to become much more agile and forward leaning in this space; and, if I may, industry needs to take some risks too, in order to protect and promote SMEs, and by companies working alongside each other for the common good, where necessary.

Thank you for your time today. Acting together, we can mobilise our armed forces to pursue the political vision of a bold, confident and active European power with a global perspective. Armed forces that campaign dynamically, adapt to threats and seize opportunities to strengthen alliances, partnerships and secure national advantage.

Working together we will ensure Defence is more closely integrated and modernised to deliver the IR and gaining advantage in science technology data and AI. And we can upskill our Armed Forces for the digital age.