<u>Speech: Chief of the Defence Staff at</u> <u>Air Power Conference – 12 Jul 18</u>

Great privilege to have the chance to be with you in this the RAF's 100th Year and my first conference as Chief of the Defence Staff – I'm 4 weeks in and rapidly building my tri-Service knowledge – and it was very helpful for me on Tuesday in terms of understanding some aircraft recognition and that sensational flypast that we saw.

And it's been quite a week really — the first death of a British citizen on British soil from nerve agent poisoning, dynamic politics at home and internationally, a pivotal NATO summit — and sadly football's not coming home just yet.

These are demanding times that seem to become more demanding every year – and the resources don't become any easier. Meanwhile, the strategic context is complex and dynamic, and the threats that were identified in our 2015 Strategic Defence and Security Review have diversified, proliferated and intensified rather more rapidly than we anticipated. The upshot is a global playing field characterised by constant competition and confrontation, which has increasingly assertive and aggressive states, utilising techniques below the threshold of what we would once have called conventional war, all of which is overlaid by the threat of terrorism from violent extremist organisations – hence we are presented with challenges on multiple fronts.

This is felt in every domain, but it is particularly marked in the Air Domain with six Air Expeditionary Wings deployed, involving some 16 missions in some 28 different countries across five continents. And these missions are also remarkably varied, from sustaining a now four-year task of countering violent extremism in the Middle East, requiring great precision and integration; and as we saw in April, the need to take markedly greater risk in response to the Syrian regime's use of chemical weapons; and in Europe the 24/7 task of protecting our air space, requiring a high degree of readiness and responsiveness, as well as contributing forces to NATO Air Policing.

Resolving this challenge requires us to mobilize to match the threats of today, while in tandem 'wing-walking', which I will come back to, to a modernized future with a horizon of say 2030, enabled, in Defence's case, by a multi-year transformation programme that places Defence on a more sustainable footing, and will enable us to run the 'business' better – not least by properly defining Jointery as the integration of the domains to achieve an output that adds up to far more than the sum of the parts.

This level of commitment inevitably begs questions about prioritisation, about long-term sustainability and about the importance of striking the right balance between 'fight tonight' and 'fight tomorrow'. Particularly as it's rarely possible nowadays to retain forces as dedicated contingent capability - we are now far more likely to recommit forces that are already deployed. The problem though is compounded by the nature of the threat. But there are also some difficult questions being posed about the evolving character of warfare in which our state-based competitors have become masters at exploiting the seams between peace and war — what constitutes a weapon in this grey area no longer has to go 'bang' — energy, cash, corrupt business practices, cyber attacks, assassination, fake news, propaganda — and good old-fashioned military intimidation — are all examples of the weapons used to gain advantage in this era of 'constant competition'; and the rules-based international architecture that has assured our stability and prosperity since 1945 is, I would suggest, therefore threatened.

To be clear, we face a strategic challenge that requires a strategic response – we will fail if we see this as a series of crises.

The deduction we should draw from this — is that there is no longer two clear distinct states of 'peace' and 'war' — we now have several forms — indeed the character of war and peace is different for each of the contexts in which these 'weapon systems' are applied. And the risk we run in not defining this clearly, and acting accordingly, is that rather like a chronic contagious disease, it will creep up on us, and our ability to act will be markedly constrained — and we'll be the losers of this competition.

While not alone in employing these techniques, the arch exponent of this is Russia — probably the most complex and capable state-based threat to our way of life since the end of the Cold War — and recapping on Russia's approach provides a useful lens through which to view this type of challenge. In so doing we should recognise that they have no single model for conflict. They use a multi model approach — utilising conventional, unconventional and nuclear domains — a hybrid version that might involve little green men, big green tanks and huge green missiles.

Their thinking is very flexible – their General Staff is able to change, evolve, learn lessons with agility – for example they know that demography is not on their side – so they are developing capability that needs fewer men. They have developed coherent concepts of equipment and training that are focused on our vulnerabilities – for example, our dependency on technology, space and digital communications; our lack of massed fires; and so on and so forth.

They apply a ruthless focus on defeating their opponents – not seizing ground for the sake of it – but making sure that our vital ground and our long assumed freedom to project power as we see fit is denied to us, and this has major implications for the Air domain – I shall return to their missile capability in a moment. Since 2016 we have seen a marked shift to cyber, subversion and coercion as well as sophisticated use of smear campaigns and fake news – for example interference in the US democratic process and the attempted coup in Montenegro.

Chris Donnelly at the Institute for Statecraft suggests that they are creating new strategic conditions — their current influence and disinformation campaign is a form of 'system' warfare that seeks to delegitimise the political and social system on which our military strength is based — and undermine our centre of gravity which they rightly assess is our political cohesion.

China is also developing its military capabilities, reported recently in the open press that it is expanding its expeditionary capability to, I quote, "manage a crisis, contain a conflict, win a war" – developments include the testing of stealth and anti-stealth technology, and the application of information technology in all aspects of military operations is becoming ever more prominent.

