cityforum
cutting through

Cityforum Intelligent Defence Series 2019

Maximising Smart Power & Public Value

A Report on a Series of Round Tables & Conclaves

March - October 2019

Sponsored by:

BAE SYSTEMS

Cityforum Chair Marc Lee and CEO Veronica Scott have been supported in this project by a number of private sector organisations, particularly BAE Systems and with helpful support from Lockheed Martin

Intelligent Defence 2019: Maximising Smart Power & Public Value

Table of Contents

Foreword

Foreword

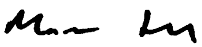
Cityforum has been engaged in defence analysis since the time of the George Robertson Strategic Defence Review in 1998. The particular work covered in this report 'Maximising Smart Power & Public Value' and one that preceded it in 2018, stemmed from a discussion with the last Chief of the Defence Staff and thereafter the active involvement of the Vice Chief and the Commander JFC. The agenda has been prepared after asking senior officers and officials what we should most usefully consider and we have had inputs from business, notably BAE Systems, members of the Cityforum group of Associates and other experts. The help of BAE Systems and other corporates has been vital since the project has involved no public subsidy.

Smart power and public value could scarcely be more pertinent as focal points in 2019 since the number of challenges confronting defence is growing and while budgets have recently increased, the global economic outlook is concerning and most forecasts for the UK are, at best, gloomy. Budgetary pressures could well reappear.

This report prepared by Paul Cornish, Cityforum Chief Strategist, with the help of my staff, covers a broad swathe of territory. We have been particularly interested in the thinking we have been able to do about the contribution of the defence sector to skills, capability, the national spread of jobs and the maximisation of the tax take that is made possible by work done in this country. The guidance on public value given in this series by the recently retired Comptroller & Auditor General highlights an area to which I wish Cityforum to return next year. In October, our principal sponsor, BAE Systems, presented a powerful argument for the industry contribution to value in national prosperity terms.

Cityforum has had considerable guidance from senior officers, co-ordinated by the Director Development, Concepts and Doctrine Centre (DCDC) and our forums have included direct contributions by the present Vice Chief, the Commander Strategic Command and the Director General Joint Force Development.

I look forward to our constructing a programme for 2020 and am grateful to BAE Systems, Lockheed Martin and others for their continuing interest in our defence activity.



Marc Lee
Chairman, Cityforum

Introduction

The Defence and Security landscape is changing. More attention is now being paid to the virtual and cognitive elements of warfare bringing concepts such as grey zones and persistent competition to the fore. Against this backdrop, information superiority has never been more important. The digital environment is becoming a battleground.

The UK Defence industry is highly innovative and contributes significantly to the UK's prosperity. It is a world leader in key technologies such as aerodynamics, stealth technology, propulsion and cyber. The UK also recognises the importance of maintaining defence skills, such as those needed for nuclear submarines, and there is a strong desire to nurture and apply newer skills, such as data science, to defence – something that BAE Systems is passionate about.

Given the rapid rate of digital development, our industry must also leverage leading advantageous technologies from outside of defence and adapt them to provide trusted, safe and dependable operational benefit.

From both an economic perspective and a national security perspective, the UK Defence industry needs to continue to thrive. As discussed in the Intelligent Defence Series, this is an industry that has a turnover of £22 billion and supports 260,000 jobs – many of which are in high technology and over half of which exist outside the South East. Defence exports contribute to the balance of trade and provide mechanisms to support the exercise of soft power. Furthermore, it is a highly efficient industry; in fact at BAE Systems we are seeing a productivity per employee that is 27% higher than the national average.*

As the defence industry continues to evolve amidst the digital environment, it has been a privilege to engage with and support Cityforum in this series of round tables and conclaves. Under Marc Lee and Paul Cornish's stewardship, diverse and valuable consideration has been brought to many of the issues facing the MOD and industry.

We look forward to seeing more progress in 2020.

Julian Cracknell
Managing Director, BAE Systems Applied Intelligence

* Oxford Economics - The contribution of BAE Systems to the UK Economy - published September 2019

The following report details reflections on the proceedings of Cityforum's 2019 Intelligent Defence Series 'Maximising Smart Power and Public Value, which comprised two Round Tables and four private Conclaves and culminating in an end of series lunch discussion. Speakers and participants included UK Government and Parliamentary officials and members of the Armed Forces, officials from other governments and allied armed forces and representatives of the private sector, policy research institutes, academia and the media. This report was prepared by Cityforum Chief Strategist Professor Paul Cornish. All contributions to the Round Tables and Conclaves were made under the Chatham House Rule. The key themes listed for each session were offered as guidance to participants in the light of Cityforum's own analysis and our discussions on programme content with MOD, sponsors and key speakers.

First Round Table: What do we need to do?

Thursday 14 March 2019
The Gladstone Library, One Whitehall Place, London SW1

Key themes:

- Keynote address: what do we mean by innovation and where and how should we prioritise for success in an information environment?
- How the United States approaches innovation in the emerging information environment
- Business, innovation and the acquisition process – how can defence and the nation gain the most benefit?
- Behaviours and capability – the 'how' and 'what' of innovation in defence
- Thinking through the achievement and maintenance of information advantage – what do we actually need to do?
- Increasing effect in conflict – in and beyond the grey zone

'Smart Power', is defined by Professor Joseph Nye as 'neither hard nor soft – it is the skilful combination of both. Smart power means developing an integrated strategy, resource base, and tool kit to achieve American objectives, drawing on both hard and soft power.' This brief form of words serves not only to clarify one of the central themes of Intelligent Defence 2019 but also to make clear that while national power should be understood as the 'skilful combination' of coercive (i.e. 'hard') and persuasive (i.e. 'soft') power, it also requires a 'resource base and tool kit' with which to ensure that national political, economic and strategic objectives can be met. The second central theme of the series is that of public value, in defence as well as in the exercise of national power more broadly. It was with both themes in mind that the first Round Table of the series set out to discuss innovation as a means to deliver value, in the form of an effective and efficient 'resource base and tool kit', to the UK economy in general and, specifically, to UK national power (both hard and soft).

Any discussion of the policy and practice of innovation soon invites difficult questions. Why are we so concerned about innovation – where should, or could it lead us? Do some sorts of innovation, in certain sectors, matter more than others? Is innovation itself something to

be designed, planned, developed and implemented programmatically, or should we allow for innovation to be 'organic' and evolutionary, as conveyed by the expression 'innovation by instinct'? How can we know when innovation is (and is not) successful)?

But the first question to be asked in any such discussion is the most obvious one: What is innovation? With echoes of Thomas Kuhn's 'paradigm transition', is innovation a mysterious agent of change where, by one account, existing knowledge is transformed into new products, processes and services? Or does innovation take us further still, into what the late Peter Drucker called a wholly 'new dimension of performance'? Alternatively, should we conceive of innovation in a more open-ended and less output-oriented way, irrespective of context; either as creating *more* value by acting and thinking in different ways, or as creating *new* standards and ideas of value by acting and thinking in new ways?

Consistent with what we tend to expect of it (to break boundaries, pose new questions, find new answers etc.) innovation should perhaps be allowed to encompass all definitions just discussed – everything, in other words, from new products to new philosophies. Such an unstructured and exploratory approach to innovation is, however, unlikely to find favour with governments tasked with solving complex and often urgent problems and spending public money wisely and accountably. It is at this point, in the context of public policy, that the distinctive nature of innovation becomes clear. Governments are often questioned about the level of their investment in science and technology (S&T) research. For others, the concern is less with the level of investment in S&T than with its management and distribution across the country and across sectors and also with the exploitation of its results.

But whether or not there should be greater investment in, or better management of such research, it would be wrong to conflate that investment and the research it enables, with innovation. Research, however sponsored, is of course a necessary condition for innovation, and the hardest and clearest test of that relationship lies in the claim that S&T research funding must to a large extent be undertaken at risk – the expenditure might result in nothing new having been developed, whether in the form of a new product or a new idea. Even so, assuming that normal research standards were met, it would be inaccurate to describe the outcome as 'failure' – the S&T investment could properly be judged to have been scientifically valid and a risk worth taking. Innovation asks a fundamentally different, more direct question, not "Was the investment properly made and scientifically valid?" but "Did it make a difference?" In other words, unlike the scientific and research foundations upon which it is built, innovation can be judged to have succeeded or failed according to context and output. The test that innovation must meet is thus a very concrete and practical one. In defence, for example, as one participant put it, the test of effective innovation is whether it delivers new capability or functionality, into the hands of its (military) users, and at sufficient pace to meet the urgent challenges they face.

Innovation is dependent upon, yet not synonymous with S&T research inputs. By the same token, innovation is more than simply implementation or output, i.e. the deployment or further adaptation of new or recent developments to meet specific, emergent requirements. Innovation should instead be understood as a process that links S&T policy, investment and exploratory scientific research inputs in a continuum with concrete, practical outputs which are necessitated and validated by strategic context and circumstance. To the extent that it can integrate both scientific exploration and practical application, innovation can be seen as a strategic capability in its own right. But this capability is more of a complex cultural phenomenon than the intellectual

equivalent of an 'urgent operational requirement'. One participant usefully encouraged an 'ecosystemic' approach to innovation; an ecosystem is a complex, interactive system in which 'life' forms (both biological and non-biological, benign and malign) interact with each other and with their environment.

Public sector-led, defence-oriented innovation is the purpose of the UK Defence Innovation Initiative, established in 2016 with a fund of c.£800 million to be allocated over ten years. The UK has also taken other steps to stimulate innovation such as the internationally oriented Defence Solutions Centre. And each of the UK armed services has its innovation hub, responding to specific service needs. But innovation is by no means the exclusive province of public policy, even allowing for the demands of national strategy and its thirst for new and ever more decisive technologies. Other sectors have their own approaches, indeed their own cultures, when it comes to innovation. In the financial sector, venture capital has played a significant role in the development of what might be termed 'investment-led innovation'. By one account, innovation within the start-up community is outpacing government programmes. This in turn has made it possible for larger companies to build their innovation strategy on mergers and acquisitions and venture capital investment, rather than fund their own, risk-laden, in-house effort. The venture capital culture, with its emphasis on 'failing fast' in order to minimise loss, can also be a brutally effective and more output-oriented antidote to slower, more cautious public policy-led innovation. That said, as one participant pointed out, the defence culture is not one that can easily tolerate failure in any circumstances – rather than reach the point of failure, it might simply be better to know when to bring the innovation and development process to a halt. Nevertheless, investment-led innovation can offer useful lessons. It might have relatively straightforward goals of resolving business difficulties and improving performance. But it can also be the basis of disruptive business models, as in the Tesla automotive and energy company. Furthermore, the venture capital sector is taking a close interest in 'pure tech' such as quantum computing, next-generation artificial intelligence and materials science; all areas which seem likely to be very highly significant strategically and particularly for the increasingly 'IT-aware' defence sector.

