cityforum
cutting through

Cityforum Intelligent Defence Series

- Report from the Conclaves and Round Table

November 2017 - July 2018

Biography - Paul Cornish, Chief Strategist Cityforum

Paul Cornish is Chief Strategist at Cityforum Public Policy Analysis Ltd, where he leads on cyber security, and director of his own consultancy company, Coracle Analysis Ltd. He has held several academic and research appointments in the field of cyber security policy: at Chatham House (where he established the institute's cyber security research project); as participant in UK-China Track 1.5 discussions on cyber security and global cyber governance from 2013; as Associate Director of the Global Cyber Security Capacity Building Centre, University of Oxford from 2013-18; as Principal Research Associate in the Department of Computer Science, University College London from 2015-17; and as Professorial Fellow in Cyber Security at the Australian National University's National Security College in 2017. He is currently a member of the Cyber Futures Council at the GLOBSEC Policy Institute, Bratislava and a member of the Programme Committee of CYBERSEC, the European Cybersecurity Forum in Kraków. Most recently he designed and directed the Wilton Park Conference, Military Operations in Cyberspace from 5-7 September 2018. He has published widely in the area of cyber security and cyber governance and is editor of the Oxford Handbook of Cyber Security, to be published by Oxford University Press in 2019.

Table of Contents

Foreword

Cityforum was encouraged by the last Chief of the Defence Staff and actively supported by the Vice Chief to develop a series of short reports, conclaves and an authoritative final round table on 'Intelligent Defence and Smart Power'.

This project, involving an independent study over more than six months from the end of 2017 to mid summer 2018, included the preparation of five positioning papers and the holding of five conclave discussions with contributions from the military, officials from MOD and other departments, as well as from industry experts and authoritative assessors from academe and the media. Each event included participants with pertinent views from the United States, the European continent and elsewhere.

Cityforum was asked to identify and bring together groups of people able to provide individual assessments of the questions that require an answer if the UK is to have a defence policy fit for purpose in the next decade and beyond.

The project concluded with a round table, attended by some 100 delegates. At this event, we explored the important elements required in intelligent defence and the projection of smart power, if the UK is to continue as a major player in the foreign policy, defence and security arenas. We were particularly asked to include discussants who do not normally participate in defence and security forums.

The whole project was meticulously supported by the Development, Concepts and Doctrine Centre (DCDC) whose Director played a constructive moderating role throughout.

The project was devised by the Chairman of Cityforum, who has been following UK Defence for five decades, and by its Chief Strategist, Professor Paul Cornish, who has a unique reputation among European academics working in this domain and whom we wish to give special thanks for his work on the creation of this report.

Cityforum is engaged with the office of the Vice Chief and the Director of DCDC on a number of themes for a continuation of work in this area in 2018 / 2019 culminating, we hope, in a further Smart Power round table in the middle of next year. Essential to this programme has been the support of several corporates who see particular merit in a study of what needs to be done, in challenging political and financial circumstances, to make sure the UK is capable of using its defence and security resources to best effect over the next decade and beyond. We are particularly grateful for the support of BAE Systems in helping us finance this project and are also grateful to Boxarr, Frazer-Nash, Fujitsu, KBR, NATS Limited and QinetiQ for their help in its realisation. We are also most grateful to the US agencies, notably the NSA, that gave us valuable international perspectives as we developed this project in a period when the UK is experiencing no little difficulty in charting a new course in especially challenging times.

Marc Lee
Chairman, Cityforum

12 September 2018

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclave One: Non-stop trouble

Tuesday 7 November 2017
Royal Over-Seas League, 5 Park Pl, St. James's, London SW1
1300 to 1700

Agenda

1300 - 1330 **Light buffet lunch**

Chaired by: Ms Bridget Kendall *Master of Peterhouse* Cambridge University & *Former Diplomatic Correspondent* BBC

Session One: **The World We Are In or Shall Be In**

1330 - 1345 Welcome and Introduction
Ms Bridget Kendall with General Sir Gordon Messenger *Vice Chief of Defence Staff* MOD &
Professor Paul Cornish *Chief Strategist* Cityforum and co-author of *2020: World of War*

1345 - 1515 Discussion including contributions from
Dr Liane Saunders *Strategy Director and Strategic Programmes Coordinator* FCO: *Managing UK interests in a world of non-stop trouble*
Mr Stephen King *Senior Economic Adviser* HSBC; *Author* 'Grave New World': *An economist's assessment of de-globalisation and nationalism*
Professor Gunnar Heinsohn *Visiting Professor* at the NATO Defense College: *Demographics and disorder*
Ms Bridget Kendall: *Do we really understand the world we are in?*

Followed by a conversation around the table

1515 **Tea**

Session Two: **Non-stop trouble – Rethinking UK Defence and Security**

1530 – 1700 Opened by Professor Paul Cornish with points from the first session followed by a discussion including contributions from
General Sir Gordon Messenger: *Intelligent defence in a difficult environment*
Ms Elisabeth Braw *Senior Consultant* Control Risks & *Non-resident Senior Fellow* Atlantic Council: *Approaching high-tech conflict in the physical world and cyber space*
Mr Asif Sadiq *Chair* London Hate Crime Advisory Board at Tell MAMA and *Ambassador* Remembering Srebrenica: *The home front and its security*

Followed by a conversation around the table including DCDC with conclusions from the Chair and General Sir Gordon Messenger

1700 **Close**

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclave One: Non-stop Trouble

Tuesday 7 November 2017
Royal Over-Seas League, 5 Park Pl, St. James's, London SW1

Reflections on the proceedings of 'Non-Stop Trouble', the first Conclave in Cityforum's Intelligent Defence Series, held on Tuesday 7 November 2017. Speakers and participants included UK Government officials and members of the Armed Forces, the private sector and representatives of policy research institutes, academia and the media. This report was prepared by Cityforum Chief Strategist Professor Paul Cornish. All contributions to the Conclave were made under the Chatham House Rule.

At one level, national security strategy is concerned with guarding against security threats and with exploiting security opportunities as they arise. Strategy is also concerned with organising national resources – diplomatic, policing, development aid, military, trade, intelligence, cultural outreach and so on – to achieve the optimal balance of capabilities in the prevailing circumstances of threat and/or opportunity. Largely concerned as it is with process, resources and activity, this understanding of national security strategy lacks one essential ingredient, however – purpose. It can be easy to conflate strategic activity and strategic purpose, but to do so is to suppose that activity (strategic or otherwise) is self-rationalising when that is rarely the case. More than simply possessing the ability to identify and then to manage both threats and opportunities, national security strategy must also have purpose – it must be motivated by a larger policy goal. In other words, a society must know what it seeks security for before it can know what it needs to be secure from, and before it can know what level of expense and sacrifice it is willing to endure to achieve that desired level of security.

It was with these very large questions in mind that Conclave 1 examined the landscape of contemporary international security and its possible evolution in the short- to medium-term future. The outlook is arguably so overcast that 'Non-Stop Trouble' – the working title for Conclave 1 – could be an unfortunately whimsical understatement. A roll-call of security threats and challenges produces a long and alarming list: single-issue and one-off terrorist attacks; co-ordinated terrorist campaigns; state-sponsored (and often deniable) terrorism; inter-state conflict (e.g. Saudi-Yemen); simmering conflict in Eastern Ukraine and a sense of strategic vulnerability elsewhere in central/eastern Europe; wars within states (e.g. Syria); the risk that CBRN weapons (chemical, biological, radiological and nuclear) might increasingly be the 'weapon of choice'; and of course the structural vulnerability to cyber-attacks of various sorts and from various sources. And these challenges are being met by institutions (national governments and inter-governmental institutions) in which public trust is at a low ebb. Approaching the end of the second decade of the 21st century, the international security future seems not only far-reaching, dangerous, risky and ever-changing, but also inescapable; the most complex range of problems to which policy and strategic solutions – often dauntingly expensive solutions – must nevertheless be found, by institutions in the midst of a crisis of credibility.

When national strategists (particularly those in the West) look to the future they might be excused for finding it a rather bleak prospect; a dystopian world of competition, contest and conflict in which security and stability will be challenged in every conceivable way (e.g. economic, environmental, technological, criminal, ideological) and on every conceivable level (e.g. global, interstate, intra-state, commercial and individual). Several of these challenges were discussed in some detail during the Conclave. The mutually beneficial globalisation of international trade and economics seems to be much less than the cosy certainty until very recently taken for granted by its largely western architects and advocates.

The West appears to have locked itself in a mentality of 'perma-austerity', with obvious implications for the strategy/resources point made above and more broadly for its international outlook. In one celebrated case a form of anti-internationalist, anti-free trade populism, if not protectionism, appears to have been embraced wholeheartedly (the United States under President Trump). And in the case of the United Kingdom post-Brexit, the goal seems to be to remain fully engaged in and benefitting from the international trading economy while relying almost exclusively upon the attractiveness of its own, national market for products and services.

Within the West, and between 'the West and the Rest', there are deepening tensions between the 'have nots' and the 'have yachts' – vast (and all too public) disparities in wealth and opportunity. These tensions are already leading to human security challenges in the form of economic and political migration which, in turn, can provide an accelerant for violent political extremism, and perhaps worse. China's economy continues to expand – and with it, China's geopolitical ambitions and its insistence on joining the 'top table' in international rule-setting. While demographic pressures mount, a 'communications revolution' is underway which challenges political structures but offers little by way of a substitute, leaving traditional ideas of government and governance appearing outdated, irrelevant and untrustworthy.

Pessimism of this sort can often result in worst-case analysis which, if not understood and managed intelligently can in turn result in an exaggerated sense of crisis – if not impending apocalypse – crowding out the possibility that security challenges might well prove to be manageable and that the future will also offer plentiful opportunities for peace and prosperity around the world. But worst-case analysis can also be an intellectually respectable and, above all, practically useful device if handled carefully. Particularly in the field of national security and strategic analysis, where the consequences of failure can be high, the benefits of 'stress-testing' assumptions and expectations should be obvious – 'What if…?' Yet worst-case analysis can be reasonable and proportionate only to the extent that it is but one component of the national strategic process. And national strategy must, as suggested above, begin with purpose.

What is the UK's national strategic purpose, and how (and where) should that purpose be articulated? For some participants in the Conclave, as for many contributors to the public debate in the UK, both questions could be answered in the form of a revised 'grand strategy'; the fusion of all national means (economic, diplomatic, military etc.) to meet overarching national goals. For others, grand strategy is a tired old shibboleth from an arguably much simpler and more predictable time, when 'events' developed as expected. In the early 21st century, with international security characterised by complexity, volatility and urgency it is hard to see how any government could make political and practical sense of everything that could legitimately be said to be a national strategic concern. Perhaps international security has become a set of wicked problems too big for government – any government – to manage. If so, then surely the equal and opposite error to worst-case analysis would be to suppose, against the evidence, that international security can in fact be reduced to something more manageable and captured within a traditional and familiar policy/strategic framework. By this view, the claim that national strategy should be concerned simply with tightening the relationship between 'means' (i.e. strategic capacity – military or otherwise), 'ways' (i.e. strategic methods) and 'ends' (i.e. strategic goals) is too narrow and linear and fails to ask the vital strategic question: "Why are we taking this course of action? What national purpose does it serve?"

