Commander of Strategic Command RUSI conference speech

Thank you, Secretary of State and let me add my own welcome to our second annual conference. Fifteen months have passed since we gathered at RUSI on Whitehall for the inaugural Strategic Command conference and it has since been a seminal period for Defence, and for Strategic Command in particular. None of us could have imagined what those 15 months had in store. COVID 19 dominated every aspect of our lives, and Defence was no exception. We're going to spend most of today focused on the future, but it would be wrong not to dwell briefly on the pandemic and call out the remarkable work that sometimes goes unsung in Strategic Command.

Defence Digital enabled secure remote working extraordinarily quickly and effectively. Defence Support was central to the procurement of PPE and rapid distribution of vital medical supplies. Defence Intelligence provided critical medical intelligence to the heart of government decision making. And our overseas bases, remote and cut off for sustained periods of time, managed the risk with extraordinary skill and discipline and supported stretched local medical infrastructure. But I want in particular to shine a light on the Defence Medical Services who have been fully mobilised and embedded on the frontline of the NHS for 14 months: consultants, doctors, nurses, combat medics, paramedics, medical support staff and carers. They have done no more or less than their NHS colleagues, but their skills – military and medical – have been vital. They shun the limelight and claim no credit or recognition, but I want to pay tribute to them, to recognise the burden they have borne, the sacrifices they have made, the suffering and grief they have witnessed and to thank them as publicly as I can. I am immensely proud of them all.

The pandemic has been a global tragedy. But from every fight we draw lessons, and the pandemic has been no different. I want to pick out three. First it has highlighted the importance of national resilience and in particular our reliance on cyberspace as a domain – the internet has been a lifeline for many during lockdown. But it has also been a conduit for disinformation – fraying the bonds of society, the seams of alliances and undermining the workings of democracy including our healthcare responses, all fuelled by digital authoritarians.

Just in the last few months cyberspace has been the vector for espionage. From Solarwinds, which was attributed to Russia; the Finnish parliament, attributed to China; the crippling of critical US national infrastructure through ransomware attacks and, chillingly – on the Irish health service in the midst of the pandemic, both attributed to Russian cyber actors. Now the UK is ranked by the Harvard Kennedy School's Belfer Centre as one of the world's three leading cyber powers. The record investment in the Integrated Review reinforces that.

I want to underscore just how critical this will be in strengthening our cyber resilience, and growing our ability to project power in cyberspace and to establish norms of responsible behaviour in cyberspace. We will never be complacent. As a key priority, I and my partner in GCHQ, Jeremy Fleming, urgently need the nation’s cyber and digital talent, part time or full time. These cyberwarriors will be as vital to our defences as an F35 pilot, a special forces operator or a submariner – and in contact with the enemy more frequently and persistently than any of them.

Secondly, the pandemic has reminded us of the advantage conferred by being at the leading edge of science and technology. Our world-leading ability to conduct gene sequencing, identifying new variants of the virus and developing and deploying effective vaccines has – literally – meant the difference between life and death for tens of thousands of us. But as well as highlighting the opportunity it also demonstrates the peril in falling behind in the race to develop and exploit emerging and disruptive information age technologies.

We are confronted by a technological tsunami of which the most consequential include bio tech, QT, micro-electronics and semi-conductors, robotics and 5G. But the most significant, the 1st among equals, the one ring to rule them all, is Artificial Intelligence. Why? Because it is a new knowledge and reasoning system, it will be both foundational and an accelerant to every other field of emerging technology. It will become a pervasive and therefore decisive technology. We’re not alone in making this assessment. In 2017, President Putin said that the nation that leads in AI will rule the world. China in particular is pursuing superiority in AI. Why does it matter to Defence? Well, as Eric Schmidt the former chairman of Google testified to congress recently, defending against AI capable adversaries without employing AI is an invitation to disaster.

AI will compress decision timeframes from minutes to seconds, expand the scale of attacks, and demand responses that will tax the limits of human cognition. Human operators will not be able to defend against AI-enabled cyber or disinformation attacks, drone swarms or missile attacks without the assistance of AI enabled machines. Even the best human operator cannot defend against multiple machines making thousands of manoeuvres per second at hypersonic speeds and orchestrated by AI across domains. Humans cannot be everywhere at once, but software can – it can augment human capability and can have enormous benefits. It can defend society and democracy, it can enable operational advantage, and remove humans from harm’s way.

We are not starting from a low base – in 2019 the UK was ranked 3rd after the US and China in the global AI index. But that ranking conceals a huge gap in a winner takes all competition where first mover advantage is everything. The IR and the Defence Command Paper both cite AI as a strategic priority and a thousand narrow AI flowers are blooming across Defence – but we have not mobilised this at the pace and scale needed.