What might the future hold, and how should we respond to these possibilities? For one participant, noting that by 2020 there could be in circulation as much as 5,200 gigabytes of data per person, we are in the midst not of technological evolution but of a data-led revolution. This revolution is spawning new ideas such as 'cognitive security', 'cognitive manoeuvre' and 'predictive warfare'. These and other, similar expressions invite us to consider the relationship between human and non-human cognition, analysis and prediction, and which of these will deserve more of our trust in the highly complex and rapidly changing circumstances of future armed conflict.

The final session of the Round Table examined these complex and changing circumstances more closely. In the first place, what is the best shorthand description of what the future might hold? It has become fashionable to coin new expressions such as 'next generation', 'grey zone' and 'hybrid' warfare. Yet expressions such as these, for all their modishness, bring little if any clarity to the discussion. To speak of 'generations' is to suggest that technology and its military applications evolve in more or less discrete and recognisable phases; this has rarely if ever been the case and seems even less likely in the early twenty-first century given the pace of change in digital technology. The idea of a 'grey zone' is epistemologically destructive, but with few if any redeeming consequences. It relativises established knowledge frameworks to the point of incoherence and suggests, fatalistically, that the future is fundamentally unknowable rather than

something to which existing frameworks of knowledge and analysis must adapt. And 'hybrid' warfare is simply a category error; the distinctive feature in much of what is often described as 'hybrid' warfare is that it is *not* 'warfare' – it is competition that has been 'hybridised', absorbing some military methods, rather than vice versa. And if 'warfare' is allowed to persist in explanations of 21st century strategic competition it can too easily lead to the assumption that the response should be the task of armed forces – the experts, after all, in warfare. Yet a military response might be the least appropriate, desirable or effective. This is not to encourage complacency, however. Whether or not it makes use of war, warfare and warlike methods, strategic confrontation in the 21st century threatens to be destructive (physically and otherwise) and decisive.

More valid would be to attach our analysis of the strategic future (some of which seems already to have 'arrived') to ideas that are extant, coherent and robust. One particularly useful and widely understood idea is that there is a 'threshold' which must be crossed before armed conflict, as traditionally defined and understood for the past century or so, can be said to be taking place. The threshold is made explicit in Article 5 of NATO's Washington Treaty NATO (an 'armed attack' within the treaty area) but is also explicit in the United Nations Charter (Article 51) and in the body of International Humanitarian Law. This is not to say that whatever takes place 'below the threshold' is simply beyond comprehension and analysis; it is instead to invite closer analysis, a more accurate understanding of what is taking place and a more tailored response. Perhaps the most useful contribution to the management of conflict 'below the threshold' would be for armed forces to maintain a credible capability to act and deter above that threshold.

Where there can be little doubt is that the strategic future will require armed forces to be increasingly adaptable to changing circumstances and to become highly proficient in understanding, protecting and exploiting information. 'Cyber' operations, for example, will embrace both the defensive (i.e. resilience) and the offensive (based on rapid and accurate attribution of an attack). This is far from being an abstract problem or challenge. Russia is very well known for its long-standing interest and proficiency in information operations. If an increasing proportion of the arena of conflict (with or without the use of armed force) is to be defined by a struggle with and for information, then the UK and its allies should adapt accordingly. Armed forces around the world have struggled to redefine warfare in the digital age. In the process, information has gradually been reconceptualised from being a tool (or 'force multiplier') to being a domain in its own right. This debate is particularly well developed in the United States in the form of U.S. Cyber Command's strategy of 'persistent engagement' and 'defending forward'. But as one participant noted, 'persistent engagement' is only as good as the 'persistent presence' and the 'persistent innovation' that must underpin it.

Second Round Table: How can we do it?

Thursday 14 March 2019
PwC UK, 7 More London Riverside, London SE1 2RT

Key themes:

- Maximising capability for intelligent defence
- Building engagement and the will to contest as the nature of conflict changes; providing for domestic security
- How to gain the most benefit from the human resources available to UK Defence
- Intelligent defence, smart power and the national interest

The second Round Table in Cityforum's 2019 Intelligent Defence series began with a discussion of a relatively new addition to the UK security policy lexicon – the 'Fusion Doctrine' launched by the 2018 National Security Capability Review. The initiative was presented in the following terms:

> The Fusion Doctrine starts with strategy. We must identify the most effective and efficient combination of ways to achieve the government's objectives over the long term, anticipating how adversaries and allies could react to avoid unwanted second and third order effects. Sometimes the best approach may be weighted towards particular capabilities or asymmetric to the threat we face.

The Fusion Doctrine draws upon three sets of capabilities: Economic (private sector, regulation, development, economic levers); Influence (social policy, soft power, diplomacy, communications); and Security (law enforcement, armed forces, covert and border controls). In other words, the Fusion Doctrine offers an evaluation and decision-making process which is in some respects strikingly similar to 'smart power', a central theme of Intelligent Defence 2019. That said, when compared to Joseph Nye's definition of 'smart power' (see page 6), what is noticeably absent in the definition of the Fusion Doctrine given above is mention of 'resources' or, in the traditional British formulation, the 'means' that must accompany 'ends and ways'. If Fusion is concerned with the more effective co-ordination of 'ends' and 'ways' but lacks its own 'means' or resources with which to encourage co-ordination (perhaps because available resources have already been distributed to, and spent by the relevant departments and agencies), then it might more realistically be understood as 'smart power-lite'.

If Fusion is indeed intended to implement the central idea of smart power (i.e. the co-ordination of different types of power) then it is essential for there to be a clear understanding of what UK Defence could – and could not – contribute. Defence is the principal resource for hard, coercive power; an obvious point, perhaps, but an important one to make nonetheless. Smart power does not set 'hard' and 'soft' in competition with each other – both must be available if the sophisticated and nuanced use of national power is to be both effective and efficient. But defence can also offer other resources which, usefully, shade the boundary between 'hard' and 'soft'. UK Defence can offer extensive experience in the deployment and management of Provincial Reconstruction Teams; a framework for cross-governmental/inter-agency collaboration and local liaison developed in Afghanistan and Iraq. Where a more rapid, operational response is required, Defence has deployable headquarters held in readiness – described as 'sockets' into which other government departments can 'plug'. Defence can also react, rapidly and effectively,

to non-combat crises such as natural disasters. For example, according to the Royal College of Physicians 'the British military had significant involvement in shaping the UK's Ebola response' in West Africa in 2014. Working 'in harmony with efforts coordinated by DFID', British military contingents were closely involved in the establishment of military Ebola Treatment Centres dedicated to training healthcare professionals, both international and local. The Royal Navy provided important offshore support while a 'command and logistical hub' was established for 'operational management early in the epidemic.'

Britain's three Armed Services have little if any difficulty in working with other government departments and with deployable agencies such as the UK Border Force. All that said, UK armed forces face constant calls to adapt and improve and cannot be complacent. Armed forces must compete, in an often bewildering array of different circumstances, and they must also deter, on several levels. There is a pressing case for closer integration across the five dimensions of operation (land, sea, air, space and cyberspace) and for ensuring that the 'information advantage' can always be maintained against adversaries who are proving to be increasingly adept in the 'weaponisation' of information. Important questions also arise over the availability of resources for defence, and their optimal use. In spite of the rhetoric of agility, adaptability and versatility, UK Defence often has difficulty in understanding the multi-mission capabilities of its platforms. And there are questions to be asked – as there have been for decades – about UK Defence's relations with the industrial sector and whether, more broadly, the potential of a UK defence industrial strategy and prosperity agenda is at present unrealised.

Appreciation of the military contribution to Fusion could nevertheless be much improved – both across UK government generally and within UK Defence itself. If there is a case for the Cabinet Office and national security infrastructure to have a clearer understanding of the range of military capabilities, it might by the same token be said that UK Defence should develop a clearer understanding of Fusion, and what it seeks to achieve. Defence Engagement – a wide range of activities including security and non-combat operations; defence diplomacy (i.e. the defence attaché network); defence and security exports; and conflict prevention, post-conflict reconstruction and stabilisation operations) – is too often, and too easily seen as peripheral whereas these activities could be highly influential contributions to the exercise of smart power. Britain's armed forces are highly proficient at operational analysis, planning, command and control – a considerable national asset which could be drawn upon in the deployment of national planning cells, for example.

What are the limits to the fusion effort? The 'fusion' of relevant governmental capabilities in an effective and cost-efficient manner is not a simple matter but it is a necessary task, and one which is showing results. A rather more difficult challenge would be to find ways to join governmental and non-governmental resources in a common national effort. If fusion can be a source of efficiency in the exercise of national power and influence, then it follows that fusion should also contribute to an improvement in the public value (both perceived and actual) of security, defence and national strategy – more 'bang' for a smaller 'buck', perhaps. How much more value could be created if non-public assets such as the West's larger manufacturing industries and companies could be part of a joint public-private strategic collaboration? But at whatever level fusion is sought and achieved – cross-governmental, public-private and perhaps even international – it should also be borne in mind that the accretion of national power should not be an end in itself; we must at some point ask what this power is for.

The second session of the round table ventured into the relationship between society and its armed forces. By one account there is a complete lack of understanding among the public (particularly the post-Cold War generation) as to what the armed forces actually do. This is frightening and possibly even dangerous; if the public show no interest in and have no understanding of the risks associated with the deployment and use of armed force, then it is likely, if not inevitable that politicians will find it harder to decide and to lead in these matters. Who will then make these strategic decisions, and on what basis? As far as recruitment and retention are concerned, it is one thing to have passive respect for, and trust in the armed forces but that does not translate into a willingness to serve in the armed forces, let alone to understand why armed forces might be an essential feature of national life. Some of the difficulty experienced in recruiting young people into the armed forces might also be a consequence of what might be perceived to be disproportionate exposure to legal process. Over the past 25 years or so a 'post-Nuremburg landscape' has developed in which legal accountability for military action has become ever more difficult to ascertain and in which the lower ranks of the armed forces have increasingly been expected, reasonably or otherwise, to carry the responsibility for such actions. In the UK we therefore face a two-sided problem; not only is our ability to think strategically being hollowed out, but the national 'will to fight' is gradually being eroded.