If government can no longer be expected to solve every strategic problem with which society is confronted, nor exploit every opportunity with which it is presented, then what is the purpose of national security strategy – and even government itself – in this 'wicked' new world order? One answer might be for government to take a vocal and visible lead in the one area in which its authority ought

to be unrivalled – in acting as the chief communicator and custodian of a national strategic purpose reduced to just two, broadly defined and adaptable objectives: the protection of interests (territorial, political, cultural etc.) and the promotion of national prosperity. This might be considered a rather limited response to the perpetual debate as to the meaning of 'national interest' – but deliberately so, and not without precedent. The essence of this approach was notably expressed in a speech by the (then) British Foreign Secretary Lord Palmerston in a speech to the House of Commons in 1848: 'We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow.' A 21st century version of the 'Palmerston doctrine' would see government encouraging and enabling the many stakeholders in national security (governmental, non-governmental, third sector, commercial and individual) to gather around this national strategic purpose. The strategic role of government (and of its national security strategy) would be clear enough; to ensure that each 'wicked problem' is met with a comprehensive and carefully orchestrated 'virtuous solution'.

Although there are grounds to be sceptical of the familiar 'ends, ways and means' formula as being too reductive for the complexity of the 21st century security environment, it is nevertheless the case that not even the simpler idea of national purpose – and not even the most 'virtuous' of solutions – is likely to amount to much without investment in practical capacity and expertise. At this point, the strategic role of government becomes more complex; it is not only the conductor of the 'national strategic orchestra', it also one of the leading instrumentalists. The most valuable and highly polished instrument in the national strategic orchestra is governmental expenditure. Here, government must find respectable and durable answers to urgent questions. Is the government spending as much as it could, or should, on the various components of national strategy? Is government spending allocated optimally, and in proportion to strategic need? Is a national defence budget of roughly two per cent of GDP adequate to the task? Should more be allocated to defence and, if so, from where should the additional spending be drawn? Is it reasonable to spend 0.7 per cent of GDP on overseas development aid, and just 0.1 per cent on diplomacy? And is government (both national and local) paying sufficient attention to its other instruments, including those intended to influence and shape the domestic security environment for the better, such as community cohesion and counter-radicalisation policies?

The largest and loudest of the government's strategic instruments – one that only government can play and without which the national strategic effort would be severely depleted – is of course armed force. Here, the challenge facing government is to find a way to modernise and prepare for a largely unknowable strategic future, and to do within spending constraints. If the United Kingdom can no longer afford large-scale armed forces sufficient to meet any conceivable military-strategic challenge (if indeed it ever could), then where should it invest? What is the optimal balance to be struck between the physical and non-physical components of the UK force posture, between the human and the technical? Can the Ministry of Defence and the Armed Forces compensate for the lack of conventional mass (i.e. the volume of naval, ground and air forces available for deployment) by investing in national and operational resilience and in network redundancy? Do UK Armed Forces work well with – and trust – their allies in Europe and elsewhere? Are UK Armed Forces an efficient strategic resource, in the sense of being 'cross-domain capable', able to respond to a wide variety of security challenges? As the traditional separation between 'peace' and 'war' becomes ever-more blurred, how effectively can the Armed Forces operate in what one participant described as 'an ongoing state of pre-conflict tension' involving both state and non-state adversaries? Or are the UK's diminishing Armed Forces being overwhelmed by so many tasks that they are fast becoming the master of none? If so, the problem then arises of a country that has forgotten that the first task of its armed forces must be to deter aggression and adventurism – a task for which its armed forces must be fully and effectively equipped.

What is also needed is a culture of innovation – but with a difference. A departure must be made from

the cause-and-effect, linear, reactive mentality in which government and the strategic establishment allow themselves the time to innovate in order to solve a given security problem as it arises, Instead, innovation must be prospective (or, indeed, innovative), such that the UK's strategic community is culturally, technologically and economically positioned to anticipate a security problem before it arises or, at least, can identify the challenge at its earliest, formative stage and can deal with it effectively and at pace.

With innovation comes the second 'I' – initiative. A large part of government's strategic role must be to convince society that its challengers do not possess all the initiative and that not every form of 'trouble' in the international security environment is the harbinger of apocalypse, or at least national collapse. A culture of 'prospective innovation' can help in this regard. If innovation can itself be as speculative, agile and open-minded as the Armed Forces and other strategic instruments are expected to be, then it should be possible to reclaim some (not necessarily all) of the initiative from adversaries and security challenges that can only be assumed to be unknowable – until, that is, knowledge of them becomes all too immediate and all-too painful.

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclave Two: Modern deterrence – what should the UK do?

Monday 11 December 2017
Royal College of Defence Studies, Seaford House, 37 Belgrave Square, London SW1

1300 to 1700

Agenda

1300 - 1330	**Light buffet lunch**
Chaired by:	Vice Admiral (Retd) Sir Jeremy Blackham *former Editor* Naval Review
1330-1345	**Opening remarks:** *Where does deterrence now fit into power projection?* Vice Admiral (Retd) Sir Jeremy Blackham *Flexibility in deterrence thinking* Professor Paul Cornish *Chief Strategist* Cityforum and & *Leader* Oxford University Harms Study
1345-1515	**Session One: New challenges to thinking about deterrence** *Deterrence in cyber conflict – what will count?* Mr Nick Ayling *Head of Cyber & Space Policy* MoD *Deterrence in hybrid war – what works?* Mr Charlie Winter *Senior Research Fellow* ICSR *& Associate Fellow at the ICCT (The Hague)* Followed by a conversation around the table
1515-1530	**TEA**
1530-1645	**Session Two: Re-thinking deterrence and state on state conflict** *Will Ballistic Missile Defence (BMD) reduce the value of nuclear deterrence?* Ms Ivanka Barzashka *Research Associate, Department of War Studies* King's College London *US thinking about the future for deterrence – where is it leading?* Dr Brad Roberts *Director, Center for Global Security Research* Lawrence Livermore National Laboratory and *former Deputy Assistant Secretary of Defense for Nuclear and Missile Defense Policy* Followed by a round table discussion with comment from Major General Mitch Mitchell *Director* Development, Concepts and Doctrine Centre and Professor Paul Cornish
1700-1705	Conclusions from Sir Jeremy Blackham
1705	**CLOSE**

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclave Two: Modern Deterrence - what should the UK do?

Monday 11 December 2017
Royal College of Defence Studies, Seaford House, 37 Belgrave Sq, London SW1

Reflections on the proceedings of the second Conclave in Cityforum's Intelligent Defence Series, held on Monday 11 December 2017. Speakers and participants included UK Government officials and members of the Armed Forces, the private sector and representatives of policy research institutes, academia and the media. This report was prepared by Cityforum Chief Strategist Professor Paul Cornish. All contributions to the Conclave were made under the Chatham House Rule.

Deterrence seems to be coming back into fashion. In one form or another, the idea features over 50 times in the UK's most recent defence review – the National Security Strategy and Strategic Defence Review, published in 2015. The review includes the insistence that 'Defence and protection start with deterrence, which has long been, and remains, at the heart of the UK's national security policy.' If deterrence has indeed been such a central, and perhaps such an obvious feature of UK policy, the cynic might wonder why quite so much attention must now be paid to something quite so self-evident. A clue emerges later in the 2015 review when mention is made of the need to 'lead a renewed focus on deterrence to address current and future threats.' In other words, the more accurate explanation for the UK's interest in deterrence is not that the idea has somehow wafted back into fashion of its own accord, but precisely the opposite; for whatever reason, interest in this important body of ideas has waned, and needs to be rekindled. The fruit of that effort is embodied in the idea of 'modern deterrence', a theme of the 2018 National Security Capability Review: 'As the world has become more uncertain and volatile, our approach to deterrence has become more comprehensive. Modern deterrence is whole-of-government in nature and strengthened by the Fusion Doctrine.'

The principles of deterrence – and indeed of modern deterrence – are not at all difficult to comprehend. Deterrence is a feature of many human activities, behaviours and relationships, ranging from the private matter of bringing up children, to society's attempts to control crime. The central idea is simple enough; at any level, and in any sector, deterrence works by promising to impose costs on a given action, either by making success more difficult or by threatening a punitive response. The perpetrator, if acting rationally, should then be convinced that the benefits of the action will be outweighed by the costs incurred or the punishment received, and will thus choose not to act as intended. It follows that the purpose of strategic deterrence is to convey the message that the benefits expected from adventurism or aggression will be outweighed by the costs and/or punishments imposed. Understood in this way, it is clear that strategic deterrence is both a passive and an active posture; deterrence is about having the capacity both to resist and to act.

Cityforum's second conclave in the Intelligent Defence series began with probably the most succinct explanation of strategic deterrence and its importance. In the pithy words of the fourth century Roman military writer Publius Flavius Vegetius Renatus, 'Si vis pacem, para bellum' ('If you want peace, prepare for war'). This seems straightforward enough although, to paraphrase a well-worn Clausewitzian aphorism, 'Everything in deterrence is very simple, but the simplest thing is difficult.' As every student at the UK's military academies and staff colleges will have been taught during the decades of the Cold War, several components must be in place for deterrence to function; often described as the 'three Cs'. First, as suggested above, the deterrer must have the capability to impose the costs he has promised or threatened. Second, the deterrer's promise must seem credible to the potential aggressor. As well

as the appropriate capability, credible deterrence also requires that the deterrer has the will – personal, political or moral – to carry out his promise, and that this can be communicated to, and understood by, the adversary. As one Conclave participant observed, 'deterrence resides in what and how opponents think – not how we think.'

But the challenge of modern deterrence is much more than a matter of dusting off Cold War staff college teaching materials. Having rediscovered its purpose and its principles, the challenge now is to reapply deterrence in a global strategic environment that is arguably far less tractable than that of the Cold War. The use of nuclear and other weapons of mass destruction (WMD) must continue to be deterred. But so must 'kinetic' force be deterred at lower levels, and particularly where there is a possibility that such confrontations might escalate to WMD use. In certain cases, the object of deterrence might be the acquisition of weapons, rather than their use – what does the experience of the Cold War offer in this respect? Then there are non-kinetic uses of what might best be described as 'soft' force – orchestrated cyber intrusions and social media campaigns, for example, which can have destructive effects and could conceivably result in the loss of territory. And finally, there is the problem of deterring so-called non-state actors such as organised criminal groups, terrorist organisations and hybrids of both, as well as those which are backed by governments acting under the veil of 'plausible deniability'. Non-state actors are not a new phenomenon, but what is of growing concern is the ease with which they (and/or their sponsors) can acquire the finance, weapons and other means to act on the global stage, often with unrestrained violence, and to influence global politics to their own ends. In some cases, non-state actors seem to have embarked upon a strategy of provocation; far from being sensitive of their own vulnerability and acting accordingly, it is as though these groups invite attack. How can deterrence be applied consistently and effectively in this turbulent mixture of old, new and unorthodox security challenges?