Now I'm not in any way suggesting that Russia, or any other of these statebased threats wants to go to war in the traditional definition of the term – rather it is the risk of escalation leading to miscalculation that is the greatest threat, as we don't have the same level of understanding that we had in the Cold War, and the tried and tested systems and diplomatic instruments are not what they were – confidence building measures, arms reduction negotiations, public monitoring and inspection of each others' military activity etc. But that said we should be wary of bigging them up too much – remember what we found at the end of the Cold War.

This then is the context in which we are conducting the Modernizing Defence Programme.

There are two major themes to this: the compelling need to mobilize rapidly to meet the threats I have described, while in parallel modernizing for what the future may bring, with the latter being enabled by a multi-year transformation programme that I referred to earlier, that will lead to the 'business' of Defence being managed very differently in ten years-time.

Starting with mobilization, this envisages much improved readiness — recognising this is about speed of recognition, speed of decision making and speed of assembly. It's about resilience and lethality — and the important thing, it's about demonstrating that we are prepared to fight the war we might have to fight, because that is the best way of deterring that war from happening.

The NATO Readiness Initiative seeks to do just this, linked to an exercise rhythm that increases the base load of activity so that the foundation of readiness is much higher. But it' got to become much more integrated and much more joint by design. At the moment the domains work in stovepipes, we must pull them more closely together. It's also about forward basing, stockpiles, much improved resilience and getting serious about rapid deployability. It's about giving real meaning to the SDSR statement that we would be 'international by design'. And it is tremendous to see in this auditorium today the extent to which our allies and partners are with us. We have a number of bilateral and multilateral relationships as Armed Forces – for example the recent signing of the UK Joint Expeditionary Force Comprehensive Memorandum of Understanding is a significant step in working together to develop genuine interoperability which will be a force multiplier.

As a lead framework nation, the UK must enable interoperability by providing technical systems that are extrovert by nature so that our partners have the sockets they can plug into for shared situational awareness, for a common

operating picture, and for the coordination of digital joint fires. But deep interoperability is built on long-term relationships, developed by exercising together, testing doctrine and tactics together, and building mutual trust and understanding.

International by design is also about delivering more capability in partnership with Allies. We see that in the Land domain with general support engineering with the Bundeswehr in Germany, and the international collaboration with the US Navy and Norway on maritime patrol aircraft – partnerships of this kind deliver economies of scale and generate a higher operational tempo than we could achieve on our own.

And as we mobilize we must think creatively — it is not about matching an adversary's strength with strength, but thinking about how to out-manoeuvre him by threatening his vulnerabilities, by holding what he cares about at risk and by thinking laterally and asymmetrically. This will likely involve prioritizing some new capabilities — such as those that will allow us to manoeuvre in the information domain to create information advantage, enhancing our range of capabilities in cyber, space, electronic warfare and information operations — and to build our own resilience and protect our critical national infrastructure and other vulnerabilities — such as our networks, such as CBRN, and survivability — all working within a cross-Government framework to utilise all of the levers of national power.

And we must build our strategic depth — seizing the opportunity that the newly amended Data Protection Act allows, for us to retain effective contact with those ex-Regulars who are statutorily liable for mobilization. And in due course, starting next year, conduct routine mobilization exercises for the Reserve and the Regular Reserve, with Ministerial engagement, as we used to in days gone by.

Rarely are there any purely military solutions, so we must maximize Defence's contribution within the idea of 'Global Britain' and in a cross-Whitehall context for best strategic effect. This means thinking of ways to generate more points of presence, making more productive use of those capabilities that are not designed for the higher levels of risk associated with war-fighting scenario. Holding these at a lower 'war-fighting' readiness and utilising them on tasks to generate understanding and build relationships, to enable soft power to have effect, building institutions, capacity and resilience in nations that matter to us — as well as countering the agendas of our competitor states ... not least in Africa — which will be a source of significant instability by 2030 if nothing is done.

In tandem with mobilizing — we must get the right balance between 'fight tonight' and 'fight tomorrow' — hence the importance of placing the right emphasis on modernization.

As Richard Susskind advised in his book 'The Future of the Professions: How Technology will Transform the work of Human Experts' – the best way to predict the future is to invent it. The Chief Scientific Adviser, who I think you will hear from later this morning, identified what he calls 'big bets.' It is reasonable to assume that information technology — sensors, computing, communications, cyber, machine learning, artificial intelligence and autonomy and so on — will continue to evolve apace and that information manoeuvre, which enables information advantage is already a domain in its own right. This will clearly be at the heart of modernisation — and it is absolutely vital that we establish the information architecture to provide the open systems framework for all of our capability.

In the underwater battle space, new information technologies will revolutionise detection, tracking and understanding of potential threats – using advanced machine learning methods for acoustic signal processing and increasing the use of autonomous systems for mine control measures and fleet protection.

In the land domain, resilient communication networks combined with pervasive, organic and real-time intelligence surveillance and reconnaissance will give unprecedented understanding and situational awareness. Combining this with modern effects – directed energy, electromagnetic attack, delivery of tactical offensive cyber – will substantially contribute to war-fighting mass and deterrent effect.