If the relationship between society and its armed forces is in need of attention, so too is the public's understanding of national security. National security, as one participant observed, is a psychological construct, expressing the public's expectation of, and confidence in government's ability to provide for public security and safety. In this regard resilience – a much-used term in this context – is much more than simply a matter of business recovery planning and the strengthening of critical infrastructure. In order to reinforce the psychological construct known as national security, what is needed is a collaborative effort to create a resilient society. One step in that effort should be to make more use of the risk equation (likelihood versus impact) when describing national security concerns. Balanced and well-communicated analysis of risk allows for a sense of proportion and, with it, the beginnings of public confidence that government might, after all, know what they are doing. The UK is without doubt a safe and prosperous country, and likely to remain so. Although there are security threats and challenges, e.g. financial and identity crime, terrorism, extremism, hate crime, cyber security, chemical weapons misuse, all of which merit very close attention and prevention, these threats are unlikely to unravel the UK, either in detail or in the very unlikely event of being orchestrated in some way. If the UK is, as one participant put it, just 'three or four chess moves away from a national crisis' that need not be an indication of imminent defeat provided, of course, that the UK realises it is indeed playing chess with various skilful adversaries.

The title of the concluding session of the Round Table was 'Intelligent defence, smart power and the national interest'. The last of these is arguably the most important and decisive; defence can be 'intelligent' and power can be 'smart' but if the nation's 'interest' in these matters is at an ebb, for whatever reason, then we have a shaky edifice with very shallow foundations. In the course of the past century the UK has demonstrated something of a fondness for the idea of a 'strategic holiday', stubbornly ignoring suggestions that it might not always be wise to do so. At such moments (e.g. the 1930s and the late 1940s) there can be a tendency to look into the future, make a selective analysis of it and then reverse-engineer that analysis to show that the relaxed mood of the present is entirely rational. This tendency is difficult to resist; who, after all, would prefer to contemplate the prospect of death and destruction when more appealing alternative

visions are available? And there is always the danger that rampant pessimism about the future, even simply the excessive use of alarmist language, might prove to be self-fulfilling. But strategic holiday making is not wise; the future cannot be predicted and analysed in this self-serving way, and the future can often turn out to be much less pleasant than desired.

How to find the point of balance between complacency and alarmism? How, in other words, to be more strategic as a society? Part of the effort must be 'bottom-up', through education and improved public awareness. This effort can only, however, be initiated 'top-down'. The national leadership should realise that a strategic problem exists and should be determined to respond to that problem. Part of that response should be in the form of the serious, substantial and articulate national strategic communication programme needed to improve public awareness. But in the first place strategic communication requires there to be a strategy worth communicating. There must be evidence of a high-level strategic sense at work – evidence that government is the guardian of the national interest and is demonstrably willing to take political, strategic and financial risks to develop, maintain and protect that interest.

Conclave 1: Technology in Conflict – what are we now facing?

Friday 6 September 2019
BT Tower, 45 Maple Street, London W1

Key themes:

- How are we adapting traditional, territorially focused thinking about armed conflict to the prospect of 21st century 'technical conflict'?
- What is the nature and purpose of military operations in the so-called 'new dimensions' of space, cyberspace and the electromagnetic spectrum?
- Who has access to these 'weapons'?
- How can conflict in these environments be prevented, deterred, managed and de-escalated? Can the defence acquisition process be made more adaptable to meet new and evolving requirements? Can Virtual Design and Construction ensure that acquisition is not only more efficient (and carries less risk) but also more responsive to emergent threats and challenges?
- ICT also introduces the 'cognitive/information dimension' of warfare – what is 'information advantage' and how can it be won?

The relatively stable, monolithic structures of the Cold War have given way to an international security environment in which conflict is more diverse in character, more dispersed in origin and seems generally less susceptible to political and strategic management. Conflict is also fast acquiring a notable – and often bewildering – 'technological edge'. In the modern industrial era technology has often been described as 'enabling' or 'multiplying' the military effort. But by some accounts the 21st century 'edge' is more revolutionary than evolutionary, perhaps even becoming 'post-human' to the extent that it subverts the human role in many aspects of conflict, if not replaces it altogether.

If a technological revolution is indeed underway then its implications could be very far-reaching. At the highest levels of politico-military strategy, we could be in need of a complete reassessment of the purposes, modalities and management of modern conflict. But how straightforward could it be to abandon one strategic mind-set, developed over centuries, and replace it with another? Should we, instead, proceed by drawing analogies with past strategic experiences and modes of thought and expect contemporary solutions to emerge? What sorts of operations do we have in mind when we imagine 'technological conflict'? What could it mean to engage in a form of conflict (i.e. cyber conflict) which need not involve violence or destruction?

There are also questions to be asked about the invention, design, production and ownership of modern military technology and the purposes to which such innovations should properly be put. Who might have access to these technologies and weapons? What should be expected of the defence acquisition process in this changing environment? And how could 'technological conflict' be prevented, deterred, fought, managed and de-escalated?

The changing international security environment has prompted long lists of investments to be drawn up – all of them deemed essential for one reason or another. Thus, in addition to arguments for more to be spent on conventional systems (more and better armoured vehicles, warships, combat aircraft etc.), a case has been made for the UK to invest more in cyberspace

(including offensive cyber operations) and in outer space, to develop new weapon platforms offering improvements in both lethality and survivability, and to prioritise information integration across all defence functions. As well as the depth and breadth of defence acquisition there is also the pace of investment to consider; is the UK adapting fast enough to the changing environment or have we, instead, settled on incrementalism as the best way forward? However fast we are, or should be, adapting to the new environment, we should also question whether we are moving in the right direction. This question is pertinent in the case of cyber security, where the so-called 'threat landscape' seems to change almost on a daily basis. And behind all of these discussions lies another: how can the UK adjust its force posture to meet 21st century challenges while being constrained by a government spending plan which, for some critics, continues to be influenced by the 'peace dividend' mentality prompted by the end of the Cold War in the early 1990s?

Any discussion of defence innovation and acquisition must acknowledge that the relationship between the public and private sectors – a very well-trodden path in the UK – is changing fast. If, for example, space is to be prioritised by defence then some thought should be given to the fact that the vast majority of innovation in this area takes place within the private sector. In general, innovation in the private sector also happens at a tempo that, by one view, is 'exponentially' quicker than the defence acquisition process can accommodate. In short, with the strategic 'demand' lying in the public sector and the strategic 'supply' lying in a very differently geared and incentivised private sector, better ways must be found to ensure the alignment of innovation with national strategic priorities. One participant suggested that improvements could be sought in the pace and rigour with which new systems (both digital and non-digital) are accredited. Equally, the idea of 'prototype warfare' (sometimes described as 'battle in beta mode') could offer the possibility, albeit at some risk, of testing and evaluating new systems in the field rather than the laboratory. Whereas China, for example, has managed to achieve very close integration of the public and private sectors, one participant asked whether the time had come to accept that in the UK the public-private partnership in defence acquisition was beyond repair and reconstruction. If so, then perhaps our more modest ambition should be that of being 'as little wrong' as possible.

Difficulties in managing 21st century conflict will be compounded by the proliferation of threats and threat platforms and by the difficulty, especially where space operations are concerned, of attributing the source of an attack. Some of the risks appearing on the threat landscape appear to be self-inflicted. The emphasis on information integration in all aspects of defence reduces, arguably, to an ever-deepening dependence on ICT. Unless carefully (and expensively) managed, dependency equates to inflexibility and brittleness and, ultimately, to vulnerability. Conflict will also be influenced by new waves of innovation already visible on the horizon. Artificial intelligence, which in many respects has already 'arrived', merits careful consideration. In the view of one contributor, where AI is concerned the cycle of innovation and implementation spins much faster than in other areas. The military environment hosts several classes of AI, many of which exceed human capability, raising questions as to who – or what – will be 'in charge' of 21st century conflict. One benefit claimed of AI is that it can remove humans (both combatants and non-combatants) from dangerous environments. But this possibility, appealing though it might be at first glance, also invites close examination; after all, it is the fact that conflict places human combatants in danger (and not just for the adversary) that is the basis of ethical and legal constraints on conflict.

The Conclave turned, finally, to the prevention and management of technologically advanced 21st century conflict. It seems reasonable enough to ask whether highly evolved, Cold War

mechanisms such as conflict prevention, confidence building, deterrence and escalation control might also be effective in the cyber environment. They might, but only after careful thought and adaptation; these ideas and protocols were formed in the peculiar circumstances of the Cold War and should not be expected to survive in a new environment without careful nurturing. The goal of these efforts should be twofold: to reduce unpredictability; and to emphasise the management of delicate, tense and deteriorating situations, over the reaction to unexpected crises for which little or no preparation has (or, indeed, could be) made – a high-risk prospect that might result in costly and, it must be assumed, avoidable conflict.

Conclave 2: Technology Futures – what might we face and how should we manage the response?

Friday 6 September 2019
BT Tower, 45 Maple Street, London W1

Key themes:

- What technological possibilities and challenges lie in the distance or over the horizon (e.g. Artificial Intelligence, Human Machine Learning, Qunatum Computing)?
- How should government both manage (predictable) technological change and respond to (unexpected) technological challenges?
- When we describe these technologies as 'challenges', do we overlook the compensating opportunities and benefits they will also bring?
- Is the relationship between public and private interests optimally configured? Is the private sector fully involved and willing to take risk in preparing for long term technological change? Is there scope for public/private risk-sharing in defence R&D? Could venture capital have a role to play?
- Is innovation fully understood and prioritised by the public sector and by business?
- In what ways can government use its management of/response to technological change in a positive, proactive way, as a lever of national (and allied) power and influence?
- In what ways can government use its management of/response to technological change in a positive, proactive way, as a lever of national (and allied) power and influence?

The second Conclave in the 2019 series made a closer and more critical examination of the 'technological edge' discussed in the preceding meeting. Weapon systems that might have been considered the stuff of science fiction just years ago are now science fact, forcing change in the conduct of military operations. For example, research into electromagnetically powered cannons (or 'railguns') shows that these devices could offer far greater range and kinetic impact than conventional direct- and indirect-fire guns. Directed energy weapons such as high-powered lasers are already being deployed on warships for air defence and anti-drone purposes. Other developments such as unmanned aerial vehicles (UAVs) and autonomous weapon systems (AWS) go one technological step further by supplementing or, in some cases, supplanting the role of the human combatant. The prospect of the hybrid human/robotic combatant is enabled by developments in artificial intelligence (AI) and human-machine learning (HML). And very rapid advances in the scope and speed of information processing, especially with the prospect (albeit probably long distant) of functioning quantum computing (QC), also suggest that the traditionally human roles of command, control, communications and intelligence (collation and assessment) will increasingly be undertaken by machines.