'Cyber deterrence' emerges as a particularly difficult variation upon an old theme. Described in the course of the Conclave as 'a domain of constant contest between adversaries', cyberspace is a notoriously opaque environment. While we might expect the fundamental cost/benefit calculus of deterrence to obtain in this, as in any other environment, it is not easy to be confident of the 'three Cs' of deterrence when the identity of an adversary might be difficult to establish, and his intentions even more so. If 'deterrence by denial' requires a country's critical national infrastructure (CNI) to be resilient to attack, then how much of these sophisticated communications and information systems must be hardened, and against what? If 'deterrence by punishment' requires the ability to act offensively (albeit reactively), then 'offensive cyber' might be as simple as 'non-permissive manipulation of data'. But could such a capability be described as strategic? Must there not also be a clear sense in the mind of the adversary that the threatened data manipulation could have adverse – and tangible – consequences? Whether passive or active, if the decisiveness of a capability cannot be communicated to any and all adversaries in a convincing manner, then the capability is simply not credible. More generally, there are (as yet) too few worked examples of cyber warfare for us to know how cyber conflict begins, how it might escalate, how it might proliferate into other strategic domains and how it might be brought to a conclusion. In a strategic environment that is highly technological yet also technologically opaque, could any government ever argue, persuasively, that if a 'technical' standard of proof (of cyber aggression) cannot be met, then perhaps a looser 'political' standard will suffice?

Cold War strategic deterrence was most certainly concerned with security and defence. But it was also part of a broader concern with making the global strategic environment stable and predictable, and as immune as possible to misunderstanding and miscalculation. If Cold War deterrence is difficult to apply in 21st century cyberspace, then so too are the various mechanisms, developed over decades, with which strategic animosities were stabilised into an adversarial partnership. The Cold War saw arms races, proxy

wars, mutual assured destruction and deterrence, but it also saw arms control, verification agreements, spheres of influence, confidence-building measures and détente. Yet the prospects for a similar, 'twin-track' approach for cyberspace seem limited. The case for a stable and predictable cyberspace is compelling enough; it would enable shared benefits to be enjoyed by those involved. But it is never enough simply to describe the benefits that might accrue from mutually self-interested collaboration; the spirit of multilateralism must be accompanied by unilateral impetus. The parties concerned must want to share, they must need the benefits on offer and they must be persuaded that there is no better or easier way to secure those benefits. Efforts by the United Nations Group of Governmental Experts on Information Security (GGE) to agree rules of behaviour for states in cyberspace ended in June 2017 without agreement on a consensus report. If 'outright failure' is an overly critical judgement of this outcome, the best that could be said of it is 'deferred success'. One proposition considered by the GGE was that certain target areas – such as a country's digital CNI – might be considered off-limits. Mutual agreement that CNI should be immune from attack would have been a clever adaptation of Cold War 'crisis stability' for the digital era. But as a result of disagreements in the GGE it is unlikely to make progress for the time being. And even if it were to come to light as a drafted treaty proposal, serious thought would have to be given to the challenges of verifying any such agreement.

The second part of the Conclave returned to the more established and familiar area of the deterrence debate – that concerning the deterrence of state-on-state conflict, particularly where nuclear weapons might be available for use. Here, the outlook is barely less encouraging than that concerning cyber deterrence, not least because the global strategic environment has shifted from being largely bipolar, during the Cold War, to being distinctly multipolar, with consideration having to be given to new 'regional challengers'. In spite, or perhaps because of its origins in the mid-twentieth century the highly-evolved and sophisticated deterrence debate is facing a crisis of scepticism. Some argue that a 'deterrence inflection point' has emerged and call for a 'new strategic synthesis of Cold War and post-Cold War environments'. Nowhere is the need for new ideas more apparent than in the relationship between missile defence and nuclear weapons. Concerned that 'the proliferation of ballistic missiles poses an increasing threat to Allied populations, territory and deployed forces', NATO allies agreed in November 2010 to develop a 'territorial ballistic missile defence (BMD) capability'. In spite of NATO's reassurances that the system was 'purely defensive and not aimed at Russia', the decision was not welcomed by Russia, who argued that the stability and predictability of their strategic relationship with NATO would be undermined.

Russia's objection echoes a peculiarity of Cold War-era deterrence doctrine that is too often overlooked; for mutual deterrence to function, the parties involved had to accept a degree of mutual vulnerability. In other words, two highly-armed adversaries were expected, counter-intuitively, to achieve strategic stability not by going to war and defeating their opponent but by making themselves vulnerable to that same opponent. To a considerable extent, therefore, mutual deterrence was, and is, concerned with trust. But in the post-Cold War environment to what extent – and with whom – should mutual vulnerability be the strategic goal? Who can be trusted, how far and what degree of verification will be required? More broadly, will the development of BMD systems improve the deterrence of missile attacks and nuclear weapon use in and around Europe? Or will such systems create a destabilising 'security dilemma' whereby one party's defensive preparations are seen as precisely the opposite by another party, resulting in an arms race and a strategic environment which becomes ever more vulnerable to misunderstanding and miscalculation?

Part of the 'new strategic synthesis' might be to accept that a multipolar world will require a more nuanced and differentiated understanding of deterrence. The United States, for example, might simultaneously pursue a Cold War-style relationship based on mutual vulnerability with Russia, reject

any idea of mutual vulnerability with countries such as North Korea and Iran, and remain undecided, at least for the time being, as to the nature of its strategic relationship with China. Although much less tidy than its Cold War antecedent, multi-modal deterrence of this sort would be more consistent with the strategic environment as it is, rather than as it used to be.

If modern deterrence is proving so difficult to implement, in circumstances both old and new, then perhaps the problem lies not with deterrence itself, but in our failure to see that we need an alternative to it. It is hard to imagine what that alternative could be, however, and until it emerges in a coherent and durable form we are left with finding ways to reconceive and reapply the long-established principles and techniques of deterrence in ways which are more appropriate to 21st century security challenges (both familiar and emergent). This must be much more than an effort at strategic archaeology, however. Deterrence must not simply be rediscovered; it must be normalised with the national, regional and international security discourse and on the broadest conceivable level, integrating all departments, functions and levels of government and including non-governmental bodies, the private sector and even individuals.

The Conclave was posed the question, 'What should the UK do?' The answer is clear enough: the UK should set out to 'normalise' deterrence as a strategic posture, as a set of capabilities (not all of them military) and as a body of ideas. As a first step, this means accepting that deterrence is neither simple nor a cost-free alternative to expensive preparations for war. Strategic deterrence is about preventing war and managing its in-built tendency to escalate. The goals of deterrence cannot be achieved without substantial investment in capability. But when, as now, the scope for financial investment is limited there is still much that can be done to make deterrence more credible. The UK should continue to emphasise the merits of cross-governmental integrated deterrence. The UK should work more closely with allies to ensure that deterrent postures are complementary. The UK's deterrence doctrine must be communicated more effectively to both the domestic UK audience and to strategic competitors. And finally, the UK should seek to enrich the body of deterrence thought by inviting 'trusted agents' from outside government to act as a critical friend to policy-making in this complex and critical area of national strategy.

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclave Three: The data tsunami

Monday 22 January 2018
Royal College of Defence Studies, Seaford House, 37 Belgrave Square, London SW1

1300 to 1700

Agenda

Principal sponsor FUJITSU **Co-sponsors** NATS

1300 - 1330 **Light buffet lunch**

Chaired by: Professor Paul Cornish *Chief Strategist* Cityforum

1330 - 1335 **Welcome**
Mr Marc Lee *Chairman* Cityforum

Session One

1335 - 1515 Discussion including contributions from

The implications of data driven defence – complexity, cost and security
Professor Paul Cornish

The data tsunami – challenges now and what may be expected over the next five years?
Professor Sadie Creese *Director* Global Cyber Security Capacity Centre University of Oxford

Overcoming the challenge of extracting meaningful insight from data - a GCHQ perspective
Mr James Babbage *Director, Analysis* GCHQ

Co-creation, innovation, and commercial aspects of the Big Data challenge
Mr Don McAll *Client Managing Director, Defence & National Security* Fujitsu

Followed by a conversation around the table to include military personnel present

1515 **Tea**

Session two

1530 - 1700 Discussion including contributions from

Understanding and mitigating the risks to government from the data tsunami?
Professor David Hand *Emeritus Professor of Mathematics* Imperial College, London

Maximising the benefit of all available data – lessons learnt from another sector
ACC Richard Berry *Communications Data Transition* OSCT Home Office

Change to defensive versus offensive approaches to data
Mr Raymond Lim *Domain Expert (Data and Information)* NATS

Followed by a conversation around the table including **Major General Mitch Mitchell** *Director* DCDC

1700 **Close**

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclave Three: The Data Tsunami

Monday 22 January 2018
Royal College of Defence Studies, Seaford House, 37 Belgrave Sq, London SW1

Reflections on the proceedings of the third Conclave in Cityforum's Intelligent Defence Series, held on Monday 22 January 2018. Speakers and participants included UK Government and House of Commons officials, members of the Armed Forces and representatives of policy research institutes, academia, the media and the private sector. This report was prepared by Cityforum Chief Strategist Professor Paul Cornish. All contributions to the Conclave were made under the Chatham House Rule

The world is flooded with digital information and data. It has been said that every second, one hour of video is uploaded to YouTube: the equivalent of one decade's worth of video being uploaded every single day. By another account, YouTube's monthly uploads are roughly equivalent to all video transmissions by all US television networks over the past 30 years. According to Mary Meeker's Internet Trends report, in 2015 something in the region of 3.25 billion photographs were uploaded every day to Facebook, Facebook Messenger, Snapchat, Instagram and WhatsApp. There could be as many as 500 million Tweets sent each day and according to the Radacati Group by 2019 we could see 246 billion emails sent each day. In 2010 Eric Schmidt (formerly CEO and then Executive Chairman of Google) claimed that every two days as much information is created as throughout the history of humanity up until 2003; approximately five exabytes (i.e. five quintillion, or 5000,000,000,000,000,000 bytes).