We are putting the fundamentals in place beginning with an AI strategy, to be published this summer, and it will be guided by 3 main principles: (1) we will adopt and exploit AI for Defence at scale. (2) we will catalyse and strengthen the UK Defence and Security ecosystem for global leadership and (3) we will shape the global development of AI to support security, stability and democratic values. For Strategic Command, this begins with the establishment of a Defence AI centre this year as part of a wider digital ecosystem across Defence that we call The Foundry. And forgive me if I unashamedly get a bit techno techno, but the technology and the terms matter.

It will begin by integrating existing digital technologies now – for example using machine learning and automation to support Intelligence analysis. It will be enabled by improving our digital infrastructure – the digital backbone – with a data strategy that enables data curation, data sharing and data exploitation, cloud services at Secret and Above Secret, and a common network architecture. It will lead to investing in more S&T in partnership with DSTL and to experimentation to ensure responsible development of AI enabled and autonomous systems.

And above all it must mean building a talent pipeline with a Defence Digital Service and Digital Academy, with career fields in software development and data science. A career management system will nurture these rare talents across Defence – as well as growing a base of junior leaders in digital skills and computational thinking. The third lesson from the pandemic relates to this last point. As a society – whether in government, corporations or as individuals – we have adapted to the enforced changes brought about by lockdown at a pace that challenges all our previously conservative assumptions about how agile our organisations can be.

It shows that bold and radical change can be adopted and absorbed in our stride. Decisions in government that would normally take months or years were decided and implemented in hours. This rapid decision-making is only routinely seen during times of great crisis such as war, but this culture and mentality must become habit. We must be daring and entrepreneurial because the threat is moving towards us and the technological advantage away from us.

I want to turn now to the theme of this conference: Integration. As the Defence Secretary pointed out, two of the three seminal Defence related documents published this year contain Integration in the title. And last month in Honolulu, US Secretary of Defence Lloyd Austin described a concept of Integrated Deterrence echoing three of the principle conclusions of the Integrated Operating Concept and the Defence Command Paper.

First, as CDS has said, if you are up against rivals who seek to win without fighting, you cannot afford to be passive. In other words you have to compete below the threshold of war to deter war. And to prevent your adversaries from achieving their objectives in fait accompli strategies like those in Crimea and the South China Sea. Second, and hence my earlier comments on AI, our ability to innovate and develop a competitive edge in emerging disruptive technologies will be fundamental – which is why sustaining strategic advantage through science and technology is integral to the strategic objectives in the IR. And third is that our ability to deter above and below the threshold of conflict will rise or fall on our ability to achieve Integration: of the levers of national power, across the five operational domains, and alongside allies.

But the key question we should be asking ourselves is who and what are we seeking to deter? Today’s first panel session will explore this, but let me offer a trail. In his confirmation hearing to the US Congress in 1993, CIA Director James Woolsey characterised the threat as being composed of Dragons and Snakes. Both are still with us, only the Dragons are more powerful and malign and the Snakes are more prolific and diverse. Sometimes they act in concert. Some snakes cannot be deterred – they have to be suppressed or disrupted. This is why we will maintain cutting edge CT capabilities in our Special Operations Forces. Other snakes – like the Wagner Group for example or malicious cyber actors are used as proxies by the Dragons.

The largest Dragons in this metaphor are China and Russia. Russia is the acute and most menacing threat – the Defence Secretary described it as the number one threat to the UK just this Sunday. China is very different – a global power, a strategic rival and in some areas (we hope) a strategic partner. But our ability to manage this strategic rivalry requires the same tools of deterrence, modulated and applied to these Dragons in different ways.

Foremost among these is our ability to orchestrate our levers of national power, in a dynamic and persistent fashion, to contest the strategies both rivals are using against us. These strategies have been given a variety of labels: Hybrid Warfare, Liminal warfare, Grey Zone, Sub-threshold – the list is extensive, but they all describe the same essence. George Kennan captured this best in his telegram from Moscow in 1948. He used the term Political Warfare which he defined as: “The logical application of Clausewitz’s doctrine in times of peace. In broadest definition, political warfare is the employment of all the means at a nation’s command, short of war, to achieve its national objectives, to further its influence and authority and to weaken those of its adversaries. Such operations are both overt and covert.” Kennan captured the weakness in our own approach which persists today. He wrote “…we have been handicapped however by a popular attachment to the concept of a basic difference between peace and war, by a tendency to view war as a sort of sporting contest outside of all political context.”