The technological future – some of which appears already to be disturbingly 'present' – calls for carefully grounded, yet at the same time open-minded analysis. We need a clear understanding as to those technological changes that are already in train, those that are imminent and those that might be a more distant prospect. Which of these are threats, and which are opportunities? What is also required is some appreciation that governments and armed forces might be

confronted by unanticipated, disruptive innovation. How should the UK's strategic leadership both manage (predictable) technological change and respond to (unexpected) technological challenges? Is the relationship between public and private interests optimally configured to meet these challenges? Perhaps the private sector could assume some of the leadership traditionally expected of government. For example, at a time when private sector innovation is being undertaken by medium, small and micro-enterprises, which are open to foreign commercial predation, the case could be made for large defence companies to create 'protective purchase' consortia, perhaps with the encouragement of tax incentives, to acquire strategically critical SMEs (or perhaps larger companies) in order to protect them from foreign acquisition and thereby to secure their own innovation supply chain. The principles of security of supply might also usefully be applied to the provision of key building blocks of a technology or capability, such as the rare earth metals essential in microprocessor production or the proteins necessary in genetic engineering for bio-computing. Finally, is there not now a compelling case for these assessments and judgements to be co-ordinated in a national technology strategy?

The pace and scope of technological change was described by one participant as a 'major strategic issue' and by another as both 'exciting and wonderful' – and 'terrifying'. The worlds of security policy, national strategy and science & technology are all in a state of flux; perhaps the time has come for more centralised and systematic management, allowing for a closer understanding of the dynamic relationship between policy, strategy and technology, using that understanding to maximise the value of investment and to plan for the development of skills. UK Defence has the advantage of an in-house community of experts (there are no fewer than 19 defence innovation organisations in the UK – a statistic worthy of either applause or alarm) which ought to be the basis of a much-improved, multidisciplinary and cross-governmental understanding of the technological present and near-future. What would also be beneficial would be critical self-assessment of our relationship with technology. In the words of one participant, 'getting on top of the tech revolution' is as much a structural and cultural challenge as a matter simply of understanding a given technology and its defence implications. It should also be borne in mind that the UK's strategic competitors are having similar discussions and are making their own investment decisions, often in response to the proliferation of relatively cheap, yet still effective technologies.

One component of the 'cultural challenge' is behavioural and is concerned with our tolerance of risk. UK Defence is famously risk averse; by one account, 'we expect a 100% return on an investment made as much as 15 years ago'. More reasonable would be to accept a level of risk in defence acquisition. Rather than compile exhaustive lists of requirements, we should ask simpler and more constructive questions: Do we have what we need? If not, the next step should be to ask what *can* be achieved in a given period? Nowhere is the aversion to risk more apparent than in the attitude to failure. While it would be strange to encourage failure, any mature organisation must accept that failure happens and that when it does, it is a vitally important learning opportunity if its causes and circumstances can be identified and correctly understood. As well as a level of tolerance, good risk management also requires balanced, well-informed assessment of possible and likely futures. In that vein, one participant argued that four technologies in particular will have a decisive effect on the future international security environment: movement towards a self-sustaining, circular economy in molecular materials (iron, steel and plastics, for example); the transition from fossil to renewable energy, coupled with the development of synthetic liquid fuels; the use of so-called 'smart' materials – biologically derived plastics and

polymers that mimic fossil-based materials but can also self-indicate and self-heal; and finally distributed manufacturing – small scale, so-called 'additive' manufacturing undertaken on the basis of 'dial a molecule.'

The final session of the Conclave turned from science, technology, research and development to the people who – at least for the time being – must be at the heart of all such efforts. We should consider what, in the future, people (ourselves and our adversaries) will expect from technology and how they will make use of it. Answers to these questions will in large part be driven by the circumstances that might prevail. If there will be conflicts, then of what sort and on what level; state versus state, 'small wars' and insurgencies, so-called 'grey zone' conflict or 'endless wars'? Each of these will present different requirements for the skills development and training of individuals. More generally, as machines become more common in any and all workplaces, and at levels that were previously considered to be the preserve of humans, so the role of humans will have to be reassessed. Perhaps humans will be expected to take on more complex decision making? Whatever the case, it is certain that in the workforces of the future, humans and machines will be in a professional relationship of some sort. The relationship between human and machine will need very careful management; if machines are allocated simple and repetitive tasks (in manufacturing, say), leaving humans to deal with more complex judgements and decisions then two possibilities arise - either that too few humans will have too much to do and will be overloaded, or that too many humans will have too little to do.

Conclave 3: Civil Contingencies and Domestic Security

Thursday 19 September 2019
Pivotal, The Warehouse, 211 Old Street, London EC1V 2NR

Key themes:

- The resurgence of interest in domestic security and in the protection of the territory, infrastructure and interests of the United Kingdom against attack. How might GDP be affected by damage to the UK domestic infrastructure?
- What are the challenges to UK domestic security and how vulnerable is the UK to a disabling attack against the CNI or even to the breakdown of civil society?
- Which government departments/agencies are responsible for domestic security, resilience and recovery and how/how well are they coordinated? To what extent does the UK Fusion Doctrine contribute to planning and preparation in this field?
- Can/should the private sector be considered an 'agency in its own right', given that much of the UK digital CNI is privately owned?
- What is the net assessment of UK preparedness and resilience in the face of domestic security risks?

While the UK has spent much of the past two decades improving its civil contingencies apparatus and strengthening the resilience of its critical national infrastructure (CNI), recent incidents (including the use of chemical weapons on UK soil in March 2018, persistent attempts to enter the UK by illegal and highly hazardous means, the misuse of drones around UK airports and the Wannacry ransomware attack in May 2017) all suggest that there is more work to be done. This a complex problem. On the one hand, some challenges to UK domestic security and resilience have origins within the UK while others have foreign sources. Some have both. On the other hand, the response to these challenges does not fall easily and exclusively within the competence of any single government department or agency; cross-governmental collaboration is essential. Which government departments/agencies are therefore responsible for which aspects of domestic security, resilience and recovery and how/how well are they coordinated? To what extent does the UK Fusion Doctrine, discussed at length in the second Round Table on 14 March 2019 (see page 10) contribute to planning and preparation in this field?

The third Conclave in the 2019 Intelligent Defence series therefore asked not only what is at stake, and whether the UK is sufficiently attuned to the risks of attack against/breakdown of civil society, but also whether we are prepared – intellectually, materially and, perhaps above all, organisationally – to manage these risks. As with other discussions in the 2019 series, the Conclave also addressed the role of the private sector; to what extent can it be considered an 'agency', of sorts, of UK CNI, given that much of the CNI, particularly in the digital sector, is privately owned?

Counter-terrorism is widely perceived to be the most pressing domestic security concern in the UK, and the focus of a considerable joint effort involving both public and private sector bodies, reflecting the blurring of boundaries at both the operational and strategic levels. There remain some differences in culture, language and practice between the Armed Forces and the Emergency Services – the former are familiar with the 'command and control environment' while others

in the Emergency Services are less so. Many such differences are resolved through practice. After decades of training in the provision of Military Aid to the Civil Authorities (MACA), UK Armed Forces are fully cognisant with the principle that in any MACA deployment the military must always be in support of civil authorities (other than in the event of an immediate threat to life). The UK Fusion Doctrine should also contribute to more effective and efficient inter-agency collaboration; but as one participant noted, 'Fusion meetings never work with close-minded people.' More tenacious cultural or structural differences can and should be eliminated over time, possibly through the development of inter-agency doctrine. As the threat landscape continues to evolve and with threats becoming more ambiguous in source, means and intention, more use should be made of digital platforms and emphasis increased on early warning and prevention. The Police Service, by one view, is expert at reaction but less effective at looking 'over the horizon' or 'further down the line.' Critical self-assessment is also essential, particularly in the event of failure. This in turn requires the end of the 'blame culture' that can be so damaging to organisational adaptability.

The Conclave turned to resilience, a term that has become central to the civil contingencies discussion in the UK. Resilience can be defined as the return to a normal state after a shock of some sort, such as an attack. Some have argued that a system which reasserts to a position in which it can be (and recently has been) attacked could scarcely be described as resilient; resilience should not be a matter of returning to the *status quo ante* but the more demanding task of moving to a different, less vulnerable and more advantageous position. Resilience should not be a 'stove-piped' effort – it requires a systems approach and can usefully be understood as the achievement of security across dependencies and linkages. With that in mind, resilience – and an awareness of the need for it – should be woven into planning and preparation at the earliest possible stage, ensuring that linkages and vulnerabilities are identified and acknowledged. This broader understanding begs a number of questions. Are the current structures of government departments and agencies fit for the purpose of maintaining resilience at the system level? Particularly where cyber security is concerned, is the relationship between the public and private sectors adequate to the task?

Domestic security is not exclusively concerned with counter-terrorism or serious crime, highly significant though these challenges are. The domestic security debate also extends into more obviously military matters, such as the need to secure and protect the UK defence estate and infrastructure, in order to ensure that the Armed Forces are able to carry out their core military tasks when called upon to do so. In this context, domestic security should also be understood as a matter of physically hardening key facilities and assets, of technically hardening systems against electronic and other intrusions, and of attitudinal hardening. The latter might involve more extensive security vetting, firmer policy on how security breaches and losses should be treated and clear communication as to the persistent threat of espionage.

The Conclave concluded with a discussion of the broad nature and purpose of collaboration in civil contingencies and domestic security. Is the goal a genuine, mutually beneficial collective endeavour, in which all participants willingly surrender some value in order to gain more in return? Or is there a sense that collaboration is defined by that surrender of value and by little more? If the richer definition of collaboration is the purpose, then perhaps commercial joint ventures might serve as a model for cross-governmental, inter-agency collaboration? While there might be merit in comparing governmental and commercial/industrial practices in this way, attempts to 'break down the silos' (as one participant put it) between government, defence

industry and other actors will only succeed to the extent that they are driven culturally, by a common sense of responsibility shared by the public sector, the technology sector and civil society itself. Without that shared sense there are grounds to question whether the 'systems approach' discussed earlier in the Conclave will ever gain much traction.

`

Conclave 4: The Purpose of Armed Force

Thursday 19 September 2019
Pivotal, The Warehouse, 211 Old Street, London EC1V 2NR

Key themes:

- The international security/strategic landscape is in flux. Some features of the landscape are familiar – e.g. the behaviour of adversarial and potentially hostile states prompting warnings of a 'new Cold War'. Other features are less familiar, such as the emergence of non-state organisations as users of sophisticated armed violence for ostensibly state-like goals.
- The challenge seems to be less conflict per se, than competition, often below the legal threshold of armed conflict, and might thus be perceived to require a response that differs from the traditional role of national armed forces.
- There has been much talk of 'hybrid warfare' as an organising principle with which to meet these developments. But would 'hybrid policy' be more suitable, whereby military preparation and deployment (on intervention operations, for example) are but one component of a more comprehensive and nuanced posture for the analysis of, and response to, security challenges?
- How well – and how effectively – are the various levers of national power (including the armed forces) configured to compete in this so-called 'grey zone'?
- Is the fundamental and distinctive purpose of armed force – the organised and decisive use of violence for national interests – being diluted? How best can understanding of the role of armed force be communicated to broader society, and can the public be convinced?
- The effective and sustained exercise of national power requires the efficient use of limited national resources. Is there scope for 'up front' investment in order to achieve longer term efficiency savings, particularly in defence?