Responsibility for this flood of information is attributable not only to social media-obsessed human beings – there is also the Internet of Things (IoT) to consider. The IoT (or, as some prefer, the Internet of Everything) amounts to networks of sensors, devices and machines connected by an automated communications process in which data, measurements and information are transmitted to a central point for collation, monitoring, analysis and communication, all without the need for a human to be 'in the loop'. The variety of devices networked in this way seems limitless: communications equipment; domestic appliances; surveillance equipment; vehicles; health monitoring devices; energy management systems environmental monitoring equipment; industrial management systems and so on. According to Cisco by 2020 there could be as many as 50 billion such devices connected to the Internet, each generating its own telemetry.

The rate of 'take-up' of digital means recorded each year around the world, and the data tsunami which ensues can only be described as revolutionary, not just technologically but also, and perhaps more significantly, in terms of politics, economics and opportunity. And there seems no end in sight, no natural limit to this expansion. If, as we are frequently informed, the expanding global communication infrastructure not only shapes but also improves all dimensions and all levels of human life – cultural, economic, religious, diplomatic, commercial, family, individual, non-governmental and governmental etc. – then it is clear why it should be so popular; surely more take-up must be welcomed? In the UK, for example, something like one eighth of GDP has been reported to come from the digital economy, which is growing 2.5 times faster than other areas. But if the data tsunami represents economic, political and individual opportunity, it can also be a vector for challenge, insecurity, instability, crime and competition. Ironically, Tsunami was also the name given to a 'network stress tester' software application which, in certain circumstances, could be used in a denial of service attack.

For those who work in national security, intelligence and cyberspace, and for those who take a research interest in the public policy dimensions of this 'revolution', the question is how to discriminate between

the acceptable and the unacceptable aspects of this data revolution? As the volume of data and information being transmitted increases, as the number of sources multiplies and as the speed of transmission quickens, the third Cityforum Conclave asked whether, and how effectively, governments can discern challenge from opportunity. When dealing with cyber security challenges what constitutes legitimate action on the part of government? Who owns these data and telemetry? What rights and protections should attach to ownership? And critically, does government have the competence and agility to surf the data tsunami and is public-private sector collaboration effective?

The first session of the Conclave examined the data revolution from the perspective of national security and defence. What are the strategic and cost implications of data-driven defence? What future challenges can be foreseen? How can government identify those data that are useful and actionable, but that are being carried along in a flood of information that in national security terms is otherwise useless and valueless, and perhaps a deliberate attempt to distract? And finally, what are the commercial aspects of the data challenge?

The defensive and offensive use of information is not new to national strategy; electronic attack and counter-measures were familiar in the twentieth century. But the volume and velocity of data and the sophistication of its exploitation is changing almost overwhelmingly. Information and communication are no longer simply a 'multiplier' to kinetic warfare. The balance has changed. One contributor saw the problem in terms of 'three zeros': reaction times have been reduced to seconds ('zero day'); the origins of an attack might be opaque ('zero source'); and the intent of the attacker might not be identifiable ('zero intent'). This is a fundamental challenge to strategic doctrine and responses based on intelligence, discrimination and proportionality. How is military stability to be maintained in the face of such asymmetric attacks where the initiative appears always to lie with the unprincipled aggressor? And how credible is the threat of a conventional armed response to a cyber-attack (a feature of NATO doctrine since the Warsaw Summit in 2016). More broadly, is a military posture (of any sort) the best means with which to deter a cyber 'posture' (whatever that might be), without having to make so-called 'cross-domain' threats that might not always seem credible? Conclave 2 in Cityforum's Intelligent Defence series discussed the importance of strategic communication in deterrence, both in signalling a position and in creating sufficient uncertainty to make the gaming of positions and responses more difficult. But how is it possible to deter the whole range of cyber attackers including states, criminals, individuals and possibly even machines; and – crucially – whose job is this?

Not unreasonably perhaps, much of the national security discussion seems to be fixed on the need to keep up with the data explosion and to be able to scale up capabilities as and when necessary. But as society's attack surface continues to grow, seemingly with no natural limit, so it becomes ever harder to understand what matters, and why, and to prioritise threats, risks and responses accordingly. International standards on risk have barely changed, suggesting that the problem might be compounded by a leadership challenge which is generational, with senior decision-makers and management boards finding it difficult to know when and how to react.

Defence thinking, and planning, is concentrated at the edges of systems, but often with too little understanding of the structural interdependence both of society's vulnerabilities and of the corresponding layers of defensive systems needed. As such, the effectiveness of society's defensive posture might remain unknown until tested. The insider threat also remains a problem, even (or, perhaps, especially) inside the cloud. Knowledge of the skill sets, and experience acquired in attack is vitally important to organisations trying to build their defences, but there may be doubts about the long-term loyalties of the holders of hacking expertise; 'white hat' hackers have been known to sell zero-day exploits on the internet. Vulnerable organisations might therefore have to make an unenviable choice between

capability and loyalty. The major growth area in the near future is likely to be in machine learning and artificial intelligence (AI); but these are techniques rather than solutions. They will bring advantages to both attackers and defenders, the possibility of new crimes such as cyber manipulation of stock prices, and the potential to game defensive systems and to hide sophisticated probes in the noise created by blunter, more overt attacks. The attack ecosystem will become more diverse and require a scaled-up approach to resilience and redundancy. More sophisticated protection will be required for individuals as they become more vulnerable to so-called 'human hacking' or social and behavioural engineering, and more effort will be required in the detection of anomalous signatures.

The data tsunami is not exclusively a matter of threat, however; it also offers a revolution in analytical capability. Intelligence collection occurs in layers, covering the communications of hostile states and their military, personal communications between individuals and in machine-to-machine communications for purposes such as counter terrorism. Analysis looks to discover new targets and to pursue those that are known; the first of these presents the more complex challenge, largely because of the increasing availability of encryption. The IoT might help with known targets, however. Big data is also an enabler for defensive work, as the UK Cyber Security Information Sharing Partnership (CiSP) demonstrates. Nevertheless, the terrorist attacks in London in 2017 made a vivid case for a step change in the capability to exploit data. This is not straightforward because of the legal and ethical considerations that weigh heavily on governments regarding privileged access to sensitive and personal information. This argues for effective oversight of government use of capabilities rather than fettering the powers of government, a self-denying ordinance which would hand further advantage to adversaries with fewer constraints and greater freedom to experiment.

The value of data is contextual rather than intrinsic. Value arises from the uses (and misuses) to which data can be put, the questions it can answer, the insight it can provide and increasingly from the power of prediction. Defined in this way, the search for value is iterative and hypothesis- or question-led. Few organisations understand what data they hold, let alone have an evidenced view of which data can be unlocked and which needs to be protected. It helps also to understand what it is not necessary or valuable to hold or process. Finding the value in data requires partnership ('co-creation') between the holders of the data and those with the skills and capabilities to work with it. Here, an interesting contrast arises with traditional strategic thought and planning. War fighting involves capabilities that must, ultimately, be visible and tangible. But how can the value (and power) of data and associated capabilities be visualised? What is the digital world equivalent of the real-world chart or map – what are 'digital geopolitics'? And while there has been heavy investment in protecting the military's command, control and combat systems, their logistics chain remains highly dependent on external organisations and systems and therefore vulnerable.

In its second session, the Conclave took account of the perspective of other government departments and agencies. Two broader, structural problems were noted. First, public understanding of the security of data is limited and there is too little recognition of distinctions between individually sensitive personal data and the power of aggregated data which may be very substantially anonymous. Second, there appears also to be a resistance among government agencies to linking systems and sharing data flows even where trustworthy systems exist.

In the law enforcement environment, the importance of data – particularly communications data – is well recognised. However, the volumes, velocity, variety, veracity, validity and vulnerability together with the range of threat vectors and with difficulties in visualisation (the 'V8 model') make this a challenge as well as an opportunity. There have been examples in the press where the sheer volume of data has led to imperfect disclosure exercises and an undermining of the probative value of data and any insights

gathered from it. Each year, law enforcement agencies face a doubling of referrals from overseas. Meanwhile the criminal opportunities also increase with technology freely available to spoof identities and content (including voice) and to falsify SSL certificates. Police forces have been preoccupied with the idea of identity and the 'golden nominal' but may need to focus on less complete identities and on general threats rather than specific individuals. Air Traffic Control is an example of a highly data-driven service where there has been heavy investment in capability to support decision-making. There is tension between active commercial exploitation of the data and the need for robust and well protected systems for core trusted business. The balance between data access and security derives from the strategic view of the organisation concerned and should be supported by appropriate governance and assurance. Judgements are also necessary on the quality and coverage necessary to meet operational needs (which include the customer needs of defence and security). How much is enough? Are there circumstances in which the '80/20' Pareto principle might apply to data analysis, accepting just 80% of investigative value from as little as 20% of possible inputs?

Leadership in cyber security remains problematic, particularly in hierarchical and command and control organisations such as the armed forces and the police which broadly grow leadership talent from within. It may require strong 'analogue' leaders to stand back from what they do not understand and to allow greater freedom to those (usually younger) who do. This means more risk, greater willingness to fail (and acceptance of 'good faith failure' by senior colleagues), as well as the acceptance that outcomes may not be predictable. Rotating emergent leaders through different national security/defence and private sector roles can widen understanding. And organisations, including defence and security, must for their part recruit and manage greater cognitive diversity. There was strong agreement on the importance of interdisciplinary teams and perspectives drawing on the life sciences, psychology and philosophy as well as computer science.

Defence struggles with the expectation that it will be effective in the new cyber domain whilst still providing kinetic capability. The police face burgeoning on-line crime, but the public still expects to see officers on the street. There may, however, be some new opportunities such as exploitation of the IoT to support resilience and civil defence. There was recognition that the UK government struggles with consistent and effective data management across the range of its activities; but the Conclave was not convinced that the answer lay in a stronger and more directive central hand in government. Although the e-Estonia model is admired it would be difficult to translate into larger, more established states and economies.

