Defence Information Superiority Conference 2010

'Creating and Exploiting Decision Advantage'

Air Chief Marshal Sir Stephen Dalton, KCB ADC BSc FRAeS CCMI RAF
Chief of the Air Staff

Coming, as it does, in the midst of the SDSR, a Conference on Information Superiority is timely. Over these two days we are examining one of the key issues to be addressed as part of the SDSR – an issue of central importance to the conduct and outcome not only of current operations in Afghanistan, but of all operations we are likely to undertake in the future. Indeed Information Superiority is at the very heart of the Royal Air Force's Combat ISTAR capability. So let me offer you some thoughts on why!. My proposition here is quite simple – that Information Superiority is key to the achievement of that critical asymmetric advantage over opponents, and hence campaign success, and that's across the whole spectrum of operations.

So what is the broad direction of travel that UK Defence must follow if we are to achieve decision advantage in the future? And, whilst I am in no position to pre-empt the SDSR outcome, it will perhaps come as no surprise that I also want to offer some views on the central role I believe the RAF will have in shaping and delivering such a key capability.

When discussing Information Superiority in the Defence context, I believe the 'End' we are trying to achieve is 'Decision Advantage'. By decision advantage I mean the ability of our decision makers at all levels, to use information, intelligence and situational awareness to make effective decisions more rapidly than our adversary. Such advantage allows a dramatic increase in the pace, coherence, and effectiveness of operations. It applies across the fullest spectrum of conflict – including influence operations as well as more kinetic effects – which will be undertaken under the direct scrutiny of the media, where failure to act effectively and rapidly can deliver a sharp reverse in the information battle and wider campaign. And I stress that the need for decision advantage exists at all command levels from the political and strategic down to the tactical. Indeed many of the distinctions we have traditionally made between tactical, operational and strategic information & intelligence are becoming obsolete – for example, imagery intelligence that was previously the preserve of operational

commanders and their staffs is now routinely commissioned and consumed by decision-makers at the lowest tactical levels, often in real or near real-time. Full-motion Video from Reaper Remotely-piloted Air Systems and high-quality still imagery from Raptor pod equipped Tornadoes are good examples of this on current operations.

In short, if we are to take informed, decisive action – we must first sense what is going on, understand and share that information, decide what must be done and then act. And we must do all this quickly if we are to gain a decision edge or competitive advantage over the opposition. Those of you from industry will recognise clear parallels here with companies operating in a fast changing, competitive market-place, or managing unforeseen events that can quickly unfold in a way which threatens the business.

If Decision Advantage is the 'End' we seek, then the 'Means' of achieving it is the attainment of ***information superiority.***

When considering Information Superiority, I would highlight three key themes:

Firstly, Information Superiority is not a 'free good' – we do not possess it as a matter of course. Like air superiority, it must be **won,** whether in the business world or the battle-space, through offensive and defensive operations. This could include efforts to disrupt or exploit enemy systems and networks, while defending our own information, as part of a dynamic competition between hostile and friendly information capabilities.

These activities must be conducted across physical and cyber domains, if information superiority is to be established; and must add to our knowledge of our enemy and their circumstances - ideally, before they know about them themselves! Our previous, almost exclusive, intelligence gathering pre-occupation with enemy forces operating in the physical domain will no longer suffice. Moreover, information, when gained, must then be fused, processed and disseminated to decision-makers quickly enough to support their decision making.

Of course, accurate and timely information has always been critical to the military, but its importance is increasing as all of us become more networked. Our current enemies are already using effective information operations and propaganda (via the cyber-net) to influence target audiences, including our own public opinion, to constrain our activities. In the future our adversaries will increasingly use cyber attack against our networked systems; indeed our national computer systems are under constant and intensifying attacks today. In short, we must expect our adversaries to use every possible information means at their disposal to try to deny our freedom to conduct operations as we would wish.

The second theme I would highlight is quite simply that conflict is becoming more complex. Few analysts have disputed the conclusions of the MOD's *Future Character of Conflict* study. This predicts that future warfare may be inter-state or sub-state, 'conventional' or 'hybrid'. But whatever its nature, in character it is likely to be *congested*, with forces drawn into densely populated areas; *cluttered*, where targets will be difficult to distinguish; *contested*, where access will be disputed and we'll have to fight for the freedom to manoeuvre; but it will also be *connected*, through the media and cyber-space, and where critical nodes of communication and virtual networks will provide essential capabilities, but will also represent critical vulnerabilities.

