Air Marshal Phil Osborn on Intelligence and Information Advantage in a Contested World

18 May 2018, 12:30
RUSI Whitehall

RUSI MEMBERS ONLY

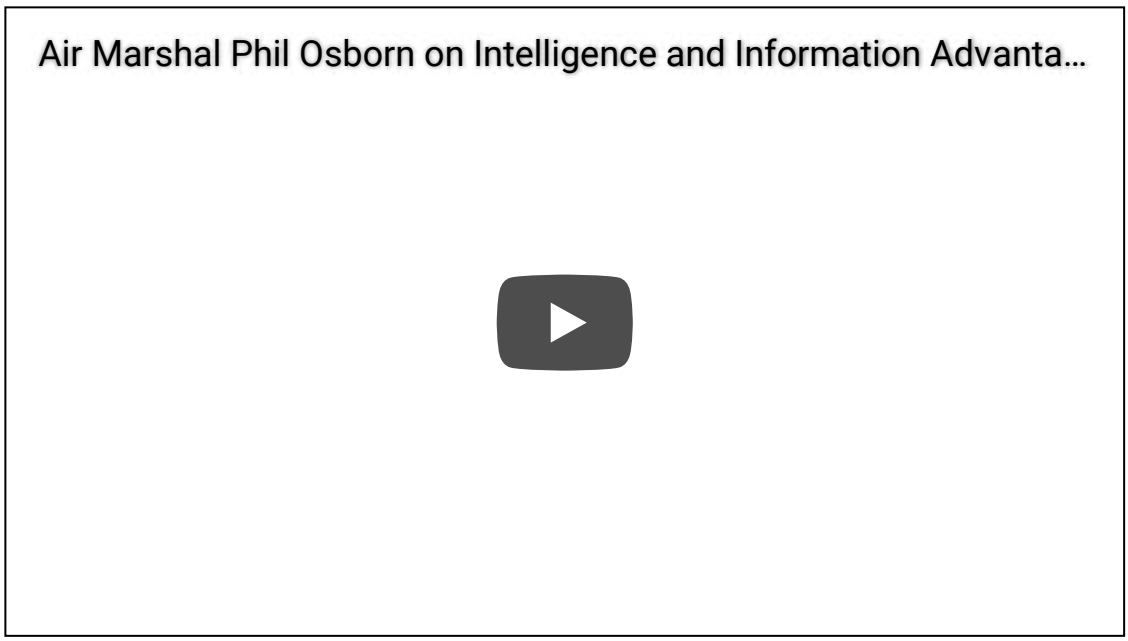
This event is sold out

A lecture by Air Marshal Phil Osborn CBE FRAeS RAF, Chief of Defence Intelligence, UK Ministry of Defence

The clarity of peace, transition to war, and war is fast disappearing. State-based competition and confrontation are now becoming the norm, played out across a multi-dimensional and multi-speed battlespace. For some, traditional levers of national power are being fused with an aggressive use of information tools, placing a premium on risk appetite, speed of decision-making and proactivity.

In his lecture, Air Marshal Osborn offered his perspective on the current operational context, the more complex challenge that faces UK defence today, and the increasing importance of a strategic military approach that places information advantage at its heart.

The Speech



Ladies and Gentlemen, good afternoon ...

As ever, it is good to be at RUSI and thank you for inviting me back … to be honest, it doesn't happen to me much. However, despite being obviously grateful to be here, I must confess to some trepidation. The RUSI audience is always extremely high-quality and I can already see that today is no exception.

Also, I am grateful to The Times for describing me today as a spy chief … first time in over 30 years that Mrs Osborn has been even vaguely impressed!

I have been the Chief of Defence Intelligence for some 3 and a half years, and over that period, I have had privileged insight into the growth in both the importance and capability of intelligence, counter-intelligence and cyber within Defence and across Government.

Indeed, it has been a constant honour to work with some of the highest quality public servants, military and civilian, within Defence and the wider MOD, and across Government and Allies.

Unsurprisingly perhaps, I want to pay particular tribute to all those within the UK's intelligence community. Whether they be in Defence Intelligence and wider Defence, the Joint Intelligence Organisation, the Agencies, or other intelligence assessment organisations in Government, our Nation and our Allies could not hope for better people to understand and then help manage what we would all agree is an increasingly dangerous world.

And it is that more dangerous world, and the role of intelligence and information, that I have been asked to reflect upon.