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclaves Four and Five

- **International by design**
- **Economics of Force**

Wednesday 2 May 2018
Royal College of Defence Studies
Seaford House, 37 Belgrave Square, London SW1

Agenda

1030 – 1600

Chaired by: Professor Paul Cornish *Chief Strategist* Cityforum and co-author of *2020: World of War*

1030-1035 **Welcome and Introduction**
Professor Paul Cornish

Session One: International by Design

1035 - 1245 Discussion including contributions from

What does International by Design mean to the MOD?
Mr Peter Watkins *Director General Strategy and International* Ministry of Defence

The US and the UK, the UK and the US
Dr Jan Halper-Hayes *Adviser to the US Administration and ex-VP* Republicans Overseas UK

International by design – with whom and what does history tell us?
Mr Francis Tusa *Editor* Defence Analysis

How can International by Design help the defence industry? What needs to change?
A discussion with industry representatives present

Followed by a conversation around the table with an opening comment on '*International by Design and future UK strategy*' by **Major General Mitch Mitchell** *Director* DCDC followed by comments from **Mr Tim Ripley** *Associate* Cityforum and *Correspondent* Janes Defence Weekly and the Sunday Times and **Mr Marc Lee** *Chairman* Cityforum and author of '*The future of banking in the world economy to 2050*', prepared for DCDC in March 2017

1245 - 1345 **Light buffet lunch**

Chaired by: Professor Paul Cornish

Session two: Economics of Force

1345 - 1600 Discussion including contributions from

Thinking about the economics of force
Mr John Ogilvie *Lead, Defence Economics* MoD

What does the UK defence budget tell us about the economics of force?
Mr Peter Cook *Managing Director* Defence Analysis Services

Stress points in UK defence expenditure
Mr Jeremy Lonsdale *Director* NAO

Economics, strategy, capability – clarity and the ability to meet the requirements
Mr Oliver Welch *Head of Defence, Aerospace and Security Policy* EEF and industry representatives present

The economics of force – how is it seen in Westminster?
Ms Eleanor Scarnell *Clerk to the House of Commons Defence Committee* UK Parliament

Changing warfare and the economics of force
Professor Paul Cornish

Followed by a conversation around the table including industry comment and further comment from **Mr Tim Ripley** and **Mr Marc Lee,** opened by and with a final conclusion from DCDC by **Lt Col RM Andrew Fergusson** *DAR Delivery and Development Lead* DCDC

1600 **Close**

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclave Four: International by Design

Wednesday 2 May 2018
Royal College of Defence Studies, Seaford House, 37 Belgrave Sq, London SW1

Reflections on the proceedings of the fourth Conclave in Cityforum's Intelligent Defence Series, held on Wednesday 2 May 2018. Speakers and participants included UK Government and House of Commons officials, members of the 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 Conclave were made under the Chatham House Rule.

'International by Design' – the theme of the fourth Conclave in Cityforum's Intelligent Defence series – has become a prominent feature in the UK defence debate. One participant suggested that the essence of the idea is not new; UK defence has always been so 'international' that it is now 'in the DNA'. Over many decades, Britain's armed forces have indeed become almost instinctively receptive to the principles and practicalities of strategic and operational collaboration with allies and partners: the UK has been a prominent member of NATO, a standing politico-military alliance, for 69 years; has been a major contributor to UN peacekeeping missions over many years; has taken a leading role in multinational and European coalition operations; is accustomed to cross-border collaboration on defence equipment development and procurement; has a global network of defence attachés, advisors and training teams; and its highly regarded military academies and staff colleges admit students from around the world.

In formal terms, the origins of 'International by Design' (IbD) can be found in the 2010 Strategic Defence and Security Review: 'Alliances and partnerships will remain a fundamental part of our approach to defence and security. Internationally, we rarely act alone.' From the outset, the intention was to build 'international' into all aspects of security and defence planning, rather than introduce it belatedly, or as an afterthought. Another feature of the UK's evolving position was set out in the accompanying National Security Strategy: 'we need to draw together, and use, all the instruments of national power, so that the sum of the British effort is much bigger than its component parts [emphasis added].' From the perspective of UK defence, the implications of these twin requirements for international policy collaboration on the one hand, and UK policy integration on the other, were set out in part in the 2013 International Defence Engagement Strategy: 'International Defence Engagement is the means by which we use our defence assets and activities short of combat operations to achieve influence. […] The effectiveness of this engagement and the way in which it can help achieve our international goals depends upon our ability to understand its impact, focus its use, and integrate it with our other levers of influence.' Most recently, the 2015 National Security Strategy and Strategic Defence and Security Review made clear that the aspirations of IbD were more ambitious and comprehensive than the 'short of combat operations' stance taken in the Defence Engagement Strategy: 'We are making our defence policy and plans international by design. Our Armed Forces have always operated internationally, deterring major threats, responding to crises and conflicts, and exercising and building defence capabilities together with allies and partners.' Michael Fallon, then Secretary of State for Defence, argued that IbD reflects 'the reality of how we operate' and observed that 'In a world with global problems we require multinational solutions'.

These arguments are compelling enough, but also rather obvious, leading to concerns that International by Design might be little more than a fashionable truism. Does this expression tell us anything about the merits of alliances and international defence co-operation that we did not already know? Does

IbD cover so much ground (domestic/international, non-military/military, non-combat/combat) that it describes very little of that ground in any practically useful way? What is the overarching purpose of the exercise; to add strategic and operational value, to reduce cost or to cover up shortfalls in equipment and capability? More specifically, what could UK armed forces offer that would persuade potential international partners to participate? Clearly, the UK can offer 'hard power' in the form of maritime, land and air forces. Or should UK armed forces offer its more specialist skills and experience in, for example, the design of military doctrine, strategic and operational planning, training and advisory missions, and command and control? Or does the emphasis on drawing together 'all the instruments of national power' point in a different direction altogether – would the UK be better placed to offer less tangible capabilities such as intelligence coverage and cyber power, and even 'soft power' capabilities such as diplomatic and economic persuasion? In short, is IbD intended to be a more cost efficient 'force multiplier' for UK strategic and operational capability, or a 'force facilitator' for a much larger, international military effort in which the UK is a participant, or is it an attempt at the 'fusion' of the various forms of power – national and international – into a coherent whole? Or is IbD intended to be all of these things at once?

Discussion of allies and partners led inevitably to consideration of the UK's relationship with the United States under President Donald Trump. President Trump has been described memorably as 'consistently inconsistent and predictably unpredictable'. Although amusing in its waspish self-contradictions, this description of the Trump Presidency – if accurate – ought to give pause for thought to the advocates of 'International by Design'. If the UK's most significant politico-military ally cannot be depended upon to decide a course of action and hold to it, then the UK's foreign and security policy outlook might in turn lose some of its coherence and durability. One Conclave participant advised working more closely with those of President Trump's senior advisers who do have a more consistent policy outlook and who do have the ear of the President, particularly Secretary of State Mike Pompeo, Secretary of Defense Jim Mattis and National Security Advisor John Bolton. Neither should the US-UK so-called 'special relationship' be seen to be the exclusive preserve of the President and the Prime Minister; a strong relationship must also develop between the UK Foreign Secretary and his US counterpart. At least one misgiving remained, however; if the culture of the Trump Administration is such that results (or 'the deal') matter more than the process and methods by which results are achieved, then this might not be the most appropriate basis for enduring alliances and partnerships.

The Conclave reviewed the industrial and defence-industrial aspects of International by Design. By one account, UK industry is now at a 'critical turning point' in the light of recent Franco-German agreements on aerospace co-operation, and other developments. As well as preliminary discussions concerning the development of capabilities in medium-altitude, long-endurance unmanned aerial vehicles (i.e. 'drones') and in maritime patrol aircraft, in late April the French and German governments signed a High Level Common Requirement Document concerning SCAF (Système de Combat Aérien du Futur), a programme for the joint development of a sixth-generation combat aircraft to replace the two countries' fleets of Rafale, Mirage III, Tornado and Eurofighter combat aircraft by 2040. While it is not the case that the UK will necessarily be excluded from this ambitious programme (and one that is not without its domestic critics in France and Germany), it might be significant that Florence Parly, France's Armed Forces Minister, is reported to have insisted that 'the priority is to ensure that the Franco-German base is solid before starting to open up to other partners' (including, it must be assumed, the UK). Elsewhere, the relatively established Anglo-French Future Combat Air System (FCAS – involving BAE Systems and Dassault) programme to develop an unmanned combat aircraft capability is reported to be 'falling foul of Brexit', the UK's continued participation in the Galileo satellite project, as well as its association with the European Defence Agency, are both in some doubt, and concerns were voiced that the UK's position as major supplier to the Royal Australian Navy might be usurped by France. As with other western

defence manufacturers the UK is also affected adversely by an international market for military systems and equipment in which the initiative seems once again to be shifting markedly in favour of the buyer; manufacturers are expected to transfer ever more of their manufacturing expertise and technology to their clients, in the form of direct technology transfers, sub-contracting arrangements, licensed and co-development and even co-production. As they fight for market share and comply with these demands, western defence manufacturers might well prove to be the proverbial turkeys voting for their own demise, by knowingly creating for themselves an ever more competitive manufacturing and trading environment.

There were, nevertheless, some traces of cautious, conditional optimism in the Conclave. The UK could position itself to be a leading contributor to SCAF; it could recover some of its capacity and reputation for defence manufacturing, such as in in armoured fighting vehicles; it could maintain its leading position in end-to-end telecommunications, data handling and rotary-winged aircraft; and it could take a more prominent role overall in the international export market. But the development of an export-oriented component to IbD seems unlikely without a far longer-term outlook than the 5-10 years that too often passes for 'strategic vision' in the UK. And without a fully-fledged industrial strategy – a strategy which also embraces defence innovation, technology, manufacturing and exporting, in all five domains of land, sea, air, space and cyberspace – the UK runs the risk of being seen by partners and customers alike as uncommitted, unreliable and uncompetitive.

In its closing stages the Conclave heard calls for a more imaginative approach to the broad themes of international partnership and alliance, and their effects on natural security. Naturally enough, governments tend to be concerned with making partnerships primarily with other governments. But perhaps the time has come to consider forging strategic partnerships with industry itself, particularly in the innovation, communications technology and defence manufacturing sectors. Given demographic shifts and the increasing economic and social significance of dense urban areas, perhaps certain cities could also be considered, in their own right, as potential strategic partners for the UK. In broader terms, does the UK review its geopolitical orientation frequently enough? One participant questioned whether the UK's long-standing loyalty towards its allies in NATO, Europe, the Commonwealth and among the 'Five Eyes' intelligence-sharing community was still relevant and sufficient. Albeit not without some difficulties in the short-term, perhaps the UK should consider establishing closer relations with countries such as Syria and Yemen, building upon these tentative relationships as and when circumstances permit? China has become deeply involved in the Gulf region, strategically and economically, and is a significant contributor to stability operations in Africa. Might the UK consider becoming a strategic partner to China? Or would that be too great a challenge to the 'purity of the narrative'; too much of a departure from the UK's strategic orthodoxy, developed over many decades, which sees China as a competitor at best and as an adversary at worst? Closer to home, the UK has always been conscious of its interests in, and to some extent its obligations to Europe's High North. But as Russia's strategic ambition continues to expand there could be a case for reviving and reinforcing these interests and obligations, and perhaps including Greenland as a potential partner on some level.