This means it will be more and more difficult to understand what's happening, and we'll have to fight for access to a battle-space where small-signature targets are difficult to identify against the background noise. Opportunities for decisive action will be fleeting and increasingly constrained by our ability to optimise such opportunities, as well as legal, political and ROE considerations, and very quickly subjected to rapid public scrutiny. So our missions are likely to be more complex in virtually every way, and this complexity will place a premium on **understanding and situational awareness.** But we should remember that our adversaries will also face greater ambiguity and uncertainty, and so we must maximise our comparative advantages, of which more later, to ensure we win the information battle – increasingly the 'vital ground' of any conflict.

The third point I would like to highlight is that the need to achieve decision advantage in complex operating environments means the need for integrated and synchronized action has never been greater. If we are to exercise genuine 'smart power' across the full range of influence and kinetic operations then our understanding of our mission and our operating environment must be a shared understanding - and that means Joint, cross-government and Coalition. Our understanding and hence our information analysis must therefore be collaborative. This is easy to say but difficult to achieve. But I think it is fair to say that part of the challenge is that we have not yet fully embraced the 'need to share' ethos within out information management culture. What we must now develop is the assured, dynamic **sharing** of intelligence, information and situational awareness if we are to achieve the **understanding** that will enable consistent decision advantage. If we do not achieve this, we will never gain the true benefit of the integrated use of hard and soft power – which is increasingly likely to mean campaign failure. But we are making steps in the right direction, and the Afghan Mission Network and associated shared intelligence databases are a very positive example of how previously held national sensitivities are slowly giving way to a more collegiate sharing of information across the ISAF coalition. We still have some way to go, but our direction of travel towards ever more collaborative intelligence working environments is clear. This sharing culture will be increasingly important as we move into a more resource constrained future where we can't do everything by ourselves, on a sovereign basis. There will be more mutual dependencies, as we rely on partners and allies to task-share on expeditionary operations. For example, in Afghanistan, the theatre-wide Air ISTAR capabilities provided by the RAF mean that the UK is seen to be contributing to ISAF on a broad regional basis, beyond the sometimes narrow confines of Helmand Province. This type of information pooling will increasingly become the norm.

So, returning to my 'ends, ways and means' - if actively achieving Information Superiority in a complex and increasingly collaborative environment is the 'Way' we impose our Decision Advantage on our enemies, then what are the best 'Means' of achieving that Information Superiority?

In answering this question, we must first accept that the way we conduct our business on the frontline has changed forever – we now work in very information rich environment and sophisticated information management and exploitation is essential to campaign success. We have come a long way very quickly. Our ability to collect, process and disseminate large quantities of information across our expanded networks has made enormous strides in recent years. The effect has been transformational, and, as I have already said, that rate of change is likely to increase. Defence must therefore keep pace with and shape that change. There is no going back – the information genie is out of the bottle, and our frontline servicemen and women will expect **at least** the same level of information support in future operations as they enjoy in Afghanistan; ideally, they would seek more. We must therefore assume a continuing and insatiable demand for more and better relevant information and intelligence – and not just data!

The second point I would make is that while there is much to learn from current operations, we must be careful to learn the correct lessons. Above all, we must resist the temptation to think that the future will inevitably mirror our Helmand experience. Because we simply do not know what the **specifics** of future operations will be. Even a cursory glance at Western military experience in the first decade of the 21st century, way after the end of the Cold War, reveals the uncomfortable truth that the next conflict rarely looks like the last!

In recent operations we have benefitted from operating environments where threats to our Information Superiority have been limited – for example, we have been relatively free to operate both piloted and remotely piloted air ISTAR systems in both Iraq and Afghanistan. However, this might not be the case in future operations, where in-country infrastructure may be denied us, and where the air environment may be vigorously contested. Getting 'boots on the ground' may be far more difficult than it has proved of late.

How then do we ensure the degree of assured information access required for campaign success in such contested circumstances? Well, as I noted earlier, we are going to have to win that access! Because, be in no doubt, it will be crucial to campaign success and so will be a key challenge for UK Defence, and one we must overcome.

It is my contention that **assured information access** will only be achieved by a combination of air, space and cyber capabilities operating as part of a coordinated campaign to achieve Information Superiority. Together they provide a unique perspective on the battlespace and a degree of access, persistence, wide-area-coverage and flexibility that other ISTAR capabilities, while crucial, do not. Importantly, they do so with limited political liability and commitment on the ground – likely to be a key consideration in any future intervention calculus.

In addition, dominance of the third dimension and cyber- space will allow us to optimize our exploitation of the fourth dimension, creating the tempo essential to the attainment of Decision Advantage. Fully networked command of the Air, space and cyber-space will therefore be central to future operational success. It follows that the ability to conduct Combat-ISTAR across the air, space and cyber domains must therefore become a core competency of UK Defence.