The fourth Conclave in the 2019 Intelligent Defence series addressed the role of UK armed forces in responding to the security and strategic challenges discussed in earlier meetings in the series. What are the particular problems that the United Kingdom's armed forces are expected to solve, and which (if any) of these problems should be solved by the armed forces acting entirely independently, without the assistance of other branches, departments and agencies of government?

The 'purpose of armed force' also invites discussion of the triangular, constitutional relationship between government, armed forces and society. When preparing for national security and defence, and especially in cases where the conflict or confrontation falls below the international legal threshold of armed conflict, do we have the right balance of initiative, authority and responsibility between armed forces and government? There is also the third part of the constitutional triangle to consider. Does the public understand the armed forces and what they do? After all, if the controlled use of violent and destructive armed force is to be the last resort in UK foreign, security and defence policy, then surely the UK public must be convinced of its value and relevance and must ultimately be willing both to support the commitment of public funds and to accept the personal, physical risks of military service. Or are the fundamental and distinctive purposes of armed force – the organised and decisive use of violence for national

interests – being diluted in the public perception? If so, what can be done to communicate the purposes of armed force – in all applications from 'soft' to 'hard' – to broader society? And will the public be convinced?

The Conclave began with a useful reminder that the purpose of armed *force* should not be elided with the purpose of armed *forces*. If the two terms become synonymous then an important distinction is lost. The purpose of armed force is relatively self-evident and rather narrow; in the abstract, it is to deter, protect, defend, coerce and defeat. The purpose of armed forces, on the other hand, is broader and more context-dependent; it is to maintain the capabilities needed to deliver armed force for the circumstances just described. Set out in this way, the challenge becomes clearer – it is to explain to the public that the purpose of the UK's armed forces is both to deliver lethal kinetic force, coercion, deterrence etc., and to take on other roles such as Military Aid to the Civil Authorities (discussed in Conclave 3). If it is the case that more public support for the armed forces is needed then all can agree that a better effort must be made by the armed forces, by the Ministry of Defence and by government in general to communicate this vital message and explain what it is the armed forces are for. The solution might be close at hand; UK Defence Doctrine already sets out, clearly and accessibly, the purpose of defence, although the document cannot yet be described as a best-seller. But we should not assume, before embarking upon it, that the task is insurmountable, or even nearly so, or that the task is to equip the public with an expert level of knowledge. The level of public understanding might be low, but still be sufficient. After all, the public generally understand the need for the judiciary and the prison service without having necessarily been a magistrate or a jury member or having spent time in prison.

Public opinion is important to defence and national strategy, but governments and armed forces can often be rather bad at understanding it, and vice versa. In the view of one participant, security experts (in government, the armed forces and civil society) often tend to under-estimate how much the public understands them and the world they represent. And the public does something similar. All three sides of the constitutional triangle need to understand each other better, and if serious attempts were made to bring this about, we might find that the gaps are less wide than as is often thought (and feared).

One way to enhance public understanding of the armed forces and what they do would be to explain the context of a given deployment, mission or operation as clearly and intelligently as possible (within the bounds of operational security). If, for example, the UK has security concerns in/with the Gulf then those concerns can and should be explained to the public and the explanations brought up to date from time to time. Similarly, if the Ministry of Defence has concerns about China's strategic ambitions, it would be helpful to explain why certain other UK government departments do not appear to share those concerns. There would also be merit in explaining why some operations are prioritised over others – how some missions might be considered important, and others urgent. What do these descriptors mean? The public might also be receptive to an explanation, even if only in general terms, of the forms and levels of contingency planning undertaken by the armed forces, and why.

The Conclave discussed the extent to which the 'purpose of armed force' (and 'forces') is understood among the UK's Black, Asian and Minority Ethnic communities. In these communities there can be a lack of understanding of the role of the UK's armed forces, but it was noted that similar things could be in other countries. In some cases, adverse perceptions of the armed forces

might take hold for a variety of reasons, some more convincing than others. There might, for example, be a perception that ex-servicemen often end up homeless and begging (something that would not often be encountered in India and Pakistan, for example), that the rate of suicide in the armed forces is unusually high, or that the armed forces are not 'BAME-friendly', and possibly institutionally racist. These adverse perceptions can be offset, however, by a generally high level of respect for the armed forces and those who serve in them and by a sense that in a troubled and unstable world, defence spending is broadly to be welcomed. These different perspectives and contending opinions on the armed forces, what they represent and what they are for, should be taken as encouraging evidence that the UK's BAME communities do not necessarily lack interest in the country's armed forces and that these communities should be no less receptive than any other UK comminuty to the clear, intelligent explanations of defence-related activity discussed above. Ultimately, the UK's armed forces rely on people and the skills they have or can learn. If, as one participant suggested, we can 'make the exceptions unexceptional', becoming entirely impartial as to cultural, ethnic, racial or social background, then the opportunity arises to attract more people into the armed forces with more of the skills (both generalist and specialist) and potential that will be needed.

Finally, the Conclave turned to a *leitmotif* in the 2019 Intelligent Defence series – the relationship between the public and private sectors. Government and industry must work together to address a shortage of skills in key areas such as cyber intelligence, machine learning and deep learning. In order for this collaborative effort to be coherent and to be understood by all those involved, and to be strategically effective, we should think less about the traditional threshold between peace and war and instead allow a seamless transition between the two. Rather than preparing collaboratively to cross the threshold into war, the purpose of public-private collaboration should be to move back and forth along a continuum, from the virtual to the cognitive to the physical (including cyberspace), and back again, and to have decisive effect at all points on the continuum. At some points the task might be distinctively military, but at others the task might be led by industry or by other actors such as the media. All contributors – public private or third sector – would then have played a decisive role in delivering a coherent effort.

Concluding Discussion: Making the most convincing argument for the public value of defence expenditure

Wednesday 30 October 2019
BT Tower, 45 Maple Street, London W1T 4JZ

Key themes:

- Defence, international engagement and influence
- Thinking about how to secure better public value
- Defence – public value and public values
- Defence – innovation, capability and prosperity
- Communicating with the public, politicians and the Treasury
- Fusion Doctrine – integration, efficiency and value
- Defence, public value and public values – what the Cityforum 2019 report tells us

The final meeting in the 2019 Intelligent Defence series reviewed several of the themes discussed earlier in the series. The session began with a discussion of the meaning of 'value for money' (VFM) – a term which is much used, and often too loosely. VFM is emphatically not a synonym for 'the cheapest' tool, product, material, method etc. available for purchase. Spending control – closely associated with the expenditure of public finances – regulates outflow but does not necessarily determine value. As several participants observed, a misunderstanding of value can too often lead to a 'race to the bottom' in expenditure decisions. Instead, VFM should be understood as the optimal use of financial resources (public or private), informed by analysis and judgement, in the achievement of an objective. Value must therefore be defined contextually. A leading authority on public expenditure warned the forum that many projects go wrong because the problems encountered along the way have not been considered at the outset. This weakness also affects defence.

In the context of defence acquisition, the clearest and most useful understanding of value is that contained within the idea of value engineering (VE) developed in the United States after World War II. Pioneered by GEC, VE has been defined as 'an organized/systematic approach directed at analyzing the function of systems, equipment, facilities, services, and supplies for the purpose of achieving their essential functions at the lowest life-cycle cost consistent with required performance, reliability, quality, and safety.' In the VE approach, value is the ratio of function to cost, inviting a systematic effort to provide the required function, at the required standard and at the lowest available cost while ensuring that unnecessary cost is identified and eliminated. In order to hedge against an uncertain future, and against the possibility that what seems an unnecessary expense today might not be tomorrow, a value-based approach to defence could also identify the costs associated with not delivering a certain function, but then having to re-equip or reconstitute at a later date. In any enterprise, public or private, a rigorously maintained medium-term planning process is essential if value is to be kept in mind and in context, and if unwanted surprises in expenditure schedules are to be excluded. And in any organisation managing complex spending plans it is, above all, a mistake to suppose that the route to 'value' lies in the insistence on making 'savings' elsewhere in the system.

Discussions about the relationship between government and the defence industry were a major element of the forum and included significant contributions by the CTO of a prime and by the head of an SME working in several sectors, including defence. This relationship has an anomalous character in that government is both the regulator of the defence industry and its principal customer. Nevertheless, both sectors could make a more strenuous and commercially mature effort to understand the experience, expertise and skill levels (particularly when it comes to the negotiation of complex contracts) of their opposite numbers. The tolerance of (or, conversely, the aversion to) failure could be another source of misunderstanding, with the public sector (especially in defence) arguably too brittle in its aversion to failure, and the private sector arguably too tolerant of the possibility.

In the view of one contributor, defence companies remain in existence only to the extent that they can innovate – the third theme of discussion. But innovation (discussed at length in Conclave 2) does not simply happen of its own accord – it requires an indigenous and resilient national culture of innovation, with accompanying investment in science and technology and exploratory research. Innovation also requires the maintenance of key skill sets, e.g. in specialist areas of design and manufacturing, through training and education and through the 'drumbeat' of defence acquisition. Innovation is also the defining characteristic of the UK's technologically-oriented small and medium-sized enterprises (SMEs) – described by one participant as the backbone of the UK economy and its fastest growing sector. SMEs lead innovation in many of those areas considered to be, or about to be, 'game-changing' in security and defence – i.e. artificial intelligence, big data analytics etc. In this respect the private sector is forging ahead of the public sector, which is too slow in recognising and exploiting the strategic lead being provided by innovative SMEs. SMEs also come to maturity at a pace which outstrips governmental assessment and decision-making cycles. Urgent thought should be given as to how the defence public sector can engage more effectively with what amounts to a national strategic asset, and how fast-moving SMEs can better engage with a frustratingly sluggish and 'cash-strapped' Ministry of Defence. The impact of skills, capabilities and employment provided by the defence industrial sector was made clear during the debate.