Future air power will also be driven by information advantage and its application in enabling understanding, protection and effect. Situational awareness must increasingly be delivered through fusion of data from multiple sensors on multiple platforms and organic distribution to all of the force – with implications for spectrum management, communication, algorithmic warfare and autonomy.

At the same time modern concepts of multi-functional antennas mean that platforms must simultaneously become sensors, communication networks, directed-energy attack vectors and deliverers of cyber effect. The needs of air survivability and our ability to project power by countering anti-areaaccess denial will drive a further step change in the use of information and physical technology — autonomy, shared information and the mixed role of air platforms and future complex weapon systems.

The joint force though must also expand to include all of government in enabling the nation to deter and defeat the full spectrum of threats and actors. The role of information technology here is profound – from bringing together understanding and situational awareness through advanced data fusion, through the use of machine learning and artificial intelligence to recommend courses and consequences of actions, to the delivery of a range of non-traditional deterrent effects.

We also know that automation and AI will change the make up of the future force, with it being increasingly made up of different types of people on different types of engagements, shared across similar sectors in the UK, thus ensuring that we can access the skills and talent we need to fight and win in the future. The force structure will need to be as adaptable as possible, whilst maintaining the core of war fighting professionalism.

None of this will surprise any of you in this room, we've heard this sort of

thing before — and you will recognise that the challenge is how we actually make it happen. And it must be different this time — it must be led from the top and it must be properly resourced. Above all we have to establish a culture of innovation — if you like, an open architecture and a Defence portfolio — in which we unlock the ingenuity and talent of every level in Defence. This means creating the headroom for experimentation, providing a laboratory in which we can test ideas and 'wing walk' our way towards a modernized future. This audience will understand the metaphor — moving on the wings of an airframe during flight — but keeping one foot on the airframe while you do it. It requires an appetite for risk, and a preparedness to accept some failure.

There are good examples of innovation in all the domains – particularly in the RAF's Rapid Capabilities Office – 'Team Tempest' – which is achieving much with the BriteCloud expendable active decoy and the improvements to end-to-end manufacture of advanced flares. We now need to take this I would suggest to a new level.

Not least because experimenting in this way would enable a very different relationship with industry – a shared approach to risk and opportunity – with innovation at the heart of procurement. It would encourage external investment, venture capital and a culture that contracted for through life outcomes, rather than setting tightly specified requirements that stifle development.

This is a feature of Philip Dunne's report, that was published this week, in which he talks of modernizing our approach to acquisition, increasing our agility and pace, and adopting a culture more focused on finding the right procurement solutions, and less on defining and avoiding obstacles at the outset. This requires us to develop better understanding of how defence requirements and the market interact and shape each other.

Despite the changing character of warfare, the nature of war does not change – it remains a human endeavor, and there will inevitably be some Industrial Age capabilities in our Armed Forces come 2030. So as we mobilize to face the threats of today, and place ever greater emphasis on modernizing – we should remember the wise advice of our most eminent military historian Sir Michael Howard when he observed: "the trick is not to perfectly predict the future, but to be not too far wrong when war breaks out, so that one is well prepared to adapt at speed".

And we must never forget that war is about fighting — so the context for all our effort must be about preparing to fight the war we might have to fight because as I said earlier, in so doing we will deter that war from ever happening. And this was at the forefront of Lord Trenchard's vision 100 years ago. As you thing about the Next Generation Air Force I'm going to present you with a deadly serious — and practical task. You have just heard me say, as I have said before, that we face a series of very grave challenges to adapt — so that we can cope with the threats that the future, both near and far term, may throw at our country with little warning.

We will not defeat these new threats by rebuilding our old Defence system,

buying a few more pieces of equipment, filling some gaps in our recruiting. We need to embrace the radical changes of the modern world and meet these challenges with new, creative thinking; by taking risks; by finding new ways to expand our Forces effectively in time of urgent need; by adapting tools we have to new, unforeseen tasks; by defeating any enemy asymmetrically – not attritionally.

The task I am setting all of you, therefore is not to design a new force structure; not to invent new weapons; not to create a new concept of Air Power. No – it is to create, invent, design, introduce, at every level of command, new ways of thinking, new forms of leadership and management that will enable us to embrace new ideas, to integrate and exploit new technologies, transforming our current system into something which is permanently innovative, adaptable, responsive and proactive.

I do not want to hear new ready-made answers; I need to hear new ways of finding answers for future, unforeseeable threats, and new ways for us to keep on finding answers. This is much more difficult and painful, I know, because it needs us to change the way we think, act, acquire equipment, exercise command and lead. We are at, I think, a paradigm shift in the character of conflict: we need to change the way we do things fundamentally.

This is the essence of modernizing Defence. Fail to change now and our adversaries, slowly but surely, will overcome us, they will erode and finally overturn the democratic, rules based, stable system under which we have all lived comfortably for nigh on three generations. I fear our 70-year long holiday from history may well be over — and we all have a job to do to fix it.