But before describing how I am re-focusing the RAF on the Combat-ISTAR mission, there are a number of implications from my analysis so far that warrant some expansion:

The first is, I believe, the enduring importance of Control of the Air, to guarantee access to contested theatres of operation and provide the freedom of manoeuvre when we get there. It is hard-won lesson that is all too easily forgotten, because we have become accustomed to considering control of the air as a given – it is not. Even if our opponents lack their own aircraft, they'll still contest control of the air, because they recognise its importance. They may use sophisticated air defence systems, like the Serbs did in the nineties and the Iraqis in 2003; or small arms and ground fire, like the Taliban use today.

And while air power will continue to provide assured, precise and proportionate firepower, or access to air lift and mobility, **it is the increasingly the unique insight and information provided by air platforms that set them apart.** They provide an unmatched vantage point above the battle-space for gathering information, coupled with the ability to act on this intelligence quickly, if not immediately. We surrender that vital

ground at our peril – control of the air is a necessary pre-condition for victory in the information battle.

Secondly - our **information dependency** on space is growing, and is essential to our operational effectiveness. We must therefore preserve our ability to utilize this asymmetric advantage. If you dispute the importance of space, just consider what a day without space capabilities would look like: both for our armed forces on operations, but more broadly, for the security of the whole nation. Our military systems – including secure communications and targeting - all rely on the precision navigation and timing function provided by space, as do all nine elements of our critical national infrastructure. It's an interesting thought that you can't even withdraw cash from an ATM without the time signal from GPS.

Of course, the UK largely relies on alliances and partnerships for access to space, leveraged through influence and specialist knowledge. The RAF has forged important relationships with key allies and has developed the British Military Space Operations Coordination Centre to enable all three services to understand and exploit space power more effectively. Equally, it is the RAF which provides the core of the management of the MOD's SKYNET satellite constellation enabling strategic comms across the globe. However, the extent to which the UK relies almost entirely on third party capabilities is a potential cause for concern. Arguably, we should cast the net more widely in looking for partners, and also monitor the technological developments that may offer affordable space capabilities; advances in miniaturization have already enabled UK companies to develop affordable 'small satellites' as an capability option. What is certain is that space is becoming a contested domain, and we must develop a concept of operations that acknowledges this. The extent to which the UK ultimately invests in space capabilities depends on our understanding of the requirements and affordability of potential solutions; within the defence sector, the necessary expertise to do this lies with the RAF's space specialists. Whatever analysis emerges from the SDSR, it is clear that we cannot ignore this vital part of the battlespace and its potential to give us that all important comparative advantage.

Cyber-space, as Graham Wright no doubt argued this afternoon, is also a contested environment and one in which we must prevail if we are to retain information advantage over any opponent. However, unlike air and space power, the barriers to entry are low, and we must therefore expect our adversaries, whether state or non-state, to seek asymmetric advantage over us by attacking our networks and information systems. We had a glimpse of the evolving cyber battlespace in the conflict in Gaza in early-2009, where operations on the ground were paralleled by operations in cyber-space and an info ops campaign that was fought across the internet. The Israeli Air Force downloaded sensor imagery onto 'youtube'. 'Tweets' warned of rocket attacks and the 'help-us-win.com' blog was used to mobilise public support. The exponential growth in the availability of information means that we must understand how to deliver and protect our national interests in the cyber domain, and although this is clearly a cross-government issue, Defence has a legitimate interest in the development of offensive and defensive cyber capabilities. This requires a cadre of people who can understand and manage the modern networked environment, and are comfortable with the concept of information as a capability in its own right.

Finally, it follows from what I have said that we need a strategy to put the air, space and cyber components of Combat ISTAR at the heart of our Information Superiority activities**.** Now I wouldn't wish to second-guess what such a strategy might look like post-SDSR, but with its need in mind, I have already begun a conceptual change of direction in my own Service, switching the RAF's emphasis from precision attack – which we've successfully honed into a highly effective capability over the last couple of decades - to focus more acutely on exploiting information for precise stiletto targeting, in both kinetic and non-kinetic ways.

This multi-role based capability offers maximum agility and underpins the intelligence-led operations that will take centre-stage in the complex and ambiguous battle-space of the future. Adopting a system-of-systems approach, it blends together a range of multi-intelligence ISTAR capabilities, including high resolution IMINT, tactical reconnaissance and SIGINT, with a range of tuneable kinetic effects, from 'shows of presence' through

to swift and assured precision attack. It therefore combines decision advantage with the capacity for precise and timely decisive action.

Much of the RAF's contribution to future operations will therefore be based on a flexible and adaptable capability-mix of multi-role Combat-ISTAR assets. These will be both piloted and remotely piloted, and will operate within a robust, joint C4ISTAR web, drawing on information derived from other, more specialist ISTAR platforms, satellite sensors and even non-specialist assets, such as transport aircraft and helicopters. This system will also form the basis of our ability to exploit – and protect – our capabilities in the emerging environments of space and cyber-space. In this way, we'll continue to deliver three of the four essential air power capabilities required by the Joint Force: control of the air; precision attack; and **particularly** timely intelligence and situational awareness.