But first, a few words of caution …

My perspective, just like everyone else's, has bias. Mine is borne of over 35 years of military service and, within my current role, a focus on the risk of instability and conflict. It is the nature of Defence, and of Defence Intelligence, that we do not spend long observing nations and non-state organisations that are living peacefully … hence, there is a risk that my perspective tends to be a littler darker than those of colleagues in, say, the Foreign and Commonwealth Office. The good news is that as an intelligence professional, albeit still a fledgling one, I hope I am aware of and hence compensate for that bias.

Secondly, much of what I will cover is my personal perspective, and is not endorsed MoD policy. This is right … we in Defence have yet to complete our Modernising Defence work and hence it would be inappropriate to draw detailed conclusions from what I will say. It also means that I may stick with generalities during questions … I will also try to be clear where I cannot, or will not, answer specific questions.

Also, I am sure that I will not tell you much that is new … the Secretary of State, CDS, Permanent Secretary and Chiefs have all spoken recently on aspects of what I will touch on, as have others in Government.

However, I hope I will give an individual perspective on what you have heard and read previously … and perhaps some newer ideas to consider …

Enough of an introduction …

I think we all have a general sense that the world is strategically more dangerous, uncertain and unpredictable, and that state-based threats have become more acute. This should not be a surprise. The 2015 National Security Risk Assessment highlighted the resurgence of state-based threats and intensifying wider state competition. Also, in her foreword to this year's National Security Capability Review, the Prime Minister confirmed this intensification and evolution of threats to the UK. However, what we probably collectively underestimated in 2015 was the pace at which that risk would begin to mature.

Some examples …

It would have been unthinkable to imagine some 4 years ago that an ostensibly European nation would invade another … and we don't talk much about the Crimea any more, do we?

Just over 2 years ago, we would have assumed that an attack on the democratic process of a super-power would be nothing other than an act of war …

Again, just over 2 years ago, you would have accused me of being alarmist if I had suggested that a nation just about to be admitted to NATO would suffer a state-sponsored attempted coup …

You would also have scoffed if I had suggested some 18 months ago that an entirely attributable proxy war between international and regional super-powers would be the norm in the Middle East …

And just some 3 months ago, it would have been inconceivable to imagine that we would see a highly likely state-sponsored chemical weapons attack in a British city …

I would observe that the nature of warfare is changing to something that is broader than previously. It is becoming more strategic and increasing features continuous full spectrum competition and confrontation … and with new, additional domains of warfare being firmly to the fore … some of which can directly target centres of strategic decision-making.

We increasingly see a multi-layered and multi-speed strategic battlespace … a battlespace where it is possible to have open, positive collaboration in one lane, while waging an aggressive confrontation in another, while preparing and prepositioning for conflict in another …

And within each of these lanes, activity is layered, each delivering part of a full spectrum approach - across physical and virtual, legal and for some illegal - and all occurring at different speeds, some focussed on reaction or short-term opportunity, others playing out over a much longer period, positioning for influence or advantage.

Let's unpick this battlespace a little further …

Great power competition has returned, and usually sets a strategic context, albeit uncertain, for lower level regional power, state and non-state confrontation. Proxies are widespread, and end-states at every level differ … put simplistically, 'the enemy of my enemy is my friend' is an approach which may or may not be sustainable, even from week to week.

Now, a battlespace that simultaneously features collaboration, confrontation, and preparation for a prospective future confrontation is not new. Many collaborative international relationships are founded on a notion of deterrence, which requires the maintenance of credible critical capabilities through time.

However, the key words here are 'credible' and 'through time'. In important areas, prospective opponents already overmatch, or will soon, Western capability. This manifests itself in many areas but the most acute is probably the inexorable pressure on our, and Allies, ability to operate at a time and place of our choosing. A few examples amongst many …

We see an increasingly complex web of overlapping and integrated land, maritime, and air defence systems in almost every area of prospective UK military operations, including Europe, reaching out hundreds, and in some cases thousands, of kilometres. There is also notable investment in counter-space capabilities, threatening an increasingly non-discretionary domain of warfare.

Secondly, we are also witnessing substantial growth in land and maritime attack capability. Many nations are developing significant non-strategic nuclear and conventional land attack missiles, in some cases capable out to thousands of kilometres. Of note, ballistic missile proliferation is rife in many areas of the world, including the Middle East, and as well as holding critically important national

infrastructure at risk, this capability will increasingly challenge our ability to base and resupply deployed forces.