Discussion turned, finally, to public perceptions of the value of defence. To a considerable extent, public perceptions are shaped by the way government describes the purpose of defence and the armed forces and rationalises the expenditure of public money to those ends. In this regard, as well as more information (see below), more transparency would also be welcome as to the size and shape of the defence budget. This important discussion is often truncated to bland reassurances that the UK is 'meeting' the NATO commitment to spend two per cent of GDP on defence. But what is not explained often enough to the public is that the defence budget is not committed entirely to current military tasks and equipment, and that 'defence' spending also includes non-operational items such as pensions and housing. It is perhaps for that reason that estimates of 'real' UK annual defence spending can vary by several billions of pounds.

More broadly, in the words of one participant, the UK defence and security debate too often takes place in a 'vacuum', with too little effort to engage with the public and to offer articulate and well-informed explanations of defence thinking. Defence and security have, in other words, become a niche area in public policy – both as far as the public are concerned and in Parliament. There is, however, a public appetite for high quality information and debate on matters of defence and security, and especially the value judgements that underpin defence preparations and decisions, and that appetite should be fed. Parliament should be at the heart of this improved debate,

undertaking a liaison function between government, armed forces and society as a whole. In a western liberal democratic society, the values that underpin national decision-making should be a critically important point of debate in all areas of public policy. And where defence is concerned, parliamentary accountability is arguably as important as any configuration of military capabilities.

When it comes to the informed, critical and inclusive debate that should feature in all matters of public policy the media also play a central role. Or at least they have done so until recently. The media industry is in the throes of change, and possibly decline. The UK national media is shrinking (particularly when it comes to regional media reporting 'local boy' and 'local girl' stories with connections to the armed forces) and newsrooms have lost much of their specialist knowledge and research capacity. This shift was exemplified by what passed for newspaper reports of the British Army combat power demonstration taking place on Salisbury Plain on the day preceding the meeting – one syndicated photograph of an armoured vehicle moving through flames with no caption or accompanying story describing, or even merely summarising the extent of the capability demonstration!

If the public are under-informed about defence, if the defence and security debate in Parliament has become self-referential, and if the media are losing interest then what is to be done? The forum concluded with a plea to the armed forces to do more on their own behalf – to enable the public to gain a more physical or 'hands on' understanding of defence; to invite more of the public to more events; to make the recruiting infrastructure more visible in towns and cities; and to distribute more information direct to the public about what the Royal Navy, the British Army and the Royal Air Force are actually doing, where they are deployed and why.

Cityforum is grateful to the following organisations for their kind sponsorship and hosting:

cityforum
cutting through

Cityforum has been contributing to public policy debate since 1990. The organisation comprises a small, trusted, independent group of experienced individuals, respected for their intellectual honesty, knowledge and extensive contacts spanning the private, public and not-for-profit sectors at all levels. In addition, it works closely with a large network of associates, providing depth, breadth and genuine expertise and practical experience. They include a former Cabinet Minister, a retired Member of the Episcopal Bench, public service officials, military, police, intelligence and security specialists, senior medical figures and business executives, academics, journalists and publishers. They contribute in London and elsewhere to Cityforum events and to the studies we undertake, including interviewing at all levels in organisations and sectors of interest.

From its inception working with the Bank of England on the Basel Accords; with the Reserve Bank of South Africa on the transition from apartheid; hosting and planning with the Scottish Government the Adam Smith Bicentenary; Cityforum has been active in an increasing number of areas that now include collaborations in security, policing, crime and justice, emergency services, critical national infrastructure, cyber, privacy, health and social care, transport, financial services, regulation and energy.

It researches and publishes reports and develops and hosts events in the UK and, where invited, around the world. As part of its bespoke advisory and strategic guidance service the organisation also acts as a 'candid friend' to senior public-sector executives, and undertakes studies and reviews, providing sound impartial advice and specialist judgement to assist in meeting the enormous challenges faced by the public service today.

With over 25 years shaping strategic thinking, building understanding and adding value within and between diverse groups, the organisation has a proven track record. Its highly regarded round table discussions and smaller conclaves are well known both for bringing together an enviable mix of decision makers and practitioners and for stimulating new thinking in response to some of the most difficult contemporary public policy challenges.

Cityforum has a particular interest in working with the police and holds three or four Round Tables a year on strategic, technological, human resources, value for money and strategic communication questions affecting the service. It also undertakes specialist advisory and monitoring work for individual Police and Crime Commissioners, and Chief Officers. This has been particularly useful when PCCs - Police and crime commissioners and Chiefs require studies to be undertaken by a seasoned group of specialists who operate methodically and quickly, and have particular skills in interviewing at every level in the organisations requesting assistance. Its reports are succinct and written in readable English rather than in management speak loaded with acronyms.

Biography - Paul Cornish, Chief Strategist Cityforum

Professor Paul Cornish is Chief Strategist at Cityforum Public Policy Analysis Ltd and director of his own consultancy company, Coracle Analysis Ltd. He is Visiting Professor at LSE IDEAS, the foreign policy think tank at the London School of Economics, and has held senior appointments in UK research institutes and universities: Chatham House (where he established the institute's cyber security research programme); the UK Defence Academy; the Centre for Defence Studies at King's College London; RAND Europe; and the Universities of Cambridge, Bath and Exeter. His work covers international security, national strategy, arms control, the ethics of armed force, and civil-military relations. He became a member of the UK Chief of Defence Staff's Strategic Advisory Panel from 2013, was Co-Director of the Global Cyber Security Capacity Building Centre, University of Oxford from 2013-18 and Professorial Fellow in Cyber Security at the Australian National University's National Security College in 2017. He has published widely on national strategy, international security, cyber security and cyber governance and is editor of the *Oxford Handbook of Cyber Security*, to be published by Oxford University Press in 2020.

The organisers reserve the right to amend the programme at any time

Intelligent Defence – Maximising Smart Power and Public Value

A programme of round tables, analytical papers and conclaves arranged by Cityforum in association with the Development, Concepts and Doctrine Centre of MOD (March to June 2019)

First Round Table – What do we need to do?

14 March 2019 - The Gladstone Library, One Whitehall Place, London SW1A 2EJ

Agenda

Principal Sponsor BAE SYSTEMS Co Sponsor LOCKHEED MARTIN

SME Co Sponsor BOXARR Supporting Organisation MAKE uk Supporting Sponsor Palantir

MORNING: Opened and Chaired by **General Sir Jack Deverell** *Associate* Cityforum with **Mr Francis Tusa** *Editor* Defence Analysis

09.30 – 10.50 Session One:

Keynote address: what do we mean by innovation and where and how should we prioritise for success in an information environment?
General Sir Chris Deverell *Commander JFC* MOD

Followed by Q&A

How the United States approaches innovation in the emerging information environment
Ms Teresa Shea *Executive Vice President, Technology* In-Q-Tel

A private sector viewpoint
Mr Mark Phillips *Head of Government Affairs* Lockheed Martin UK

Followed by a round table discussion

10.50 COFFEE

11.10 – 12.45 Session Two: Business, innovation and the acquisition process – how can defence and the nation gain the most benefit?
Moderated by **Mr Francis Tusa**

Challenges and ways forward
Air Vice-Marshal Simon 'Rocky' Rochelle *Chief of Staff Capability (RAF)* MOD

Ways forward: a defence industry viewpoint
Mr Michael Christie *Director Future Combat Air Systems* BAE Systems

How an investor sees innovation
Mr Nick Kingsbury *Partner* Amadeus Capital

A view from outside defence
Mr Toby Jones *Head of ACE* (*Accelerated Capability Environment*) OSCT, Home Office

Managing complex interdependencies
Mr Fraser Hamilton *VP for Global Alliances* Boxarr

Followed by a round table discussion

The organisers reserve the right to amend the programme at any time

12.45 LUNCH

AFTERNOON: Chaired by **Air Marshal Edward Stringer** *Director General* Joint Force Development and Defence Academy MOD and **Professor Paul Cornish** *Chief Strategist* Cityforum

13.45 – 14.15 **Lunchtime Session: Behaviours and capability – the 'how' and 'what' of innovation in defence**
Opened and Chaired by **Air Marshal Edward Stringer** *Director General* Joint Force Development and Defence Academy MOD

Ms Clare Cameron *Director of Defence Innovation* MOD

Followed by Q&A

14.15 – 15.40 **Session Three: Thinking through the achievement and maintenance of information advantage – what do we actually need to do?**
Opened and Chaired by **Air Marshal Edward Stringer**

Brigadier Sara Sharkey *Head* Application Services and DevOps ISS
Mr Ed Gillett *Director Defence* BAE Systems
Wing Commander Keith Dear *Chief of the Air Staff's Fellow* Oxford University
Professor Michael Mainelli *Executive Chairman* Z/Yen Group and *Member* City of London Corporation

Followed by a round table discussion with comments from **Ms Teresa Shea**

15.40 TEA

15.55 – 17.30 **Session Four: Increasing effect in conflict – in and beyond the grey zone**
Moderated by **Professor Paul Cornish**
Opened by **Air Marshal Edward Stringer**

Force design for capability in the grey zone and beyond
Major General Robert Magowan *ACDS (Capability and Force Design)* MOD

Issues in the grey zone
Mr Chris Donnelly *Co-Director* Institute for Statecraft

How the development and exploitation of AI may help us in the grey zone
Mr David Tagg-Oram *Artificial Intelligence and Data Programme Director* Royal Navy

Cyber issues
Ms Wendy Noble *SUSLO* United States Embassy, London

Conflict via the internet
Mr Carl Miller *Research Director* Centre for the Analysis of Social Media (Demos)

Followed by a round table discussion with conclusions from **Air Marshal Edward Stringer** and **Professor Paul Cornish**

17.30 CLOSE

The organisers reserve the right to amend the programme at any time

cityforum cutting through

Intelligent Defence - Maximising Smart Power and Public Value

A programme of round tables, analytical papers and conclaves arranged by Cityforum in association with the Development, Concepts and Doctrine Centre of MOD (March to September 2019)

Second Round Table – How can we do it?