We're already taking this forward in our strategy work on Combat-ISTAR, including space and cyber. In the shorter term, RAF Air Command is leading in developing more coherence across the Air ISTAR sector on current operations, and we're seeing the fruits of this work in operational practice. In Afghanistan, highly effective networks have been developed. Strategic, wide-area search capabilities, like ASTOR or Nimrod R1, are being used routinely to cue platforms like the Reaper remotely piloted aircraft system with its high-resolution, but narrow field-of-view sensors, onto targets of interest. This in many ways demonstrates the seamless integration of air, space and cyber power that I've been talking about; Reaper is only the 200-mile physical capability at the end of an 18,000-mile space and cyber link stretching back to the Continental USA and forwards to analysis units here in the UK.

The Tornado also provides a genuine combat-ISTAR capability, data-linking video imagery to troops on the ground in real time and attacking a wide range of often time-sensitive targets. Critically the ability to provide comprehensive photographic and Infra Red images of the whole Sangin valley in 45 minutes and employ its targeting sensors, launch precision dual-mode seeker Brimstone missiles, and use the internal cannon, all on the same sortie and over a very wide geographical area, demonstrates the value of

genuine multirole Combat ISTAR aircraft. In the future, an asset such as the Joint Strike Fighter should be regarded primarily as a hugely capable comprehensive ISTAR hub sitting at the centre of a C4ISTAR network, but providing the option to deliver near real-time kinetic effects through its organic Control of the Air and Attack capabilities.

For the future, as our Combat-ISTAR Strategy develops, we will increasingly stitch together the potential of air, space and cyber capabilities to ensure full-spectrum domination of the information domain. This will include increasing the flexibility of all our platforms - adding ISTAR capabilities to Combat systems, and combat capabilities to ISTAR platforms – with JSF, as I've already said, being a fine example of a platform that combines both. Our network dependency means that this need for resilience will be true of cyber-space too; we will have to fight to gain and protect information. This is why we've recently established a Cyber Cell in the Air Warfare Centre, to help us understand how we can retain our freedom of manoeuvre in this important, emerging domain.

To maximise all of these capabilities a robust structure is required. What's needed is a coherent and effective C4ISTAR organisation: that is Command, Control, Communications, Computing, and ISTAR. Clearly, this needs to be joint, because the Information Domain is inherently joint, and C4ISTAR feeds will come from air, land and sea, as well as the other government agencies involved in the space and cyber domains.

I believe the ownership of assets and intelligence sources is largely irrelevant: it's achieving the desired outcome that really matters. Here, it does make sense to establish a collegiate, single-service lead, to **coordinate** activities efficiently, and to ensure coherence, and I believe the RAF is well placed to take on this role, because the specialist expertise in the majority of the areas connected to Combat-ISTAR, including space and cyber, resides overwhelmingly with the RAF; and because as airmen, the traditions of networked operations and information management have been embedded in our DNA since the Battle of Britain, the 70th anniversary of which this year reminds us of the importance of intelligence and information in delivering the 'decision advantage' essential to Dowding and Park then, and equally important today. I also think the very

close links we've developed with the USAF and many other NATO air forces over the last twenty years of continuous operations has also forced us to embrace networking and information management more fundamentally, including reach-back to the UK for networked expert analysis in support of the front-line operations. The organisational culture of the RAF is therefore a real strength for UK Defence, and its contribution in the information domain should be maximised.

Clearly, any C4ISTAR structure must be affordable, and I'm determined to wring the most value out of every Defence pound. We all understand that - as the chancellor has remarked - 'we have to live within our means'. Inevitably, we'll have to cut our cloth. However, one element that I'm absolutely determined not to sacrifice is quality – not only in our equipment, which gives us the inherent adaptability I've just described, but most importantly, in our people, and their training from which we gain our agility.

History demonstrates that hollowing out capabilities is usually a recipe for disaster, and is often worse than having no capability at all. In a period of rationalisation, it's more important than ever to focus on quality, even if this comes at the expense of mass. If we sacrifice quality, I'm in absolutely no doubt at all that we'll lose the institutional agility that provides the basis of our ability to deliver adaptable and relevant frontline capability. Not only that, we'll lose the people who give us the ability to innovate, and to develop the imaginative approaches that will be necessary if we're to exploit the full potential of air, space and cyber power in the most cost effective way in the twenty-first century.

UK Defence will face very significant challenges in the post-SDSR world, not least the never-ending information battle with current and potential adversaries. I will be doing my part to ensure the RAF uses the considerable experience, skills and inventiveness at its disposal to make a full contribution to meeting these challenges in the interests of Defence and the Country.