And, finally, the proliferation and use of chemical weapons, some very sophisticated, is on the rise, a worrying trend that will complicate significantly future military operations.

These examples, and others, underline that our ability to operate whenever and wherever we wish, and hence our ability to exercise the Nations will, is more challenging than we have experienced for decades.

There is also a newer aspect to a multi-speed battlespace. We of course prepare for conflict for years … capability development and training are core to Defence. But this tends to be capability-specific and battlefield agnostic … generally, we do not know in detail where we will fight next. Conflict itself tends to be measured in certainly weeks, usually months and sometimes years.

Today, all of this remains true … except in cyberspace. Depending on opposition capability and intent, and critically our resilience, a full-scale cyber confrontation could have nationally strategic crippling effects in minutes and hours. Moreover, the preparation of the offensive and defensive aspects of this type of conflict will be time and resource consuming, perhaps measured over years and will be battlefield specific, albeit that this battlefield will transcend geographic boundaries.

Even coming in from the extremes, this difference in pace between the physical and virtual, particularly in an integrated context, will not just provide a significant challenge across the full range of Defence activities, but most importantly also in terms of understanding, and strategic command and control.

I talked to aggressive confrontation. We know that there is significant growth in information-based capabilities such as offensive cyber and sophisticated information operations. Unconstrained by geography, these capabilities, when used, are often difficult to attribute, at least quickly.

For some, this ability to wage hidden and difficult to attribute warfare, in cyberspace and elsewhere, brings the opportunity to be much more aggressive and to take risk.

We can see numerous examples of this today … unprecedented industrial espionage activity against the UK and Allies; private security contractors being used in high-end expeditionary warfare in Syria; cyber attacks against national infrastructure and reputation across Europe; information operations that attempt to pervert political process and frustrate the rule of law; and attempted assassinations.

In sum, if we have an increased sense of strategic danger … and I think we should … it is the product of witnessing the combination of increasing capability and escalatory choice for many, and a growing intent in some to use these capabilities, at higher levels of risk.

The consequent risk of confrontation and miscalculation is rising.

Which brings us to the ‘so what? …

Well, I mentioned Modernising Defence, and you will know that this includes ensuring we are as efficient and effective as we can be in our approach and processes, taking advantage of best-in-class ways of working and technology to deliver the Defence mission. There is however a more operational imperative, set against the increasingly challenging operational context that I have just described.

Put bluntly, without change, we risk quickly falling behind in today and tomorrow’s full-spectrum confrontation.

This context demands that we are more strategic in our approach, and that our capabilities are better tailored to this accelerating shift in operational environment. ‘More of the same’ just won’t cut it …

I said that we must be more strategic. This continual confrontation across a multi-layered and multi-speed battlespace requires: that we understand more comprehensively and then decide quicker than

the opposition; that we have a better risk/benefit calculus; that we preposition earlier; and that if necessary we act sooner. We need to compete, sometimes proactively, and certainly not just observe.

In this more complex battlespace, risk-informed pace will secure the initiative … and to wait for risk to mature before action is to contemplate strategic failure.

There are many attributes to success in this context. For me, the priorities are: strategic agility and adaptability; interoperability rather than just interconnectivity; and Information Advantage from a resilient, integrated Defence Operational Platform.

Looking at Strategic agility and adaptability first, this will be required to execute the necessary and enduring strategic campaign across the multi-layered and multi-speed battlespace. We will need to secure a deep and persistent understanding of a prospective opponent's strengths, weaknesses and options, and then develop, preposition and employ our own capabilities for advantage, defence and deception. Those capabilities must of themselves be agile, and capable of 'last safe moment' deployment and employment to avoid being physically or virtually fixed.

Our aim should be to understand first, to decide first, and then if necessary to act first, across the physical and virtual, to secure decision advantage and then operational advantage, seeking swift yet controlled exploitation of vulnerabilities and the proactive denial of opportunities. Deception and counter-deception will be critical, as will an understanding of not just the risk of action, but also of inaction.

What will also be important will be our ability to adapt. Relying on agility to cope with a shifting sense of warfare is not sustainable in the long-term. We have to be able to adapt our thinking and capability, as our prospective opponents adapt theirs.

We must also view publicly available information as an operational domain, as the fight for the narrative is arguably as important as the actual fight. We need to have a convincing justification and narrative for our actions, while countering opposition disinformation and lies with the truth, both at speed and with releasable evidence. Throughout, we will need to be guided by a clear and transparent sense of legality and proportionality.