The scope and impact of International by Design should not be considered entirely in geopolitical terms, and not necessarily through the prism of the alliance-seeking nation-state. If International by Design is an accurate, yet in some respects still an aspirational summary of the UK's foreign and security policy outlook, then we should certainly ask what effect it might have on national security-relevant research and development in such fields as outer space, cyber space, data management, artificial intelligence, machine learning and human-machine teaming. But we should also reverse the trajectory of the question and examine the effect that these new, even revolutionary developments might have on the relatively 'analogue' idea of partnership and alliance between nation-states and their governments. International

by Design must also satisfy at least one other criterion before it can be considered a success. Security and defence should never be rationalised exclusively in terms of protection from challenges, threats and adversaries; security and defence – and, by extension, International by Design – should also be for socio-economic prosperity and cultural stability. This insight took the Conclave to the heights of political metaphysics: before we can answer the question 'What is International by Design for?' with as much confidence and conviction as we might like, perhaps we should first find a satisfactory answer to another question: 'How does the UK wish to present itself internationally?'

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Conclave Five: Economics of Force

Wednesday 2 May 2018
Royal College of Defence Studies, Seaford House, 37 Belgrave Sq, London SW1

Reflections on the proceedings of the fourth Conclave in Cityforum's Intelligent Defence Series, held on Wednesday 2 May 2018. Speakers and participants included UK Government and House of Commons officials, members of the 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 Conclave were made under the Chatham House Rule.

The final Conclave in Cityforum's Intelligent Defence series asked how national strategy should be shaped and managed when there appear to be too many challenges to national security and well-being, on too many levels and of too many different types, yet too few resources with which to meet all of those challenges. This dilemma is not a novel one: other than in the case of the most militaristic or paranoid regimes, it is difficult to imagine any government, least of all that of a liberal democracy, deciding to commit resources sufficient to meet every conceivable challenge to national security. And in an unsteady world it is equally difficult to imagine any such government opting for absolute pacifism and announcing that the defence budget has been distributed elsewhere in the public accounts.

As ever, it is easier to describe (and dismiss) the extreme points of a political debate – in this case, 'security first' versus 'economy first' – than it is to identify and occupy a point of balance between them. But in essence, national strategy is a matter of compromise, of finding precisely this point of balance. Just as no strategist worthy of the name would ever prepare a plan without considering the resources available, so national security and national wealth are not binary alternatives – neither is credible without the other. In his most recent work On Grand Strategy, John Lewis Gaddis, the eminent historian of the Cold War, defines national (or 'grand') strategy as 'the alignment of potentially unlimited aspirations with necessarily limited capabilities. If you seek ends beyond your means, then sooner or later you'll have to scale back your ends to fit your means.'

National strategy is therefore a bargaining process, of sorts, in which, to paraphrase Adam Smith, the (imperative) burden of national defence must, somehow, never be allowed to exceed what society can maintain (or, in modern parlance, 'afford'). The point of balance is not fixed in time and space; it must be allowed to respond to changing circumstances, strategic and economic, and it is above all a matter of political choice rather than conformity to some unbending law of nature. In an article published in 1992, at the conclusion of his four-year tenure as Permanent Under-Secretary at the Ministry of Defence, the late Sir Michael Quinlan memorably described the way in which UK defence spending does not work:

> *There is an occasional caricature-stereotype of defence planning which supposes that it is – or if it is not, that it ought to be – a basically linear process. One starts by identifying one's commitments; one assesses professionally what forces are needed to meet them; one costs these; and then one sends the bill to the Treasury, which pays up. It is not only in the final particular that this model departs from reality.*

The economics of force are manifested on two levels: the quantum of limited public funds allocated to defence relative to other areas of public spending such as health, social care, education and transport; and the subsequent distribution of the resulting defence budget among many competing strategic and

military claims. The first of these gives rise to what often seems to be a never-ending struggle between the Ministry of Defence and the Treasury over the size of the defence budget and over the outcomes of any interim public spending review. Exacerbated by the phenomenon of 'defence inflation', whereby the input costs of defence rise faster than general inflation, this is a struggle in which defence is too often seen as a regrettable exception to public spending rather than one essential component of it. This in turn gives rise to a fatuous argument in which the input costs of defence (particularly where capital equipment purchases are concerned) are judged, rather simplistically, against input costs in other areas of public spending. Hence, the cost of, say, a Queen Elizabeth class aircraft carrier is debated in terms of the number of hospitals, schools or libraries that could have been bought with a similar amount of public money.

Cross-sectoral comparisons such as these are inane at their worst and, even at their best, are especially difficult to achieve if they are to be both fair and credible. The value of hospitals, schools, libraries and so on, might all be assumed to be self-evident, but what is too often missing in these cost-comparison debates is some sense of the value of defence. A large part of the explanation for this is that economic theory is not particularly helpful when outputs are not readily quantifiable, as is the case in defence. National security and strategic defence can seem to be rather abstract ideas, not least because they suffer from the burden of negative proof; much of their 'value' is hidden and resides in their not being tested – i.e. in preventing the very thing (armed conflict) by which they would be validated. Where defence is concerned, therefore, there is a strong tendency to resort to input measurements or costs, with little attempt at the much more difficult task of setting these costs against the value of the outputs. The result is that defence is too often, and too simplistically, seen simply as a cost – even as a burden upon an otherwise thriving economy – rather than a benefit. It is useful to think in terms of a spectrum of defence benefits, the most obvious of which is of course national security. Then there are other, broader social and economic benefits to consider such as diplomatic and trade ties, social mobility, employment, scientific and engineering innovation and even the popularity among tourists of British military ceremonial. But what is lacking is a credible methodology to quantify, analyse and present these benefits, wherever they appear on the spectrum.

When it comes to the second level of the economics of force – the distribution of the defence budget among competing professional and military claims – we find, in contrast, that the outputs of defence are understood and argued in very much more detail, possibly to the detriment of the national strategic debate. When resources are scarce, inter-service rivalry (sometimes known as 'tribalism') places the interests of an individual service (i.e. the Royal Navy, the Army or the Royal Air Force) at the centre of the discussion. When this rivalry is complemented by 'campaign tribalism', i.e. the insistence that a particular style or theatre of warfare (e.g. carrier-based maritime operations, air interdiction or desert warfare) is sure to be the paramount strategic concern for the foreseeable future, various results follow. First, the national strategic outlook becomes foreshortened to a period (perhaps as little as five years) that could scarcely be described as 'strategic'. Second, the national strategic posture begins to lose its own, internal balance and coherence as this or that 'tribe' threatens to win resources at the expense of others. And finally, when defence is divided internally, it makes it simpler for the managers of the nation's financial resources (i.e. the Treasury) to resist calls for overall budgetary increases. The alignment of national strategic ends and means then reduces to a set of sub-strategic expedients: defence as a whole is subjected to 'salami slicing' where equal misery is inflicted upon all, ensuring that no interest can claim to have been overlooked completely; cuts might be made in 'soft' targets such as training and employment benefits; small equipment orders might be cancelled and larger, capital investments 'slipped to the right'; and at all levels, defence can be subjected to what often seem to be endless calls for improved 'efficiency'.

The spectre of a downward spiral then presents itself. As far as armed forces personnel are concerned, these cost-cutting devices can affect the recruitment, morale and retention of highly-motivated and well-trained men and women. When investments are made in a small number of very costly capital systems such as the Queen Elizabeth class aircraft carriers, these can absorb a disproportionately large share of an already stretched defence budget, further reducing strategic flexibility overall and increasing the pressure on personnel. Another casualty is the depth and breadth of the national strategic outlook; the ability to identify and manage a wide variety of strategic challenges and to prioritise risks. If national strategy cannot do everything, then what should it do? On what basis – and how systematically – are strategic risks analysed and assessed? As one participant observed, whereas it is possible to conduct cost/benefit analyses of the construction of the High Speed 2 rail project, national defence is not analysed in the same way simply because there are no 'units' of peace and security, and so the scale tips in the direction of cost, which can be quantified relatively easily. The misalignment of ends and means is then felt at the operational level, where there are yet more questions awaiting a convincing response. What is the best force posture to meet the range of security and defence challenges the UK might confront? How can armed forces be made more agile and adaptable? Can a 'kinetic' force posture with limited manpower be amplified and optimised through consideration of non-military alternatives (e.g. soft power, sanctions and strategic communications), through a more credible and convincing deterrence posture, and through the most innovative use of emerging technology?

With these thoughts in mind, concerning both the quantum of the UK defence budget and the harmony and efficiency with which it might be distributed, and concerning the quality of strategic analysis in the UK, the mood of the Conclave was rather gloomy as far as the prospects for the 2020 defence review were concerned. That gloom only deepened when it came to consideration of another pillar of national strategy – defence industry, technology and innovation. Participants from the defence and technology sectors spoke of their concern at the scale of underfunding in UK defence manufacturing and research & development. One participant suggested that the pattern of underfunding in defence was likely to continue and that the next defence review would see still less freedom for the Ministry of Defence. The outlook is not good: defence will either be invited to achieve yet more 'efficiencies' or the defence budget will have to increase. If the goal is to align strategy and resources then the first of these options simply does not work, and the second option is simply not likely.

Reflecting what had become a leitmotif of the Conclave, there was deep unease that defence and procurement planning and budgeting in the UK would continue to be input-driven, a situation described as 'perverse'. Emphasis upon the inputs, or costs of defence favours short-term analysis and decision-making, making it difficult to identify and respond to strategic challenges as they begin to emerge, and introducing unwelcome uncertainty into long-term equipment procurement, through-life maintenance and upgrade programmes. And if continuing pressure for savings and efficiencies in the defence budget means that longer-term orders are not made and sustained, then industry will be forced to reduce its investment in research and development and perhaps reorganise its overall portfolio, thus making the downward spiral even more likely and even more hazardous.

If, as is often said, there are grounds for anxiety as to the ability of the Ministry of Defence to manage the defence budget, then there also questions to ask about the basis upon which the government allocates that budget, and the quality of the decisions that it makes. The current view in government is that the functions of defence, intelligence and security (and their associated budgets) are all to some extent indivisible. Given the complexity of international security challenges in the early 21st century this is an intellectually reasonable position to take. But it is also a position that, unwittingly or otherwise, challenges the very notion that national defence is still a largely discrete policy (and budgetary) concern and not simply a throwback to the soon-to-be forgotten years of the Cold War. If government is

ambiguous on this point, then it is easy to see how the defence budget itself can become a subject for debate rather than commitment. Parliament also carries some responsibility for the quality of the debate. Government is held to account for its defence decision-making, but often rather patchily. The highly expert inquiries and reports of the National Audit Office and the House of Commons Defence Select Committee do much in this regard, but Parliament in general lacks knowledge and expertise in defence, meaning that inconsistent and even eccentric ideas can often go unchallenged. In a circular fashion, Parliament's partial engagement with defence is a reflection of the position taken by the electorate, bombarded as it is by the narrative of input and cost, to the exclusion of a sense of output and value.