It’s not as if we don’t recognise this. The comprehensive approach and fusion doctrine are both attempts better to integrate the levers of power. And it’s not as if we haven’t historically had the strategic culture. We have levers of national power that in each field rank among the most influential and extensive of any in the world: diplomatic, economic, legal, development, intelligence and security and defence. But our historically strong strategic culture has atrophied since the end of the cold war – it needs to be rekindled.

In some areas we do this well: our larger embassies overseas can be exemplars of an integrated approach, responding dynamically to threats and opportunities and giving us significant influence and purchase. And the National Cyber Force is in many ways the perfect expression of the power of combining the different capabilities and operational cultures of government arms: the marriage of GCHQ, MOD, SIS and DSTL working to strategic priorities from the NSC is proving very potent.

But it’s also fair to say that we have further to go in adapting the strategic machinery to the persistent and dynamic campaigning across Whitehall that the IR demands. We know it responds well in a crisis as it did following the poisoning of Sergey Skripal on British soil confirmed that, but it has yet to demonstrate it can campaign persistently and dynamically. The second facet of Integrated Deterrence is our ability to combine effects across all domains and all levels of warfare to create, find and exploit unprotected vulnerabilities and pose multiple dilemmas. And if needed to have the ability to impose cost in another domain entirely to the one an adversary is contesting.

This is Multi-Domain Integration – the precise role Strategic Command was established to lead and enable. Where each of the Services exist to conduct operations within their physical domains, we exist to conduct operations across and beyond them. That's why the Command holds the capabilities that allow Defence to sense, understand, orchestrate and enable effects across domains. There is no ready template for MDI and I have no easy answers, hence why we have drawn you together today to draw on your collective expertise and insight as we explore this further in the second panel. But we do know that our ability to develop the necessary expertise will hinge on a number of things and I want to touch on these.

First of all we will need to experiment and adapt as we harness new technology and new techniques. The hardware won't change between now and 2025 but the software will and our ability to exploit data with AI, establish a single information environment and extend our reach in cyberspace will allow us to push the boundaries of MDI with innovation and agility. We have established a formal programme of experimentation under AM Windy Gale, our new DG JFD, but the most valuable lessons will come from operations and here we have an inherent advantage with our special forces and PJHQ placed in the command. They are our vanguard and are already practising MDI, combining effects through cyberspace and space, with platforms and manoeuvre by air, land and sea to achieve cognitive and physical effects, overt and covert, in partnership with other government departments. It is happening on CSG 21 orchestrated by PJHQ and it is happening on special operations.

Secondly we need to change how we develop and field capability. The real source of military advantage lies less in platforms, it lies in our ability to sense, understand and orchestrate – in the kill chain as Christian Brose colourfully described it in his book of the same name: the sensor networks, the data, the PED and the effectors: kinetic or non-kinetic. But our requirements process is geared towards the acquisition of platforms, not to the networks that enable rapid decision-making across all levers of power. It is slow and We have a tendency to be impervious to disruption, lagging behind. We need to incentivise industrial partners by refreshing capabilities constantly, develop strategic partnerships including with SMEs and develop a two-speed acquisition system that is fit for software DevSecOps, MVPs and with greater appetite for risk. The PUS is determined to unlock this and you can press him on it in the final session.

And third, MDI will require a cultural shift across Defence. We are still largely and recognisably a tri service organisation. Coordination across the services is still more of an afterthought than a reflex. 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. Our approach to managing rare talent and skills that are needed across domains is still stove-piped, though our approach to managing cyber talent offers a model for how to change this.

Promotion and reward occur based primarily on how well you perform in your service, with service in joint (soon Integrated) posts of less import. An occasional paper published by RUSI and authored by Trevor Taylor and Andrew Curtis reminded us that as far back as 1964 Generals Pug Ismay and Ian Roberts advocated for greater integration in the MOD and between the Services than we see now. It’s hard to avoid the conclusion that the requirement to develop expertise in MDI provides even more of an imperative now than it did then and I really welcome the fundamental reforms to our personnel strategy that are being pursued.

I haven’t spoken about Integration with allies and partners. I’ve chosen not to partly because we have such excellent representation from the US and our colleagues in NATO on the panels, but mainly because it seems self-evident to me that the true source of our deterrent strength comes from the alliance and our close bilateral relationships with partner nations. That integration and the values we share and the respect for the Rules Based International System are what distinguish us from the Dragons and the Snakes.

At our inaugural conference last year I described the priorities I had for the IR: Cyber, Intelligence and Understanding, Special Operations and Multi-domain Integration and how they come together in Strategic Command to strengthen our deterrence and our competitive edge. These now lie at the heart of the Integrated Review outcome. We’ve been given the resources and the responsibility to lead the transformation of Defence for the Information age; we’ve now got to deliver.