The second priority, for me at least, is the need for interoperability rather than just interconnectivity. In this full spectrum context, we will need to redefine what we mean by Joint … this time as an integrated cross-Government full spectrum approach, essential to deliver Fusion Doctrine as set out in the March NSCR report. Of note, the relationship we have with the Agencies is more mature than ever … but there is always more we can do.

We will also have to redefine how we work with like-minded nations. We will want to integrate full spectrum effects with Allies, building on and enhancing our strategic strength of working in Alliances. As the cornerstone of our national security, NATO is overwhelmingly important here and we need to help this incredible example of collaborative endeavour to remain contemporary.

Both imperatives – working across Government and working with Allies – will require true interoperability in new ways of working. Interconnectivity, although essential and necessarily far better than today, will not be enough.

The third priority is to deliver Information Advantage, from a resilient, integrated Defence Operational Platform. The concept of Information Advantage, still in formulation within Defence, owes much to the thinking of previous and current Commanders of Joint Forces Command, particularly around Warfare in the Information Age and now 'innovation, integration, and information'.

Part of Modernising Defence, Information Advantage is a concept which of course encompasses the increasing employment of information- and data-based capabilities. This audience will not need reminding of the exponential growth in this area, from information operations to offensive cyber.

However, many of us also believe that the aggressive application of machine learning, artificial intelligence, and quantum computing to full spectrum operations is likely to be as disruptive to modern warfare as Air Power was over 100 years ago. Therefore, Information Advantage also encompasses enabling, through leading edge AI tools, the intelligence- and information-led strategically agile approach to warfare I described earlier … strategic campaigning with the aim of understanding first, deciding first, and then acting first.

Finally, axiomatic to Information Advantage is a resilient, integrated Defence operational platform. No longer can we consider Defence as separate operational and corporate organisations. The full spectrum Defence threat surface encompasses the breadth of the Defence platform at every level, including critical HR functions, finance and reputation.

Moreover, an integrated Defence operational platform provides the essential launchpad for full spectrum operations, with resilient systems and ways of working, reputational defence and offense, and integrated strategic communications all being pivotal factors in the delivery of full spectrum confrontation.

So, what might be the initial steps towards Information Advantage, initial steps which will be important of themselves but will also set a strategic trajectory?

We will need enhanced resilience across the integrated Defence operational platform. This might include greater organisational and network resilience, and an enhanced counter-intelligence and security culture, as well as the more efficient and effective ways of working which are a fundamental part of Modernising Defence.

Next, Contemporary Understanding is the beating heart of Information Advantage and Strategic Agility. We have been working hard on improving our intelligence capability across Defence, with Defence Intelligence transformation already delivering significantly higher influence in Defence and across Government. We will build on this by providing pervasive, full spectrum situational awareness, a continuously available intelligence picture, and more predictive and anticipatory intelligence.

Our pervasive situational awareness will include understanding what has changed as well as what is happening, and our predictive and anticipatory intelligence will integrate the prospective actions of many different actors, enabling us to forecast significant events, and then deliver real-time indicators and warnings.

Potential capability improvements would be aimed at ensuring analysts are focused on our most difficult analytical problems, and that our situational awareness is truly ubiquitous. These improvements might include: increased investment in artificial intelligence and machine learning to manage burgeoning data volume and velocity, and to enhance analytical techniques; further broadening of our open source capability; investing in a blended mix of sovereign and commercial space; and investigating the use of every platform as a sensor.

Delivering interoperability, and not just interconnectivity is already underway with detailed engagement with the Agencies and within the Five Eyes community as we collectively look at ways of working in an Information Advantage-like context. Possible capability themes include participation in similar US work and enhancing Defence's datalink capability.

Turning to effects, a key part of Information Advantage will be operations in Cyberspace and across the Electromagnetic environment. We continue to work in very close partnership with colleagues in GCHQ to deliver the Nations offensive cyber mission, looking at maximising the strengths of each of our organisations and investigating how we can grow the scale of our already significant offensive cyber capability. Other potential non-cyber capability examples include greatly improved mission data management capabilities, and an enhanced land signals collection capability.

Lastly and probably most importantly, the major challenge around Strategic Agility and Adaptability will be to bring to life the concept of strategic campaigning, at a pace and complexity previously

unimaginable. In this, we should deliver an increasingly integrated strategic intelligence, planning, and command and control function, closely linked to training, mission rehearsal and capability acquisition.