The United Kingdom could do better than this; better than lurching from one emergency, cost-driven defence review to another. For example, there is a pressing, and not unreasonable, need for the government to produce a genuine, forward-looking defence industrial strategic outlook for land, sea and air power. But the paramount requirement is for the government to lead a defence debate that focuses more closely upon and achieves a knowledgeable and sustainable national consensus regarding the broad value of defence. Without this consensus, it is difficult to see how any government could ever develop a durable strategic outlook, and least of all in an international security environment that seems so complex and volatile. The alternative is to delay difficult and costly decisions until the next crisis arrives, in the vain hope that there will be enough time for strategic and technological reaction and decisive reinforcement. In short, the choice facing the UK strategic community, both official and non-official, is either to encourage political will to move in the direction of a balanced, dependable and industrially supportable force posture, or wait for tragedy to make that case.

A UK Defence and Security Round Table arranged by Cityforum in association with DCDC

Intelligent Defence and Smart Power
- innovation, capability, delivery, advancing the national interest

Thursday 12 July 2018
Royal College of Defence Studies
Seaford House, 37 Belgrave Square, London SW1

Agenda

Principal sponsor BAE SYSTEMS

Co-sponsors KBR

SME Sponsor BOXARR

Hosted by

Welcome and Introduction by Mr Marc Lee *Chairman* Cityforum

0900 - 1300 **MORNING SESSIONS: ADVANCING INNOVATION, AGILITY AND PACE**
Opened & Chaired by: Mr Stephen Phipson *Chief Executive* EEF

0905-1030 **Session one: Opening addresses**

Ambition for defence in an information world
Mr Charles Forte *CIO* MoD

Moving towards information advantage
Professor Penelope Endersby *Division Head, Cyber and Information Systems Division* Dstl

The challenges of change of pace – how can they be met?
Mr Martin Taylor *Chief Operating Officer – Air* BAE Systems

Advancing systems security
Mr Rob Joyce *Senior Adviser for Cybersecurity Strategy* National Security Agency

Followed by round table discussion

1030 **COFFEE**

1045-1145 **Session two: What a reimagined ecosystem requires and how to deliver it**

Adjusting military mindsets and attitudes – what is required and how to change?
Air Vice-Marshal Simon 'Rocky' Rochelle *Chief of Staff Capability (RAF)* MoD

The right ecosystem for logistics and through life support – the achieved and achievable
Major General Angus Fay *Assistant Chief of Defence Staff (Logistic Operations)* MoD

Redefining how defence partners with industry to access an open ecosystem
Mr Tim Barber *Head of Advisory EMEA* KBR

Followed by round table discussion

1145-1300 **Session three: Implementing successful change: what is now required? Where do responsibilities lie? Where do we go from here? Is there too much inertia? Is too much of the budget already committed? Is the cash position too tight for real risk-taking? How can we grapple with complexity?**

A panel discussion including the following:
Mr Fraser Hamilton *VP for Global Alliances* Boxarr
Mr Francis Tusa *Editor* Defence Analysis
Mr Mark Barclay *CEO* UK Defence Solutions Centre
Dr Lucy Mason *Head* Defence & Security Accelerator

Followed by a round table discussion with a comment from **Lt Gen (Retd) Dick Applegate** *Associate* Cityforum

1300 **LUNCH**

1400-1715 **AFTERNOON SESSIONS: THE CONTRIBUTION OF INTELLIGENT DEFENCE TO SMART POWER IN THE NEXT DECADE**
Chaired by: Professor Paul Cornish *Chief Strategist* Cityforum and co-author of *2020: World of War*

1400-1535 **Session four: Smart power and what contributes to it**

Keynote address: Intelligent defence and smart power – the delivery challenges
General Sir Gordon Messenger *Vice Chief of Defence Staff* MOD
Followed by Q&A

Conclusions from the Cityforum conclaves and acquisition discussion – delivery challenges
Professor Paul Cornish and **Major General Mitch Mitchell** *Director* DCDC

How politicians see intelligent defence and smart power – means and ends
The Rt Hon Mark Francois MP *Member of Defence Select Committee* House of Commons (Con)
and
Mrs Madeleine Moon MP *Member of Defence Select Committee* House of Commons (Lab)

Followed by a round table discussion on political priorities opened by **Mr Tim Ripley** *Associate* Cityforum and *Correspondent* Janes Defence Weekly and Sunday Times

1535 **TEA**

1550-1715 **Session five: What and how can smart power contribute to the reputation and prosperity of the UK?**

Ms Bridget Kendall *Master of Peterhouse* Cambridge University & *Former Diplomatic Correspondent* BBC with
Ms Carole Nakhle *Author, Researcher* and *CEO* Crystol Energy *(with a perspective from the Middle East)*
Mr Oliver Welch *Head of Defence, Aerospace and Security Policy* EEF
Professor Gunnar Heinsohn *Demographic and Baltic Security Specialist* NATO Defence College
Dr Liane Saunders *Strategy Director and Strategic Programme Director* FCO

Followed by a round table discussion with a comment from **Mr Ed Gillett** *Director Defence* BAE Systems

Conclusions from **Professor Paul Cornish** and **Gen (Retd) Sir Jack Deverell** *Associate* Cityforum

1715 **CLOSE**

A Cityforum Conclave in the Intelligent Defence and Smart Power series developed in collaboration with the MoD and Development, Concepts and Doctrine Centre

Round Table: Intelligent Defence and Smart Power

Thursday 12 July 2018
Royal College of Defence Studies, Seaford House, 37 Belgrave Sq, London SW1

Reflections on the proceedings of the Round Table discussion concluding Cityforum's Intelligent Defence series, held on Thursday 12 July 2018. Speakers and participants included UK Members of Parliament, UK and other government officials, officers of the armed forces and representatives of the private sector (UK and international), scientific and policy research institutes, academia and the media. This report was prepared by Cityforum Chief Strategist Professor Paul Cornish. All contributions to the Round Table were made under the Chatham House Rule.

Building upon the success of a programme of five Conclaves held between November 2017 and May 2018, Cityforum's Intelligent Defence series concluded in July 2018 with a Round Table discussion under the title Intelligent Defence and Smart Power. The five Conclaves (summary reports of each are available) had set out the international security context against which national security and defence policy and strategy must be formed. Each of the Conclaves had examined a particular theme: the difficulty of devising a national strategy that can be coherent, effective and consistent at a time of great turbulence in the international security environment; the need to revisit, reapply and normalise the ideas, capabilities and practices associated with deterrence; the problems and possibilities presented by information and communications technology and by the surge in data traffic; the meaning and value of 'International by Design' in UK security and defence planning; and finally, the problem of the distribution of scarce resources to, and within, defence – the 'economics of force'.

The goal of Cityforum's concluding Round Table was to return to the large, overarching questions concerning national interest and the exercise of power; questions which must be addressed, and answered more than adequately, if UK national security and defence strategy is to be considered credible and durable. The first three morning sessions of the Round Table covered innovation, information and the need for a more effective, productive and intelligent relationship between government, industry and the armed forces. Two afternoon sessions then addressed the relationship between 'intelligent defence' and 'smart power', asking how the latter might contribute to the UK's strategic reputation and position.

Session One began by questioning the UK's appetite for challenge, particularly in the field of security and defence. In an international security environment characterised more by discontinuity than continuity, and in which the breakdown of the much-vaunted 'rules-based international order' seems imminent, if not already underway, it is vitally important to know how aggressive the UK can, or should be in responding to change and challenge. Cyber defence was described as a dynamic challenge, with threat surfaces becoming ever more extensive and attack vectors ever more available. Cyber 'hygiene' must be part of the response, but this is a largely passive activity; efforts must also be made to close known and identified 'backdoors' to cyber intrusion. A large part of the national cyber security challenge, however, is that the public – at the same time the most numerous and the least secure users of information and communications technology – do not optimise for security; instead they optimise for usability and for cost. If that is the case, then a very large part of national cyber security might have to be achieved neither by marketing nor by persuasion but might have to be 'designed-in' at the architectural- or system-level, with all the implications such an approach might have for internet freedom and privacy.

More generally, the effectiveness and efficiency of UK defence would improve immeasurably if the relationship between government, industry and the armed forces could become more cohesive, co-operative and productive. But that relationship cannot be sustained entirely by the need to respond effectively to urgent operational need; defence industry requires a long-term strategic vision and a durable innovative and manufacturing infrastructure if it is to be sustained.

One area in which that relationship should be tightened is innovation. Real innovation begins with ideas and invention. Rather less convincingly, the meaning of innovation has also come to include the insight that existing capability can be put to better, more decisive use, or can be applied effectively in different circumstances. Either way, the various stages of the innovation process – idea; invention/insight; adoption; implementation – could be made more coherent and purposive and could run at a faster pace. But improved decision-making in defence, procurement and innovation will also require the exploitation of the information advantage – the 'credible advantage gained through the continuous use of information'. In other words, UK defence needs to ensure that its decisions are based upon the best, and most timely analysis of the best available information. The requirement for rapid, information-based decision-making could have a direct effect on the UK's strategic and defence culture and on procurement and innovation decisions. The growth in data sources and the resulting flood of data are likely to see greater interest in artificial intelligence (AI) as a means to collate and process vast amounts of data at speed, with all the ethical and practical challenges associated with AI. The data revolution might also provoke interest in more distributed and even quasi-autonomous models of command and control, as an alternative to the more traditional and centralising 'top-down' model of politico-military relations. And as if to counter any hint of confidence in our capacity to meet these challenges, Session One concluded with a gentle warning. It is commonplace to describe the pace of technological change as 'dramatic', 'unprecedented' and so on. But history could show the pace of change over the past twenty years or so to have been relatively genteel when compared to what the next decade or two might bring.

The possibility of a 'reimagined ecosystem', in which government, industry and the armed forces collaborate more effectively and purposefully, was the focus of Session Two. The traditional procurement mindset must adapt, not least to the innovation/acquisition challenge presented by Russia – and there are encouraging signs that adaptation is taking place. The MoD and industry are showing greater willingness to share financial risk at the design stage of new equipment. And the Royal Air Force's recently established Rapid Capability Office shows how civil and military expertise can be blended in an attempt to overcome commercial barriers and decision paralysis. Defence logistics – amounting to roughly one third of annual defence expenditure – are another area where improved collaboration between industry and the armed forces can yield mutual benefit. The logistics 'ecosystem' is ripe for innovation, albeit more by way of adaptation and exploitation of existing, worked practice in the civil sector than invention per se. Defence logistics are also vitally dependent upon the quality and timeliness of information, and by ensuring that information management networks are themselves resilient to attack and intrusion.

From the perspective of industry, it should by now be clear to all concerned that 'business as usual' can no longer be an option. The government-industry-armed forces relationship must be allowed to diversify, creating opportunities both for non-traditional prime suppliers and for other, smaller organisations to make more of a contribution to decision-making in procurement and supply chain management. These decisions should be viewed in the round, taking full account of the social value of contracts. In that vein, procurement should be seen to be more openly collaborative, with the supply chain also made more transparent. If the UK's defence industrial ecosystem could be reimagined and re-energised in this way and if, as one participant put it, there could be a 'clear line of sight from industry to the armed

services', then the UK defence industrial and procurement system might become more self-confident and innovative and better positioned to bid for increased market share in Europe, NATO and elsewhere.