11 July 2019 – PwC UK, 7 More London Riverside, London SE1 2RT

Agenda

Principal Sponsor BAE SYSTEMS

Co Sponsor LOCKHEED MARTIN

Hosted by pwc

Supporting Sponsor Palantir Technologies

Supporting Organisation MAKE uk The Manufacturers' Organisation

Chaired by: The Honorable Franklin D. Kramer *Distinguished Fellow* Scowcroft Center for Strategy and Security - Atlantic Council (*former Assistant Secretary of Defense for International Security Affairs)*
Mr Edward Lucas *Columnist* The Times and *SVP* Center for European Policy Analysis (CEPA)
General (Ret'd) Sir Jack Deverell *Associate* Cityforum

09:00 – 09:05 Welcome by Mr Marc Lee *Chairman* Cityforum and Mr Roland Sonnenberg *EMEA Aerospace and Defence Sector Lead* PwC UK

09:05 – 10:15 Overview Session

Chaired by The Honorable Franklin D. Kramer

The military contribution to fusion of effort and delivery of effect
General Patrick Sanders *Commander* JFC MOD

What degree of fusion is achievable?
Mr Paul Spedding *Head of Pre-Sales Defence* BAE Systems

The experience of allies and of the NATO Alliance in delivering fusion of effort
The Honorable Franklin D. Kramer

Followed by a round table discussion opened by Air Marshal Edward Stringer *Director General* Joint Force Development and Defence Academy MOD

10:15 – 11:20 Session One: Maximising capability for intelligent defence

Chaired by The Honorable Franklin D. Kramer

Opened by Air Marshal Richard Knighton *Deputy Chief of the Defence Staff (Military Capability)* MOD and Mr Peter Ruddock *Chief Executive* Lockheed Martin with Dr Simon Cholerton *Chief Scientific Adviser* MOD

Followed by a round table discussion featuring the session speakers together with Mr Conrad Prince *Former Cyber Security Ambassador* UK Government, Dr Mariarosaria Taddeo *Deputy Director of the Digital Ethics Lab* Oxford Internet Institute and Brigadier Kevin Copsey *Head Future Force Development, Directorate of Capability* British Army

11:20 COFFEE

11:35 – 13:00 Session Two: Building engagement and the will to contest as the nature of conflict changes;

providing for domestic security
Chaired by Mr Edward Lucas

Recruitment, retention and community engagement
Ms Madeleine Moon MP *Member of Defence Select Committee* House of Commons

The national will to fight and the build-up of public engagement
Professor Paul Cornish *Chief Strategist* Cityforum

The law and the soldier
Mr Steven Kay *QC* 9 Bedford Row

Thinking about domestic security and resilience
Sir David Omand *former National Security Co-ordinator* and *Visiting Professor* King's College London

The role and organisation of the Police in domestic security
Ms Olivia Pinkney *Chief Constable* Hampshire Constabulary

Followed by a round table discussion opened by Mr Francis Tusa *Editor* Defence Analysis

13:00 – 13:30 Pre-Lunch Session: How to gain the most benefit from the human resources available to UK Defence
Chaired by General (Ret'd) Sir Jack Deverell

The Rt Hon Tobias Ellwood MP *Parliamentary Under Secretary of State and Minister for Defence, People and Veterans* MOD

13:30 LUNCH

14:30 – 17:00 Session Three: Intelligent defence, smart power and the national interest
Chaired by The Honorable Franklin D. Kramer and Mr Edward Lucas

Gaining and maintaining information advantage
Lieutenant General James R. Hockenhull *Chief of Defence Intelligence* MOD and
Mr Ed Gillett *Director Defence* BAE Systems

New situations and new thinking
Mr Edward Lucas

Making our alliances and relationships work to best effect – UK/USA/Europe
The Honorable Franklin D. Kramer

The national interest: Making the case for defence (Economic climate, changing politics, CSR)
Sir David Omand, Mr Mark Thompson *Director Sustainability* PwC UK, Mr William Keegan *Senior Economics Commentator* The Observer and Mr Francis Tusa

Followed by a round table discussion including comments by Brigadier Julian Buczacki *Commander 1ISR Brigade* British Army and conclusions from Major General Mitch Mitchell *Director* DCDC, Professor Paul Cornish, The Honorable Franklin D. Kramer and Mr Edward Lucas

16:50 – 17:00 Closing Comments General (Ret'd) Sir Jack Deverell and Ms Lynne Baber *UK Defence Practice Lead* PwC UK

17:00 – 18:00 EARLY EVENING RECEPTION

18:00 CLOSE

The organisers reserve the right to amend the programme at any time

Hosted by CISCO | BT

Conclave Discussions

6 September 2019 (morning session) at BT Tower, 45 Maple Street, London W1 - 10.00am to 12.30pm

Conclave 1: Technology in Conflict - what are we now facing?

In *2020: World of War?*, an analysis of trends in international security and the strategic responses required, Paul Cornish and Kingsley Donaldson noted that 'the international security picture of the 21st century is unlikely to be organized by one salient, overriding strategic concern in anything like the way of the Cold War.' In other words, the relatively stable, monolithic structures of the Cold War have given way to an international security environment in which conflict appears to be more diverse in character, more dispersed in origin and generally less susceptible to political and strategic management.

Conflict is also fast acquiring a notable – and often bewildering – 'technological edge'. There is something unsurprisingly 'human' about the relationship between conflict and technology; ever since flint-tipped weapons were invented in the palæolithic period, humans and their ancestors have always used ingenuity and technology to create advantage in battle. Tellingly, in the modern industrial era, technology is often described as 'enabling' or 'multiplying' the military effort. But by some accounts the 21st century 'technological edge' is more revolutionary than evolutionary, perhaps even becoming 'post-human' to the extent that it subverts the human role in many aspects of conflict, if not replaces it altogether.

If a technological revolution is indeed underway then its implications could be very far-reaching. At the highest levels of politico-military strategy, we could be in need of a complete rethink as to the purposes, modalities and management of modern conflict. Then there are questions to be asked about the invention, design, production and ownership of modern military technology and the purposes to which such innovations might properly be put. With these thoughts in mind, the first Conclave in the 2019 Intelligent Defence series addresses the following questions and themes:

Themes

- How are we adapting traditional, territorially focused thinking about armed conflict to the prospect of 21st century 'technical conflict'?
- What is the nature and purpose of military operations in the so-called 'new dimensions' of space, cyberspace and the electromagnetic spectrum?
- Who has access to these 'weapons'?
- How can conflict in these environments be prevented, deterred, managed and de-escalated? Can the defence acquisition process be made more adaptable to meet new and evolving requirements? Can Virtual Design and Construction ensure that acquisition is not only more efficient (and carries less risk) but also more responsive to emergent threats and challenges?
- ICT also introduces the 'cognitive/information dimension' of warfare – what is 'information advantage' and how can it be won?

Agenda

10:00 to 12:30 - Conclave Discussion

The organisers reserve the right
to amend the programme at any time

Opening view: How are we adapting?
Air Marshal Richard Knighton *Deputy Chief of the Defence Staff (Military Capability)*

Issues in space, cyber space and the electromagnetic spectrum
Air Commodore Phil Lester *Head of Doctrine, Air Space and Cyber* DCDC
Dr Matthew J Broadhead *Principal Adviser to the Space Programme* Cyber & Information Systems Division, DSTL

Conflict in cyber space
Dr Mariarosaria Taddeo *Deputy Director of the Digital Ethics Lab* Oxford Internet Institute

Disruptive and transformational innovation: thoughts on adaptable acquisition, re-purposing mature tech from other industries, and user-centred design
Lieutenant Colonel Pete Williams *Head of jHub Defence Innovation* JFC

Emerging technology in conflict - response and preparation
Ms Amy Ertan *Cyber Security Centre Researcher* Royal Holloway, University of London

Thinking around the acquisition of adaptable platforms and approaches
Comments from industry participants, including BT

Prevention, de-escalation and deterrence
Professor Paul Cornish *Chief Strategist* Cityforum

Followed by a discussion moderated by Air Marshal Richard Knighton and Professor Paul Cornish

The organisers reserve the right to amend the programme at any time

Intelligent Defence - Maximising Smart Power and Public Value

A programme of round tables, analytical papers and conclaves arranged by Cityforum in association with the Development, Concepts and Doctrine Centre of MOD (March to September 2019)

Hosted by CISCO | BT

Conclave Discussions

6 September 2019 (afternoon session) at BT Tower, 45 Maple Street, London W1 – 13.45 to 16.15

Conclave 2: Technology Futures – what might we face and how should we manage the response?

Conclave 2 makes a closer and more critical examination of the supposed 'technological edge'. Weapon systems that might have been considered the stuff of science fiction just years ago are now science fact. Research into electromagnetically powered cannons (or 'railguns') suggests that these devices could offer far greater range and kinetic impact than conventional direct - and indirect-fire guns using chemical (i.e. combustible) propellant. Directed energy weapons such as high-powered lasers are already being deployed on warships for air defence and anti-drone purposes. Other developments such as unmanned aerial vehicles (UAVs) and autonomous weapon systems (AWS) go one technological step further by supplementing or, in some cases, supplanting the role of the human combatant. The prospect of the hybrid human/robotic combatant is enabled by developments in artificial intelligence (AI) and human-machine learning (HML). And very rapid advances in the scope and speed of information processing, especially with the prospect of functioning quantum computing (QC), also suggest that the traditionally human functions of command, control, communications and intelligence (collation and assessment) will increasingly be undertaken by machines.

The technological future – some of which appears already to have 'arrived' – calls for carefully grounded, yet at the same time open-minded analysis. We need a clear understanding as to those technological changes that are already in train, those that are imminent and those that might be a more distant prospect. Which of these are threats, and which are opportunities? What is also required is some appreciation that governments and armed forces might be confronted by unanticipated, disruptive innovation. Finally, there are questions of agency and responsibility to consider.
Conclave 2 addresses the following questions and themes:

Themes

- What technological possibilities and challenges lie in the distance or over the horizon (e.g. AI, HML, QC)?
- How should government both manage (predictable) technological change and respond to (unexpected) technological challenges?
- When we describe these technologies as 'challenges', do we overlook the compensating opportunities and benefits they will also bring?
- Is the relationship between public and private interests optimally configured? Is the private sector fully involved and willing to take risk in preparing for long term technological change? Is there scope for public/private risk-sharing in defence R&D? Could venture capital have a role to play?
- Is innovation fully understood and prioritised by the public sector and by business?
- In what ways can government use its management of/response to technological change in a positive, proactive way, as a lever of national (and allied) power and influence?
- In what ways can government use its management of/response to technological change in a positive, proactive way, as a lever of national (and allied) power and influence?