Multiple opposition, neutral and friendly potential courses of action will be integrated, offering interactive and adaptable choice in how to maximise opportunity and take advantage of vulnerability. This will build on our current, well-proven military strategic function, and deliver an Information Advantage-enabled Strategic Headquarters.

This approach might also provide further opportunity. A step-up in strategic command and control capability is required for the Defence of the 21st Century … is the same true of Government. Is this the time for Defence to facilitate understanding, planning, integration and then command and control at the National strategic level, at pace and across multiple full spectrum operations, thereby enabling the command and control behind Fusion Doctrine?

Some closing comments, if I may …

I have outlined an increasingly dangerous full spectrum battlespace, multi-level and multi-speed, which requires us to be more proactive to maintain the strategic status-quo. This will need a more strategic approach founded on understanding first, deciding first, and then acting first, with a commensurately different appetite for risk. This continuous strategic campaign should be enabled by Information Advantage, which will provide not just information-based effects such as offensive cyber and information operations, but also the tools to deliver understanding, decision and then action advantage. And through a comprehensive understanding of the risk of action and inaction, enable the exploitation of vulnerabilities and the proactive denial of opportunities.

Elements of this appreciation may prove to be off-beam, certainly in detail and possibly in some more major areas. However, regardless, there is a unique and broader Defence role in any full spectrum confrontation, broader and deeper, and certainly not zero-sum.

While we will require far enhanced Information capabilities, this should not be substantively at the expense of more traditional conventional capabilities. There is a clear need for symmetric and asymmetric choice, within a more challenging physical and virtual operating environment, and incorporating a far greater range of escalation options.

This underlines the need to expand and modernise our more conventional capabilities in addition to adding new information capabilities. British military personnel and equipment remain some of the very best in the world, and we should maximise their utility.

Lastly, there is an immediate imperative for change, specifically to maintain pace with both the prospective opposition and Allies.

I have deliberately not gone overboard on the opportunity and threat of artificial intelligence and machine learning. But, to repeat myself deliberately, I am in no doubt that the application of these technologies will change warfare, as they will change our lives and society.

The threat is obvious. What may be less obvious is that, by inevitably changing the way we work, these technologies will also threaten one of our most important strategic strengths, specifically our ability to work with Allies. Our interoperability challenge will therefore be even greater than today, as our adapting ways of working must dock with those of Allies, most of whom will be applying similar information approaches but at different speeds.

If we fall behind either key Allies or prospective opponents, we will fall behind exponentially and likely irrevocably. Hence, the imperative to act, and act quickly, is compelling.

Ladies and Gentlemen, thank you … you have been very patient. I am now happy to take your questions.

Biography

Air Marshal Phil Osborn CBE FRAeS RAF joined the Royal Air Force over thirty years ago and has served as a front-line Tornado navigator, Tornado Squadron and Station Commander, Commander British Forces Op RESINATE (North), Chief of Staff Operations and Support at Air Command and Air Officer Commanding No 2 Group. His staff experience has been focussed on capability management. Prior to assuming his current role in January 2015 as Chief of Defence Intelligence, he was the first Director of Capability in Joint Forces Command.

EVENT MANAGER

Irina Dihanova
Receptionist / Members' Events Coordinator
Contact Expert

SUBSCRIBE TO OUR NEWSLETTER

Subscribe

SUPPORT RUSI RESEARCH

Make a donation

Join Our Network

Our membership packages provide privileged networking opportunities and benefits tailored to meet the needs of both individuals and large organisations.

CORPORATE

Our corporate memberships will also offer you unique access into the defence and security community through networking opportunities and discounted conference fees.

Corporate

INDIVIDUAL

RUSI members enjoy privileged access to the RUSI Journal, Newsbrief and Defence Systems as well as invitations to our full programme of exclusive members' lectures and seminars. Members also have access to our renowned Library of Military History and online catalogue.

Individual

RUSI LIBRARY

The collection is dedicated to developing our knowledge of war and sharing theoretical approaches to modern military thinking... read more

Open 9:30AM - 4:30PM
Monday to Friday

Visit Library

SUBSCRIBE TO OUR NEWSLETTER

Receive updates on RUSI's research initiatives, publications and events, with highlights of commentary and analysis.

Subscribe

SUPPORT RUSI

Noted for its quality, RUSI's analysis is driven by an ethos of accuracy, objectivity and policy relevance.