As ever, it can be one thing to describe the nature, depth and urgency of a problem, but entirely another to do something effective about it. If the defence industrial ecosystem is to become more 'agile' and 'adaptive' (terms that have both been over-used for decades in the UK defence debate, to the extent that they are now rather worn clichés) then what is to be done? Session Three of the Round Table discussed structural impediments to change. Where do the responsibilities for adaptation actually lie, and how should these responsibilities be apportioned between government, industry and the armed forces? Is there simply too much inertia in the UK system, such that challenges can be described – often very vividly – but are rarely, if ever, resolved? Whenever there are calls to improve complex systems and processes some level of investment is often required. But does the UK defence budget have any spare capacity to allow for such investment? Is there any appetite – financial, political and organisational – for taking risk on business reform in defence? Fundamentally, is the UK defence ecosystem optimally configured to manage complexity and urgency, or must it remain confined within patterns of behaviour and decision-making that have evolved over decades; doomed to repeat the errors of the past, and perhaps at shorter intervals?

For some contributors to Session Three the UK defence acquisition environment seemed almost to be a lost cause, barely fit for purpose. In the current fiscal and political climate, the MoD has become deeply risk averse where investment is concerned. The three-way relationship between government, industry and the armed forces has too many habits and procedures that are 'baked-in', where the rationale for doing business in this or that way might be long forgotten, yet resistance to doing business in any other way is stifled. The MoD does not communicate well; rather than using plain language and clear arguments, the MoD's position (to the extent that it is explained) is too often incomprehensible to the public. The MoD should try much harder to put digestible information concerning defence policy and strategy into the public domain. Where defence-related innovation is concerned, the MoD could also take more active and confident role. The 'spin-off' trajectory of innovation – whereby the defence establishment sponsored highly classified science and technology (S&T) work leading to research and development (R&D) programmes from which civilian uses might eventually spring – has long since passed into history. The trajectory has now been reversed; it is largely the civil sector that is in the lead in S&T and R&D, most obviously in information and communications technology. But the change in trajectory from 'spin-off' to 'spin-on' ought not to mean that the UK MoD must be demoted to second-class status where defence innovation is concerned, passively accepting whatever civil research puts on offer while reassuring itself that 'adaptation' and 'implementation' are just as valid and effective as 'invention'. Indeed, the MoD appears very keen not to be demoted in this way, as the work of the Defence Science and Technology Laboratory (now encompassing the Home Office's Centre for Applied Science and Technology) and the Defence Solutions Centre would attest. There are also indications (or, perhaps, rumours) that the Modernising Defence Programme, due to report in full in late 2018, will create more opportunity for innovation, creativity and accelerated implementation. But to will the ends without willing the means can, at best, amount to hollow promises and, at worst, result in self-delusion. Real innovation requires investment at risk, and the overwhelming problem for UK MoD in 2018, to coin a phrase, is that 'there is no money'. In the view of one participant, the MoD's finances are in a parlous state: Defence has lost the budget 'battle' with the Treasury and might even have lost the 'war'; the Future Force 2025 plans are simply not affordable (even without the current 'black hole' in MoD finances); defence procurement programmes are out of control and in some cases are failing; yet the UK persists in the fantasy that it can afford 'full spectrum capability', remaining a 'tier one' power in global defence. In short, the UK government, MoD, Parliament, media and public must all begin to accept that there are difficult, role-redefining choices to be made where defence is concerned.

Session Four of the Round Table began with the suggestion that in spite of dire assessments made of the state of UK defence there is a persistent tendency to dismiss such warnings as being too inconvenient or too overwhelming if taken too seriously, and instead to paint an image of the UK defence landscape that is far more appealing than the reality. The inclination to 'put lipstick on a pig' is a common reaction among organisations (and individuals) when facing stressful situations but where UK defence is concerned it can persuade policy-makers that adverse evidence can be safely ignored and that the UK is in the fortunate position of being able to take a 'strategic holiday', much as it did in the 1930s and late 1940s. High-level reluctance to discuss UK defence 'warts and all' might also explain another enduring deficiency in the UK defence debate; the lack of a reasonably settled view of the value of national defence, in which input costs (the price of a new ship, vehicle or aircraft) are set against output benefits (territorial defence, national security, alliance cohesion etc).

The security and defence challenge the UK is likely to confront in the coming decade suggest that intelligent defence and smart power will be vital to success. The international security environment is in a state of perpetual competition, with the drivers of conflict becoming ever less predictable, the boundaries between war and peace ever more blurred and the political and legal criteria used to classify conflict ever more opaque. The UK will not, however, be able to bury its head in the sand, ostrich-like, and hope that it will be unaffected by turbulence and conflict around the world. The UK will need both the willingness and the capability to act militarily wherever and whenever necessary. But armed force is unlikely to be a sufficient answer to all global security challenges. Instead, UK defence will be a 'strategic effector'; one of many levers – 'hard', 'soft' and 'smart' – being orchestrated by the UK's national security architecture. The willingness and the capability to act will also be vital to the rediscovery of the importance of deterrence in the overarching national strategic posture. And deterrence, too, will have to be cross-governmental if it is to be successful, involving far more than simply the military instrument. Maintenance of the information advantage will be an essential component of UK smart power, and failure to ensure resilience in national information and communication networks will ensure that the UK's strategic power and influence will be anything but 'smart'. The UK's strategic decision-making processes will need to be rapid, proportionate, deliberate and comprehensive; a requirement that will see growing reliance on big data management, artificial intelligence, human-machine teaming and machine-machine learning. Technological shifts such as these will become the norm rather than the exception and for that reason UK strategy will need to be institutionally (as well as technologically) innovative; constantly re-evaluating the national strategic posture against prevailing international circumstances and adapting and changing that posture in order to maintain the strategic edge.

Before it can confront these external challenges, UK defence must first tackle its own internal deficiencies that make it too slow to adapt to changes in the international security environment. There is too much structural inertia in UK national defence and too little readiness to accept the need for change. UK defence remains embedded in processes and practices that are products of its strategic past, barely suited to the second and third decades of the 21st century. At present, the UK also lacks the practical and intellectual skills that will be necessary for any future defence force. These deficiencies can be remedied, if there is a willingness (and the budget) to do so. It should be possible, for example, to conduct far more military (and perhaps cross-governmental) training in simulated environments. It should also be possible address the shortage in key trades; to tackle the backlog in maintenance tasks; to address (through improved pay and conditions) the decline in retention of trained personnel in the armed forces; to build up reserve and reinforcement capabilities to a more convincing level; and to improve the knowledge and understanding of international security threats and challenges among Parliamentarians. Most, if not all of these measures will, of course, require further investment in defence. But the UK government seems at present to have little or no appetite for increased defence spending, in spite of the volatile international security environment and in spite of the House of Commons Defence Committee, and

others, making a strong case for an increase in the defence budget by perhaps as much as fifty percent.

The final session of the Round Table asked how smart power could contribute in the broadest sense, to the UK's prosperity and to its international standing and reputation. Discussion began by noting the contrast between the way the UK appears to see itself in the world, and (at least for the time being) the way it is seen by others. Whether or not it is useful and accurate to describe the UK as being in the global 'first tier' (whatever that term means) one participant argued that the UK is widely acknowledged to be a significant, medium-sized economic and trading power with excellent intelligence services, highly capable armed forces and very strong reserves of soft power. Yet in spite of these advantages, the UK seems to be suffering from a progressive loss of confidence in itself and risks becoming increasingly inward looking and small minded. At a time when democracy and the international rule of law are having to confront economic nationalism, populism and a deceptively benign brand of authoritarianism, the UK – one of the founding liberal democracies and an exemplar of western values – should surely be taking a more prominent role in the world, rather than shrinking from it. It is as though the UK has chosen to focus its attention on the threats (such as that of terrorism) and vulnerabilities (to economic uncertainty, for example) it faces, rather than the opportunities it can exploit and the example it is expected to set (in global energy and green politics, for example). As a consequence, the UK seems to be forgetting its own historical identity as a global actor and is satisfying itself with a very narrow, geopolitically confined understanding of its national interest and becoming increasingly suspicious of what goes on beyond its coastline. Without a more settled and self-confident sense of its own national identity, with highlights as well as blemishes, the UK is not likely to identify a coherent and durable national strategic goal and as a result is unlikely to be seen as a reliable partner by allies (particularly those in NATO) and other like-minded countries around the world. And if the UK can acknowledge all these demands and commit itself to a national version of cognitive behavioural therapy, the final task will be to invest in an urgent, sophisticated and high-level strategic communications campaign, directed at both allies and adversaries, at the UK public and at the media and other opinion formers.

Although analysis of the UK's current economic and strategic position does not generally give much cause for comfort, there are some hints, at least, of a possibly more optimistic future. If UK defence industry can accept that it must from now on be in a 'permanent state of evolution', and if the tripartite relationship between government, industry and armed forces could mature into something more genuinely collaborative and mutually supportive (perhaps even to the extent of revisiting the idea of some form of 'national service' involving the technology sector), then UK defence could regain a leading role in innovation, production, procurement and through-life support. If the UK could look beyond Europe and NATO then it might see possibilities for the development of other, more relevant alliances and partnerships; the notional seventeen nation 'Northern Alliance' was mentioned in this regard. If the UK could see China in a different light, other than as an ideological, economic and strategic competitor, then it might identify the bases of mutually beneficial co-operation. And if the UK MoD could identify a 'David Attenborough for defence' then UK policy makers and public opinion will achieve a deeper understanding of the value of defence and all will be well

Cityforum would like to thank the following for their support:

BAE SYSTEMS

BOXARR

FUJITSU

KBR

NATS

QINETIQ

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, 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 defence and 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. Its reports are succinct and written in readable English rather than in management speak loaded with acronyms.

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 had an interest in defence going back to the time of the George Robertson Review and it has been involved in numerous discussions in London, Washington, Abu Dhabi and elsewhere. It has welcomed support of the last Chief of Defence Staff for this particular Intelligent Defence and Smart Power work and has been particularly grateful to the current Vice Chief and the Director of DCDC for their engagement in developing the questions for assessment by panellists from defence and security and other significant vantage points. The help of the corporate sector in making this complex project happen has been particularly welcome.

Cityforum has a particular interest in working with the private sector to examine questions that companies wish to answer, as they develop their offers to government departments and agencies at home and abroad. Assignments are undertaken by a director of Cityforum and members of its group of associates and specialists are brought in, as required. We offer analysis, advice and guidance but do not offer a suite of solutions, since doing so could affect the independent advisory stance we see as essential.

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