The organisers reserve the right
to amend the programme at any time

Agenda

13:45 to 16:15 - Conclave Discussion

A comment from defence science
Dr Chris Moore-Bick *Head of Policy, Strategic Research & International Engagement* Defence Science and Technology MOD

Maximising responsiveness in a period of limited budgets
Air Commodore Phil Lester *Head of Doctrine, Air Space and Cyber* DCDC

Adaptable innovation
Air Commodore Lincoln Taylor *Head, RAF Rapid Capabilities Office* Royal Air Force
With comments from industry participants

Thinking about long term challenges and meeting them
Dr Kimberly Tam *Research Fellow in Cyber Security* University of Plymouth

Changing science and security – a chemist's appraisal
Professor Matthew Davidson *Director* Centre for Sustainable Chemical Technologies, University of Bath

People and futures
Ms Nicola Morrill *Principal Adviser for People Innovation* DSTL

Discussion moderated by Professor Paul Cornish *Chief Strategist* Cityforum

The organisers reserve the right to amend the programme at any time

Intelligent Defence - Maximising Smart Power and Public Value

A programme of round tables, analytical papers and conclaves arranged by Cityforum in association with the Development, Concepts and Doctrine Centre of MOD (March to October 2019)

Conclave Discussions

19th September 2019 at Pivotal, The Warehouse, 211 Old Street, London EC1V 2NR - 09.30 to 12.00

Hosted by Pivotal

Conclave Three: Civil Contingencies and Domestic Security

The past 24 months have brought renewed attention to the physical protection of the United Kingdom's people, borders and territory, and to ensuring the resilience and continued functioning of the country's critical national infrastructure (CNI). March 2018 saw what was suspected to be a Russian use of chemical weapons on UK soil. The detection, prevention and management of hazardous migration into the UK across the Channel has long occupied the UK Border Force, HM Coast Guard, the Immigration Enforcement division of the Home Office, the National Crime Agency and elements of the Armed Forces. The CNI also appears highly vulnerable. The misuse of small drones around major airports disrupts flying schedules, costs money and could possibly result in a major accident. The 'Wannacry' ransomware attack in May 2017 (considered to have originated in North Korea) reportedly affected one third of National Health Service (NHS) Trusts, caused the cancellation of 19,000 medical appointments and cost the NHS some £92m in disruption of services and in the cost of IT security upgrades and improvements.

While the UK has spent much of the past two decades improving its civil contingencies apparatus and strengthening the resilience of its CNI, the incidents mentioned above go to show that there is more to be done. This a complex problem. On the one hand, some challenges to UK domestic security and resilience have origins within the UK, while others have foreign sources. Some have both. On the other hand, the response to these challenges does not fall easily and exclusively within the competence of any single government department or agency; cross-governmental collaboration is essential. The third Conclave in the Intelligent Defence series therefore asks not only what is at stake and whether the UK is sufficiently attuned to the risks of attack against/breakdown of civil society, but also whether we are prepared – intellectually, materially and organisationally – to manage these risks. The Conclave addresses the following themes and questions:

Themes

- The resurgence of interest in domestic security and in the protection of the territory, infrastructure and interests of the United Kingdom against attack. How might GDP be affected by damage to the UK domestic infrastructure?

- What are the challenges to UK domestic security and how vulnerable is the UK to a disabling attack against the CNI or even to the breakdown of civil society?

- Which government departments/agencies are responsible for domestic security, resilience and recovery and how/how well are they coordinated? To what extent does the UK Fusion Doctrine contribute to planning and preparation in this field?

- Can/should the private sector be considered an 'agency in its own right', given that much of the UK digital CNI is privately owned?

- What is the net assessment of UK preparedness and resilience in the face of domestic security risks?

The organisers reserve the right
to amend the programme at any time

cityforum
cutting through

Agenda – Conclave Three

Welcome by Mr Marc Lee *Chairman* Cityforum

Opened and chaired by Ms Mary Calam *former Director General Crime & Policing, Director National Security* Home Office and *Associate* Cityforum

Working together for domestic security – a view from the police
Chief Constable Charlie Hall *Chief Constable* Hertfordshire Constabulary

Working together for domestic security – a view from the military
Colonel Paddy Ginn *Deputy Assistant Chief of Staff* Headquarters Standing Joint Command

Protecting the military
Group Captain James Penelhum *Principal Security Adviser* Royal Air Force

Collaborating for resilience - a view from Greater Manchester
Mr Karl Astbury *Senior Policy Adviser* Greater Manchester Resilience Unit

The contribution of the private sector
Comments from attending industry participants

Summing up
Professor Paul Cornish *Chief Strategist* Cityforum

The organisers reserve the right to amend the programme at any time

Intelligent Defence - Maximising Smart Power and Public Value

A programme of round tables, analytical papers and conclaves arranged by Cityforum in association with the Development, Concepts and Doctrine Centre of MOD (March to October 2019)

Conclave Discussions

19th September 2019 at Pivotal, The Warehouse, 211 Old Street, London EC1V 2NR - 13.30 to 16.00

Hosted by Pivotal

Conclave Four: The Purpose of Armed Force

Cityforum's 2019 Intelligent Defence series examines a wide array of challenges to UK national security. The fourth and final Conclave in the series examines more closely the role of the country's armed forces in responding to these challenges. What are the particular problems that the United Kingdom's armed forces are expected to solve and which of these problems can be solved by the armed forces acting independently, without the assistance of other branches, departments and agencies of government?

As well as being a practical question, the 'purpose of armed force' also invites discussion of the triangular, constitutional relationship between government, armed forces and society. When preparing for national security and defence, do we have the right balance of initiative, authority and responsibility between armed forces and government? For example, it has become fashionable to use the term 'hybrid warfare' when describing threats to UK national security. Yet while 'hybrid' might be descriptively useful, 'warfare' arguably homogenises and simplifies the complexity of both problem and response. Writing in 1966, Abraham Maslow observed pithily "I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail." Then there is the third part of the triangle to consider. Does the public understand the armed forces and what they do? After all, if military force is to be the last resort (or, more modishly, the 'backstop') in UK foreign, security and defence policy, then surely the UK public must be convinced of its value and relevance and must be willing, ultimately, both to support the commitment of public funds and to accept the personal, physical risks of military service. The final Conclave of Intelligent Defence 2019 discusses the following topics and questions:

Themes

- The international security/strategic landscape is in flux. Some features of the landscape are familiar – e.g. the behaviour of adversarial and potentially hostile states prompting warnings of a 'new Cold War'. Other features are less familiar, such as the emergence of non-state organisations as users of sophisticated armed violence for ostensibly state-like goals.

- The challenge seems to be less conflict, per se, than competition, often below the legal threshold of armed conflict, and might thus be perceived to require a response that differs from the traditional role of national armed forces.

- There has been much talk of 'hybrid warfare' as an organising principle with which to meet these developments. But would 'hybrid policy' be more suitable, whereby military preparation and deployment (on intervention operations, for example) are but one component of a more comprehensive and nuanced posture for the analysis of, and response to, security challenges?

- How well – and how effectively – are the various levers of national power (including the armed forces) configured to compete in this so-called 'grey zone'?

- Is the fundamental and distinctive purpose of armed force – the organised and decisive use of violence for national interests – being diluted? How best can understanding of the role of armed force be communicated to broader society, and can the public be convinced?

- The effective and sustained exercise of national power requires the efficient use of limited national resources. Is there scope for 'up front' investment in order to achieve longer term efficiency savings, particularly in defence?

The organisers reserve the right
to amend the programme at any time

cityforum
cutting through

Agenda – Conclave Four

Welcome by Mr Marc Lee *Chairman* Cityforum

Opened and chaired by Professor Paul Cornish *Chief Strategist* Cityforum

Does the UK have the 'will to fight'?
Professor Paul Cornish
with a comment from Lieutenant Colonel Mark Berry *Commanding Officer* Household Cavalry Regiment

Thinking about operations
Commodore Rhett Hatcher *Deputy Director (Military) for International Security* MOD

What does the public think about defence?
Dr Catarina Thomson *Senior Lecturer in Security and Strategic Studies* Exeter University

What does the public think about defence? A BAME perspective
Dr Mohammed Ali *CEO* QED Foundation and Ms Adeeba Malik *Deputy CEO* QED Foundation

Industry perspective
Mr Paul Spedding *Head of Defence Solutions* BAE Systems Applied Intelligence

Are we preparing our people sufficiently?
Air Commodore Paul O'Neill *Head of People Strategy* MOD

Conclusions
Brigadier Ewen Murchison *Head of Futures and Strategic Analysis* DCDC
General Sir Jack Deverell *Senior Associate* Cityforum

The organisers reserve the right to amend the programme at any time

Intelligent Defence - Maximising Smart Power and Public Value
A programme of round tables, analytical papers and conclaves arranged by Cityforum in association with the Development, Concepts and Doctrine Centre of MOD (March to October 2019)

Lunch Discussion – Making the most convincing argument for the public value of defence expenditure

30 October 2019 – BT Tower, 45 Maple Street, London W1T 4JZ

Agenda

Principal Sponsor BAE SYSTEMS SME Co-Sponsor adarga Hosted by BT

Chaired by: The Rt Hon the Lord Astor of Hever DL *former Under-Secretary of State for Defence* and *Defence Secretary's Adviser for Military Co-operation with the Sultanate of Oman* (morning)
Air Marshal Edward Stringer *Director General* Joint Force Development and Defence Academy MOD (afternoon)

11:45 – 13:30 Morning Session

Welcome by Mr Marc Lee *Chairman* Cityforum

Opening contribution from the chair – defence, international engagement and influence
The Rt Hon the Lord Astor of Hever DL

Keynote address – thinking about how to secure better public value
Sir Amyas Morse *former Comptroller and Auditor General* National Audit Office

Followed by a Q&A session

Defence – public value and public values
Ms Madeleine Moon MP *President* NATO Parliamentary Assembly and *Member, Defence Select Committee* House of Commons

Defence – innovation, capability and prosperity
Mr Nigel Whitehead *Chief Technology Officer* BAE Systems *(the vision of a prime)*
Mr Robert Bassett Cross *Founder & CEO* Adarga Limited *(benefitting from British SME innovation)*

Followed by a round table discussion

(To include a short comment from Mr James Elder *Associate* Cityforum and Dr Catarina Thomson *Senior Lecturer in Security and Strategic Studies* University of Exeter and a discussion involving all present)

13:30 – 14:15 Lunch

14:15 – 15:45 Afternoon Session

Opening contribution from the chair – the view of a senior officer
Air Marshal Edward Stringer

Communicating with the public, politicians and the Treasury
Ms Kate Adie DL *From Our Own Correspondent* BBC and *Chancellor* Bournemouth University

Fusion Doctrine – integration, efficiency and value
Mr Rod Hansen *Chief Constable* Gloucestershire Constabulary

Defence, public value and public values – what the Cityforum 2019 report tells us
Professor Paul Cornish *Chief Strategist* Cityforum

Followed by a round table discussion

(To include a short comment from Lieutenant Colonel Mark Berry *Commanding Officer* Household Cavalry Regiment and Bishop Peter Selby *former Bishop of Worcester and to HM Prisons* and a discussion involving all present)

Conclusions from General (Ret'd) Sir Jack Deverell *Senior Associate* Cityforum

cityforum
cutting through

Cityforum Limited
Clifford Farm, Bath Road
Beckington, Nr Frome BA11 6SH
tel +44 (0) 1373 831900
email info@cityforum.co.uk
www.cityforum.co.uk